4/5

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGON

ANALISIS DE LA PROBLEMÁTICA EN LA TRANSFERENCIA DE INFORMACIÓN UTILIZADO SNAX/APC ENTRE REDES INFORMÁTICAS Y PROPUESTA DE SOLUCIÓN

T E S I S

QUE PARA OBTENER EL TÍTULO DE

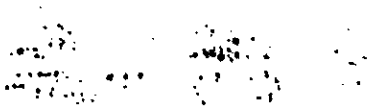
INGENIERO MECANICO ELECTRICISTA

P R E S E N T A N:

JESUS MORA GÓMEZ
OSCAR CARMONA MORA

ASESOR :
ING. DAVID B. ESTOPIER

MEXICO 2000



A mis padres con todo cariño. A quienes les debo todo lo que soy.

Los amo profundamente.

A Mi Familia:

Por la confianza y ejemplo
recibidos siempre

Chucho y Oscar:

Un Hermano puede no ser un amigo,
pero un amigo será siempre un
Hermano.

A mi Esposa Laura:

Por su amor, apoyo y ayuda que he recibido siempre

Oscar

A Mi Familia:

Por la confianza y ejemplo
recibidos siempre

Chucho y Oscar:

Un Hermano puede no ser un amigo,
pero un amigo será siempre un
Hermano.

CONTENIDO

INTRODUCCIÓN

Breve historia de las Redes Locales

El almacenamiento y el análisis de información han sido uno de los grandes problemas a que se ha enfrentado el hombre desde que inventó la escritura. No es sino hasta la segunda mitad del siglo XX que ha podido resolver, parcialmente, ese problema gracias a la invención de la computadora.

En la década de los 50´s el hombre dio un gran salto al inventar la computadora electrónica. La información ya podía enviarse en grandes cantidades a un lugar central donde se realizaba su procesamiento. Ahora el problema era que esta información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser "acarreada" al departamento de procesos de datos.

Con la aparición de las terminales en la década de los 60´s, se logró una comunicación directa, y por tanto más rápida y eficiente, entre los usuarios y la unidad central de proceso, pero se encontró un obstáculo: entre más terminales y otros periféricos se agregaban al computador central, decaía la velocidad de comunicación.

A finales de la década de los 60´s y principios de los 70´s la compañía DEC penetra en el mercado con dos elementos primordiales: la fabricación de equipo de menor tamaño y regular capacidad, a los que se denominó minicomputadoras, y el establecimiento de comunicación relativamente confiable entre ellos.

Hacia la mitad de la década de los 70´s la delicada tecnología del silicón (silicio) y de la integración en miniatura permitió a las fabricantes de computadoras construir mayor inteligencia en máquinas más pequeñas. Estas máquinas, llamadas microcomputadoras, descongestionaron a las viejas máquinas centrales. A partir de ese momento, cada usuario tenía su propia microcomputadora en su escritorio.

A principios de los 80´s las microcomputadoras habían revolucionado por completo el concepto de la computación electrónica, así como sus aplicaciones y mercado. Sin embargo, los gerentes de los departamentos de informática fueron perdiendo el control de la información puesto que el proceso de la información no estaba centralizado.

A esta época se le podría denominar la era del floppy disk. Los vendedores de microcomputadoras proclamaban: "en estos 30 diskettes puede usted almacenar la información de todo su archivo".

Sin embargo, de alguna manera, se había retrocedido en la forma de procesar la información, porque nuevamente había que acarrear la almacenada en los diskettes de una micro a otra y la relativa poca capacidad de los diskettes hacía difícil el manejo de grandes cantidades de datos.

Con la llegada de la tecnología Winchester se lograron dispositivos que permitían enormes almacenamientos de información, capacidades que iban desde 5 hasta 100 megabytes. Una desventaja de esta tecnología era el alto costo que significaba la adquisición de un disco duro. Además, los usuarios tenían la necesidad de compartir información y programas en forma simultánea.

Estas razones, principalmente, aunadas a otras como poder compartir recursos de relativa baja utilización y alto costo, llevó a diversos fabricantes y desarrolladores a idear las redes locales.

En un principio, las redes de microcomputadoras se formaban por simples conexiones que permitían a un usuario accesar recursos que se encontraban residentes en otra microcomputadora tales como otros discos duros, impresoras, etc. Estos equipos permitían a cada usuario el mismo acceso a todas las partes de un disco y causaban obvios problemas de seguridad y de integridad en los datos.

Hacia 1983, la compañía Novell, Inc. Fue la primera en introducir el concepto de File Server (servidor de archivos) en el que todos los usuarios pueden tener acceso a la misma información, compartir archivos y contar con niveles de seguridad.

En el concepto de servidor de archivos, un usuario no puede accesar, indistintamente, discos que se encuentran otras microcomputadoras. El servidor de archivos es una microcomputadora designada como administrador de los recursos comunes. Al hacer esto, se logra verdadera eficiencia en el uso de éstos, así como una total integridad de los datos. Los archivos y programas pueden accesarse en modo multiusuario guardando el orden de actualización por el procedimiento de bloqueo de registros. Es decir, Cuando algún usuario se encuentra utilizando un registro, se bloquea éste para evitar que algún otro usuario lo extraiga o intente actualizar.

Novell basó su investigación y desarrollo en la idea de que es el software de la red, no el hardware, el que hace la diferencia en la operación de una red. Esto se ha podido constatar. En la actualidad, Novell soporta a más de 100 tipos de redes.

Durante los años, entre 1985 y la actualidad, las redes lucharon por colocarse como una tecnología reconocida contra todo tipo de adversidades. En un principio, IBM no consideraba a las redes basadas en microcomputadoras como equipo confiable.

Había inclusive personas que llegaban a declarar que las microcomputadoras habían sido concebidas como islas de información en las que un usuario debería tener al alcance de su escritorio todos los elementos para constituir un pequeño centro de computo autosuficiente. Según ellos, las computadoras personales deberían ser computadoras personalistas.

No es sino hasta la exhibición COMDEX, de 1997, cuando IBM acepta esta tecnología como el reto del futuro y acuña el término "conectividad". Después de este evento se desata un crecimiento acelerado de la industria de las redes locales. Todos los fabricantes se lanzan a adapta sus equipos y a proponer nuevas posibilidades en esta área.

Las tendencias actuales indican una definitiva orientación hacia la conectividad de datos. No solo en el envío de información de una computadora a otra sino, sobre todo, en la distribución del procesamiento a largo de grandes redes en toda la empresa.

En la actualidad existe un gran interés, por parte de todo tipo de usuarios, en las redes locales. El reto importante para los desarrolladores de esta tecnología es ofrecer productos confiables, de alto rendimiento que hagan uso de la base instalada ya en el usuario final.

A este último concepto se le denomina tecnología de protocolos abierto. Es decir, ofrece a los usuarios soluciones de conectividad que sean compatibles con el hardware y el software ya adoptado por el usuario sin importar la marca, sistema operativo o protocolo de comunicación que use.

Novell, por ejemplo, ofrece desde hace algún tiempo el concepto de "conectividad universal" bajo NetWare, según el cual es posible integrar sistemas operativos anteriormente incompatibles como VMS, UNIX, DOS, Macintosh, los cuales se comunican por medio de una gran variedad de protocolos como TCP/IP, IPX, X.25, NetBios, etc.

En la década de los 90 se espera un continuo crecimiento de la industria de redes locales, así como el surgimiento de más tecnologías de conectividad independientes de protocolos y de equipos propietarios.

La creciente integración de computadoras y comunicaciones dentro de un sistema único y universal, ha llevado a la creación de una industria nueva y de rápido crecimiento: la industria de la comunicación de datos basada en computadoras. Aunque su antigüedad, apenas es de una década, los logros tecnológicos dentro de la industria han sido significativos. En universidades, complejos industriales e instituciones financieras existe una posibilidad cada vez mayor de que los servicios de comunicación enlacen la computadora central con usuarios remotos.

Los adelantos de la tecnología permiten que las comunicaciones tengan lugar a través de grandes distancias cada vez con mayor facilidad. Las computadoras hablan a las computadoras; la gente habla a las computadoras y las computadoras hablan a la gente. Así como el teléfono se ha transformado en una necesidad, el servicio de cómputo se esta convirtiendo en una herramienta administrativa corriente. Este rápido cambio ha forzado a muchos de los medios corrientes de comunicación hasta sus límites tecnológicos. Nuevas ideas de diseño y conceptos tecnológicos revolucionarios están surgiendo en todas partes.

Hoy es cada vez mayor la interrelación y la interdependencia de oficinas y lugares de trabajo geográficamente dispersos. Nuevos conceptos administrativos exigen una disponibilidad de los datos que sea eficiente y oportuna. Esto obliga a inversiones cada vez mayores en equipos y sistemas que procesen los datos con la menor demora, no importando cuál sea la distancia entre las fuentes de datos ni el lugar destino de la información.

Definir a las telecomunicaciones no es una tarea sencilla, ya que por si misma comprenden un conjunto de sistemas, dispositivos y técnicas empleados para la transmisión de información a larga distancia de modo instantáneo. Por lo tanto los principales medios utilizados en estas transmisiones son:

- La radiocomunicación. Fue impulsada desde principios del siglo XX por los trabajos de Guillermo Marconi y pretende la transmisión del sonido a través de ondas electromagnéticas que acompañan a los campos eléctricos y magnéticos producidos por diversos medios y proyectados hacia el espacio desde una antena emisora sin utilización de cables o hilos conductores.
- La transmisión por cable. Se basa en la transferencia de datos a través de un canal de comunicación. Mientras que un canal de transmisión será el camino entre nodos de una red. Puede referirse al cable físico, a la señal transmitida por el cable o a un subcanal dentro de una frecuencia portadora.
- Satélites artificiales. Los satélites ofrecen prestaciones de comunicación de datos, por lo que cuentan con canales que reciben señales digitales y analógicas de estaciones terrenas. Todas las señales son transmitidas en una frecuencia portadora. Así mismo, las señales son amplificadas y retransmitidas a la Tierra, al cubrir un área geográfica pequeña o bien casi una tercera parte de la superficie terrestre.

El proceso general de la transmisión a través de un sistema de comunicaciones comprende cuatro elementos fundamentales:

- El mensaje fuente. Hasta la fecha está suministrado por la voz, señales de TV, datos informáticos o signos gráficos. Desde el punto de vista de las telecomunicaciones, las señales son de dos clases: analógicas, esto es una sucesión de impulsos de mensaje continua y variable con el tiempo como ocurre con la voz y la música; y digital o de transmisión discreta, como los mensajes de las computadoras.
- El emisor. Es quien emite el mensaje y tiene las siguientes funciones:
  Trasformar en información eléctrica los mensajes que se desean transmitir,
  Modificar la información para que esta viaje a distancia y
  Transmitir la información por la vía o canal seleccionado.
- Receptor. Es el objetivo del mensaje emitido y cumple con funciones inversas a las del emisor:
  Detecta información trasmitida por el canal de comunicación
  Transforma la información eléctrica en sonora, visual, datos, video etc.
- Canal o vía de comunicación. Es el medio a través del cual el mensaje viajará para llegar a su destino, su función es la de transportar la información desde el emisor hasta el receptor.

El avance de las telecomunicaciones se ha visto reflejado directamente en los ambientes financieros, por ejemplo, los sistemas para usar más eficientemente los medios de comunicación, han ido de la conmutación de circuitos a la conmutación de paquetes y recientemente a la conmutación de tramas. La conmutación de circuitos que esta implementada en el país utiliza Convertidores Analógicos/Digitales (DaCa) que conmuta canales de 64 Kbps de un E1. Este sistema es útil para canalizar un E0 de un usuario a otro y puede emplearse en la interconectividad de redes, pero es necesario combinarlo con un sistema de conmutación de tramas, en aplicaciones donde se pretende hacer mejor uso del canal, sin tener que dedicarlo a un solo usuario en un esquema punto a punto.

Todas las redes locales de banco estaban conectas entre sí y utilizaban ruteadores, puentes locales y remotos a través de medios de comunicación diversos que incluían fibra óptica, rayo láser, espectro disperso y microondas. En lo concerniente a la red externa había varios tipos de acuerdo al medio y la aplicación Entre ellos destaca la red financiera que operaba con un esquema punto multipunto que utiliza señales de radio en la banda de frecuencia de los 500 MHz. Esta red enlazaba computadoras personales a los que una vez que se les insertaba una tarjeta PEP (Protocolo de modem de alta velocidad) y se cargaba el software necesario, emulaban terminales del computador central. Los problemas que se generaron con este tipo de redes fueron:

- Al hacer algún cambio se debía agregar equipo como modem, multiplexores, insertar tarjetas de terminal y tender cableado, en el caso de nuevos sitios remotos se tenían que instalar antenas y conectar nuevos equipos de radio.
- Los diversos sistemas no estaban integrados, lo cual involucraba duplicidad de canales de comunicación y de equipo, lo que hacia más dificultoso el mantenimiento.
- Las velocidades de operación eran relativamente bajas: 4,800 y 9,600 bps.
- Hacían presión de usuarios para emplear recursos que en algunos casos estaban subutilizado, como la red digital integrada de Telmex.
- El esquema de comunicación que se tenía dificultaba la implementación de nuevos sistemas de información.

Actualmente todas las Casas de Bolsa tiene enlaces de RDI, tienen Multiplexores TDM (Time Division Multiplexing) múltiple y están conectados a Conectores digitales cruzados de teléfonos de México, lo cual les permite direccionar E0 de su sistema E1 a diversos destinos.

CAPITULO 1. CONCEPTOS GENERALES

1.1. ANTECEDENTES

Desde que se inventó la primera computadora siempre se ha buscado hacer del manejo de la información un proceso eficiente.

Podemos distinguir entonces, tres etapas de la evolución de las computadoras o bien tres rangos en las que estas se dividen:

- MACROCOMPUTADORAS, computadoras con procesos múltiples, multitarea y multiusuario, capaces de soportar una gran cantidad de Terminales concentradas a la vez.
- MINICOMPUTADORAS, que con sistemas de computo similares a las primeras pero con menor carga de trabajo y menor capacidad de procesamiento.
- MICROCOMPUTADORAS, cuya aparición es relativamente joven, estas máquinas vinieron a romper el esquema de máquinas centralizadas para comenzar con una etapa de computadoras personales capaces de procesar información de manera muy rápida.

Estos tres tipos de máquinas convivieron durante un tiempo sin pensar siquiera en el momento de unirse, pero la necesidad en el manejo de información, el rápido ritmo de crecimiento económico, el gran avance de la ciencia de la computación y otros factores han hecho inaplazable el acercamiento de los diferentes tipos de sistemas de computo.

Este lazo que une computadoras, sistemas operativos e información es llamado: REDES, REDES LAN para ser más precisos, (Local Area Network – Redes de Área Local).

El desarrollo de las Redes de Área Local(LAN) a mediados de la década de 1980 ayudo a cambiar nuestra forma de pensar acerca de las computadoras, la forma en que se comunican entre ellas y él porque de ello.

Cada vez con mayor frecuencia microcomputadoras y mainframes o macrocomputadoras son parte integrante de las REDES de área local. Quizá el desarrollo más trascendental e importante de las REDES en la década de 1980 fue el reconocimiento que se hizo a los dispositivos controlados por computadora que son ahora los periféricos de la red y no la red un periférico de la computadora.

Las LAN o REDES de área local fueron inventadas teniendo en mente la *conectividad.*

Las Redes Locales pueden:

a) Servir a usuarios locales
b) Interconectarse
c) Ser nodos de una red global
d) Tener radios de acción que varían de algunos cientos de metros a cerca de 50 km.

Las redes globales se pueden extender por todo el mundo, de ser necesario.

Las LAN son un reconocimiento de la *necesidad* que tienen las personas de utilizar datos y, como un producto secundario de transmitir datos de una persona a otra.

1.2. NECESIDADES

La información siempre ha sido y será fundamental para la interacción de las diferentes labores del que hacer humano.

Las computadoras juegan en nuestro tiempo un papel determinante: de tal manera que en la medida que las empleamos resolvemos problemas que de otra manera hubieran tardado mucho más tiempo o simplemente no se hubieran resuelto.

Pero no todo es tan maravilloso y espléndido ya que al mismo tiempo que obtenemos información, surge la necesidad de compartirla para que ésta pueda ser aprovechada.

Las situaciones en las que se vuelve necesario compartir la información, puede resolverse regularmente manejando la información a través de medios de almacenamiento magnético (discos floppys, cintas magnéticas, etc.) pero existen procesos en los cuales es necesario guardar la integridad de la información mientras se comparte tales como:

a) Transacciones Bancarias
b) Reservaciones de Vuelos
c) Control de inventarios

Y más de una infinidad de ocasiones en que realmente se requiere de métodos para compartir, ya sea información o dispositivos.

También, en la medida que la tecnología crea dispositivos útiles para las labores, en la que nos vemos involucrados, surge la necesidad de compartirlos.

La Necesidad de una Red es imperiosa sí:

1. Se requiere compartir información actualizada, sea cual sea.
2. Se requiere compartir dispositivos periféricos, como impresoras, unidades de respaldo etc.
3. Existe información redundante.
4. Existen múltiples copias de la misma información, ya sean programas o datos.
5. Simplificar procesos sociales (comunicación).

Las necesidades básicas son:

a) Compartir información
b) Compartir dispositivos
c) Eficientar el trabajo en grupo
d) Controlar los procesos diarios
e) Maximizar labores
f) Disminuir los costos

Asimismo, las redes Lan son importantes para muchas organizaciones de menor tamaño, ya que son la ruta a seguir hacia en entorno de computación multiusuarios capaz de comenzar en forma modesta, pero también de extenderse a medida que aumentan las necesidades de *compartir información.*

En los próximos años muchos de los dispositivos de comunicaciones más nuevos, como los servicios de transmisión de voz y vídeo, distribución de imágenes y quizá teléfonos celulares, se convertirán en ingredientes importantes de las Redes de área local.

1.3. ROCESO DISTRIBUIDO Y CENTRALIZADO

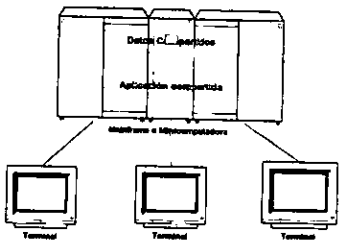
¿Qué hace una red de computadoras diferente de un *"mainframe"*, una microcomputadora o de una micro multiusuario? La respuesta simplemente es proceso distribuido en lugar de proceso centralizado.

Definición de Terminología

La terminología para describir las alternativas de proceso son por lo general similares y confusas. Por eso se harán unas breves definiciones.

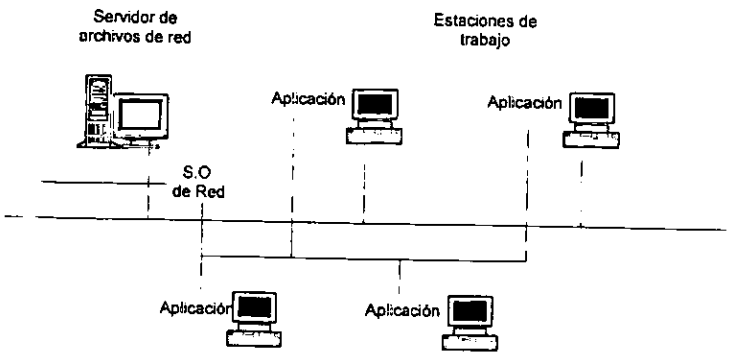
Proceso Centralizado

Se utiliza en los mainframes, minicomputadoras y micro multiusuario. Todos los usuarios comparten el poder de un procesador central y una sola copia del software de aplicación corre en el CPU central. Las terminales "tontas" enlazadas que necesiten usar la aplicación deben compartir la copia de dicho CPU.



Proceso Distribuido

El proceso distribuido ocurre cuando el procesamiento de la información se lleva a cabo en una forma descentralizada. En contraste con el proceso centralizado, que requiere que todo el procesamiento ocurra en forma central en una sola máquina, éste se distribuye entre las computadoras de la red. El proceso de información en máquinas PC's conectadas a una red es un ejemplo de proceso distribuido. Cada PC corre su propia copia del programa y el sistema operativo de red sincroniza el uso de recursos compartidos por las múltiples aplicaciones.



¿Porqué puede resultar el proceso distribuido más eficiente que el proceso centralizado?.

A un usuario de microcomputadoras esto puede sonarle muy familiar.

Hoy se tiene que correr la nómina de 400 empleados, proceso que toma unos 30 minutos, por lo que el resto de los usuarios del sistema, (dirección, ventas, administración general, contabilidad, etc.) que no tienen nada que ver con este proceso, pueden hacerse a la idea de que en los próximos 30 minutos el sistema de cómputo será inoperable, dada su baja velocidad de respuesta.

¿El motivo? Es tal el tiempo de procesador central que se requiere para procesar la nómina que la microcomputadora no tendrá tiempo de atender a tantos usuarios al mismo tiempo, degradándose sensiblemente la velocidad de respuesta de todo el sistema de computo.

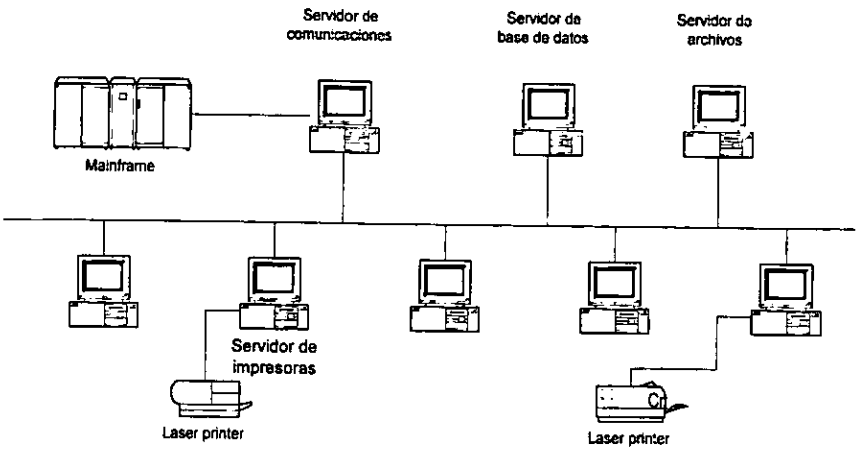
¿Qué es lo que ocurre en un ambiente de proceso distribuido (por ejemplo en una red)?

Todo el proceso se lleva a cabo en una de las computadoras de la red (la que corre la nómina). El resto de los usuarios no experimentaran efecto alguno en su velocidad de respuesta, ya que el procesador del servidor de archivos (file server), se encargará únicamente de administrar los niveles de seguridad de los usuarios y los accesos a disco, nunca del proceso de información, que es la tarea que más tiempo le quita a una computadora.

Si bien es cierto que los accesos a disco que hará la computadora que está corriendo la nómina, cargaran tareas al servidor de archivos; éstas no afectaran en forma sensible la velocidad del resto del sistema.

El proceso distribuido, especialmente en redes de computadoras donde el número de máquinas interconectadas en grande, hace que este proceso se lleve al punto llamado servicios distribuidos.

Los procesos distribuidos se llevan a cabo cuando existen varios servidores en la red y cada uno de ellos realiza tareas específicas. Algunos ejemplos de servicios distribuidos son los servidores de impresión, de comunicaciones (gateways), de base de datos, de administración de red, fax, correo electrónico, etc.



Hay ocasiones en las que se conjuntan varios de estos servicios en una sola de las computadoras de la red. Por ejemplo, si en una misma computadora se instala el sistema operativo de la red (servidor de archivos), el software de comunicaciones remoto (servidor de comunicaciones), el manejador de base de datos (servidor de base de datos) y muchas impresoras compartidas (servidor de impresión) se integran demasiadas tareas en un solo procesador y se caerá, en parte, en un proceso centralizado. A pesar de que el proceso de la información sigue siendo distribuido, el usuario de la red podría utilizar la base de datos y mandar a imprimir informes, por lo que sobrecargaría al servidor de archivos de tareas adicionales que pueden producir la degradación del sistema de computo.

En las redes pequeñas esto puede ser imperceptible, pero en redes de gran tamaño si se manifestaría tal degradación. En una red pequeña centralizada esos servicios es lo más económico y recomendable, lo mejor seria decentralizarlos hacia un verdadero proceso distribuido.

Una red de 40 o 50 nodos justifica el costo de dedicar PC's a tareas específicas, inclusive en redes más pequeñas, donde la velocidad de respuesta es uno de los elementos más importantes. Se justifican los servicios distribuidos.

1.4. EVALUACIÓN DE ALTERNATIVAS

Antes de escoger cuál de las alternativas se van a utilizar, el usuario debe tener en cuenta varios factores, tales como: rendimiento, confiabilidad, aplicaciones etc.

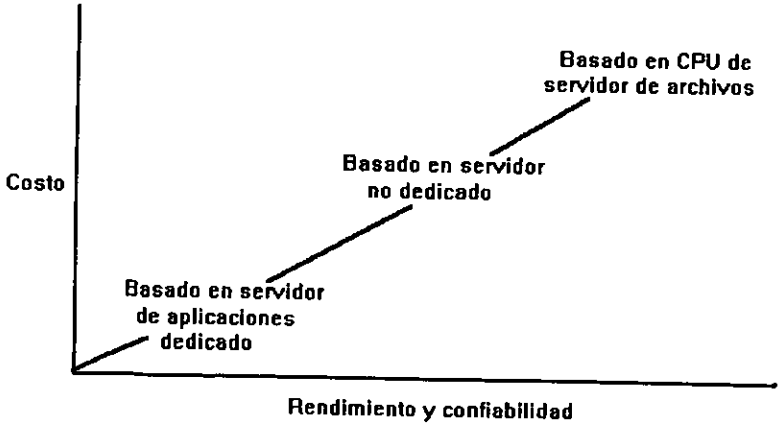
Los tres modelos principales que existen para evaluar alternativas son:

1. En el CPU del servidor de archivos. Esta es la alternativa más sencilla y económica, de hecho es la que utilizan la mayor parte de las instalaciones en México y en el mundo. Simplemente se instala la aplicación y los datos en el disco duro del servidor de archivos, donde los usuarios de DOS accesarán la información. Las aplicaciones deberán compartir los recursos del CPU con el sistema operativo de la red, lo que puede reducir el rendimiento de la aplicación y de la red.

2. En el servidor de archivos no dedicado. Esta es la solución intermedia en costo, rendimiento y confiabilidad. Consistente en utilizar un servidor no dedicado. Parte de la aplicación corre en el servidor de archivos en modo no dedicado y otra parte en la estación de trabajo. En esta opción, el procesador del CPU se comparte con el servidor de archivos.

3. La última alternativa es llevar la aplicación a una computadora diferente al servidor de archivos, convirtiéndose en una aplicación basada en servidor (de base de datos, de comunicaciones, de archivos). Esta es la alternativa que ofrece el mayor rendimiento y confiabilidad y, desde luego, el mayor costo.

En la siguiente figura se muestra la gráfica del costo contra el rendimiento de las tres alternativas.



1.8. DEFINICIÓN

¿Qué es una red?: En el campo de la computación se puede decir que una RED, es un conjunto de computadoras enlazadas entre sí y/o con otros equipos, cuya configuración permita que esto sea un medio para transmitir, recibir , compartir y manejar información.

1.9. CONCEPTOS BASICOS

¿Qué hace una RED?: una RED tiene como objetivo principal, compartir recursos fisicos (equipos y sus periféricos) y recursos lógicos (archivos de datos y programas), actualizándolos, organizándolos y explotándolos.

¿Por qué una RED?: porque la RED es la respuesta correcta a la necesidad de compartir entre usuarios los recursos más costosos de equipo y la información centralizada y/o dispersa de un organismo, obteniendo con esto la tan necesaria organización y economía en la informática.

Normalmente las microcomputadoras necesitan distintos recursos (periféricos) como son: impresoras, graficadores, discos duros, unidades de respaldo en cinta magnética, programas de aplicación, paquetería, etc. Que se tiene que adquirir a costos adicionales.

En una RED estos recursos en una sola micro se van a compartir con las demás, mediante un canal de comunicación que por lo general, es un cable dedicado a las comunicaciones. Las micros se conectan a este canal por medio de una interface, que es una tarjeta electrónica que se coloca en una de las ranuras de expansión de cada micro.

Las microcomputadoras que cuentan con los recursos periféricos reciben el nombre de servidores (SERVER) de la RED, que auxiliado por el sistema operativo de RED viene a ser virtualmente el "cerebro" dedicado a administrar los recursos y las comunicaciones entre las demás micros, mismas que trabajan así, reciben el nombre de ESTACIÓN DE TRABAJO.

1.7. COMPONENTES DE UNA RED LOCAL

Los componentes principales de una RED son:

1. Servidor

El servidor, que puede ser Dedicado o No Dedicado

- ❖ Dedicado, exclusivamente administra los recursos de la Red
- ❖ No dedicado, además de administrar los recursos de la Red, funciona como estación de trabajo

Las características y configuración de la computadora que sea disponible definir como server, están en función de los requerimientos del caso, generalmente se trata de un equipo robusto tanto en hardware como en software.

2. Estación de Trabajo

Están representadas por cada una de las microcomputadoras conectadas en Red.

En la RED, tanto el Server como las Estaciones de Trabajo, pueden ser PC's XT o AT's, equipos 386,486 o Pentium, los modelos PS/2 de IBM, sus Value Point, e inclusive microcomputadoras no compatibles como el caso de Macintosh.

En la actualidad se fabrica hardware ex profeso para REDES LOCALES como el caso de los Servidores y Estaciones de Trabajo de fábrica. En el mercado nacional podemos encontrar que todos los fabricantes de productos de marca como IBM, HP, COMPAQ, DIGITAL, ACER, etc., ofrecen productos de estas características.

3. Interface de RED

Dispositivo que permite la interconexión de los nodos de la RED. Debe instalarse en cada equipo que conformará la RED. Generalmente es una tarjeta que va instalada dentro de cada computadora que se conectará a una RED, de ahí que se le denomine inadecuadamente Tarjeta de RED. En la actualidad las interfaces de RED también se pueden conectar a un puerto (Paralelo, Serial, PCMCIA, etc.) del nodo de la RED.

Según su especificación y normas, cada interface de RED determina los protocolos de comunicación y la forma de interconexión (TOPOLOGIA) de cada RED. Existen tres estándares de interfaces de RED que dominan el mercado a nivel internacional:

- ARCNET: Que tiene una relación costo-beneficio favorable, con un sistema de cableado sencillo de amplio rango.

- ETHERNET: La de uso mas generalizado por su alto rendimiento y facilidad de interconexión de equipos heterogéneos.

- TOKEN-RING: Muy costosa, pero con el respaldo técnico y promocional de IBM, esta tarjeta puede conectar toda la línea de equipos IBM, desde una PC hasta un 309X ó 93XX en una sola RED de este tipo.

4.- Canal de Comunicación

Es el medio físico por el cual se comunican los nodos de una RED. Por lo general es un cable dedicado a las comunicaciones, mismo que puede ser:

a) De tipo telefónico
b) De par roscado (Twister Pair)
c) Coaxial
   -Broadband : Lento, varios canales
   -BaseBand : Rápido un canal
d) Fibra Optica: Más rápido y varios canales

Este canal de comunicación determina la velocidad máxima de transferencia de información que van desde 2.5 Mb/s hasta 100 Mb/s, dependiendo del tipo que se utilice.

Actualmente se están desarrollando nuevas tecnologías para que el medio de comunicación sea inalámbrico.

A partir de 1990 se comercializan interfaces de RED inalámbricas, con tecnologías de radio frecuencias, microondas, rayo láser, etc.

5.- Repetidores

Elementos que permiten incrementar las distancias del medio de comunicación, reforzando su señal sin importar la topología; pueden ser tarjetas internas o cajas externas. Se dividen en activos y pasivos.

6.- Sistemas de Cableado

Cuya forma de conexión entre equipos (TOPOLOGIA), está en función de la interface de red que se haya seleccionado.

7.- Cajas y elementos de Conexión

Son los elementos adicionales de conectarización, los cuales dependen del tipo de sistemas de cableado que se utilice.

8.- Sistema Operativo de RED

Es el software que se instala en el servidor de la RED, permitiendo la compartición de recursos y el control y administración de la información de la RED.

Los principales sistemas operativos de RED en el mercado internacional, son:

- NETWARE de Novell. En diferentes versiones.
- LAN MANAGER de Microsoft
- Windows NT y Windows para grupos de trabajo de Microsoft
- Lantastic
- Todos los NETBIOS compatibles.
- IBM LAN SERVER
- VINESS
- NETWORK
- QNX de quantum Software System Ltd
- TAPESTRY

9.- Software de Aplicación

Son las aplicaciones disponibles en la RED, para los usuarios. Las más importantes son:

- Suites de Productividad Personal. (Procesadores de Texto, Hojas de Cálculo, Manejadores de Archivos, Presentaciones, etc.)
- Manejadores de Bases de Datos.
- Correo Electrónico

1.8. NODOS

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. Se puede establecer que un nodo es un elemento conectado directamente a la RED mediante su interface correspondiente.

1.9. BANDA ANCHA Y BANDA BASE

Las señales de comunicación, que el hombre utiliza gracias a la tecnología moderna van desde transmisiones televisivas, de radio, de datos, etc. Todas estas comunicaciones respecto al aprovechamiento del medio de comunicación, se pueden dividir en dos grandes grupos.

Comunicaciones

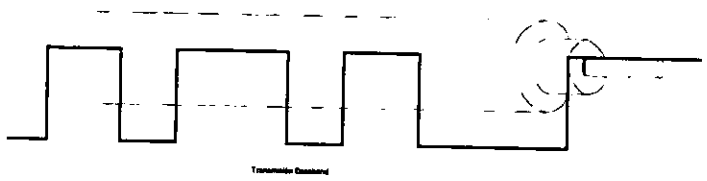
- Banda Ancha
- Banda Base

Por lo tanto en el mercado de las redes y comunicaciones de computadoras es aplicable hablar de redes de Banda Ancha (Broadband) y redes de Banda Base (Baseband).

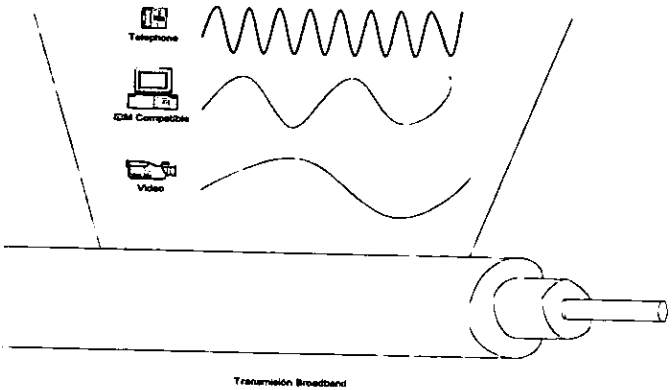
La diferencia entre redes de banda ancha y redes de banda base, radica solamente en la forma en que se transmite las señales por el canal de comunicación.

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 pulsos (discontinuos) directamente sobre el medio físico, aplicando dos niveles de voltaje diferenciados, cuyas transmisiones 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 en muy simple y debajo costo, sin embargo en redes donde se usa la modulación es necesario incluir en la interfaz un módem 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 solo 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 en canal para la recepción y otro para la transmisión, esto se puede lograr de dos formas:

1.- Dividiendo el ancho de banda de un solo cable, o bien.

2.- Usando un cable para la transmisión y otro para la recepción.

En caso de usar un solo cable, el ancho de banda necesario es el doble que si se usa 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 módem que , conectado a cada nodo se encarga de convertir las señales.

El módem 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 tratamiento integral de la información incluyendo en un mismo medio los datos, la voz y las imágenes.

Las interfaces de Red estándares tradicionales, ArcNet, Ethernet y Token-Ring, su método de comunicación es en banda base. Pero la tecnología moderna nos brinda ya comunicaciones en banda ancha para el establecimiento de redes locales, estas nuevas tecnologías de donde saldrán los nuevos estándares son:

- Frame Relay
- ATM
- Fast Packket Switching
- RDSI

Más adelante se ampliara la información sobre estas tecnologías.

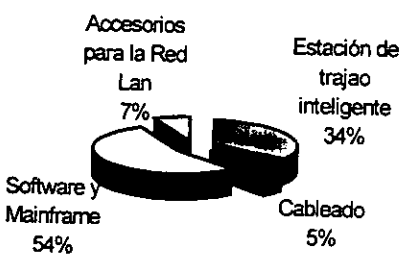
Transmisión	Multiplexaje	No. de Canales	Costo	Distancia
Baseband	TDM	UNO	$	1000's of feet
Broadband	FDM	Múltiples	$$$$	Miles

1.10. MEDIO DE COMUNICACIÓN

Según estudios realizados, de los costos totales de inversión en una RED local, establecer el medio de comunicación representa solo el 5% del costo total (en coso de medios alámbricos) y contrastemente el medio de comunicación origina mas del 70% de las fallas en una RED local.

Tiempo Improductivo en Redes LAN

Costo de inversión de la Red



Por lo anterior es fundamental darle el debido valor a la instalación del medio de comunicación, utilizando técnicas modernas como el cableado estructurado, cableado redundante, el establecimiento del backbones, etc.

La interconexión de los nodos en una red local se realiza usando medios físicos muy diversos.

Los principales medios de comunicación dentro del mercado:

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 sin blindaje (Unshielded Twisted Pair STP), éste consiste en una capa del 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 al 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.

Clasificaciones del cable Twisted-Pair

AMP	REFERENCIA	APLICACIONES
	EIA/TIA Categoría 1	Correo Voz Digital Voz Analógica
	EIA/TIA Categoría 2	ISDN (DATOS) 1.44 Mbps TI:1.544 Mbps Voz Digital IBM 3270 IBM SYSTEM/3X AS/400
100 Ohms	EIA/TIA Categoría 3[1] NEMA 100-24-SDT UL NIVEL III	10 BASE – T 4Mbps Token Ring IBM 3270, 3X, AS/400 ISDN VOZ
100 Ohms BAJAS PERDIDAS	EIT/TIA Categoría 4 NEMA 100-24-LL UL NIVEL IV	10 BASE – T 16 Mbps Token Ring
100 Ohms FRECUENCIA EXTENDIDA	EIA/TIA Categoría 5 NEMA 100-24-XF UL NIVEL V	10 BASE – T 16 Mbps Token Ring 100 Mbps DDI[2]
150 Ohms STP	EIA/TIA 150 Ohm STP NEMA 150-22-LL	16 Mbps Token Ring 100 Mbps DDI VIDEO EN MOVIMIENTO

[1] Igual que el cable UTP horizontal a 100 Ohms EIA/TIA - 568
[2] Propuesto

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 las especificaciones de este tipo de red y existen dos tipos:

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

  -Thick Ethernet.- RG-11, distancia máxima por segmento 600m impedancia de 58.5 ohms.

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

Fibra Optica

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

Este tipo de medio, 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.

Cuadro Comparativo de Atenuación

Cable	Longitud de Onda o Frecuencia	Atenuación (db/km)
Coaxial	100Mhz	61
F.O. MM[3]	850 Nm	2.4 – 3.2
F.O. MM	1300 Nm	1.0 – 1.5
F.O. UM[4]	1300 Nm	Menor a 0.5
F.O. UM	1550 Nm	Menor a 0.25

Señales Radioelectricas

Este medio se basa en 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 radioelectrica de 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.

Para la elección del medio de comunicación adecuado se deben de considerar principalmente los siguientes aspectos:

- Cubrir el ancho de banda necesario
- Cubrir las velocidades requeridas
- Cubrir las distancias requeridas
- Adaptación al entorno fisico-geografico
- Minimizar posibilidades de fallas
- Posibilidades de crecimiento y modularidad
- Minimizar costos de instalación y mantenimiento

[3] Fibra óptica Multimodales
[4] Fibra óptica Unimodales

Cable	Costo	Velocidad de Transmisión de Datos	Susceptibilidad a Interferencias	Distancia Típica
Coaxial	$$$	10 Mbps	Regular	100's – 1000's of feet
Unshielded Twisted – Pair	$	1 –10 Mbps	Pobre	100's of feet
Shielded Twisted – Pair	$$	1 – 100 Mps	Bueno	100's of feet
Fibra Optica	$$$$	100 Mps	Excelente	1000's of feet to miles

Estimación de LAN's instaladas en el mundo

Tipo de Medio	1992	1993	1994	1995	1996
COAX- Grueso	21.5%	20.1%	18.6%	17.1%	15.5%
COAX- Delgado	13.3%	12.8%	12.1%	10.5%	8.7%
COAX - Banda Ancha	4.2%	4.0%	3.8%	3.5%	3.0%
Fibra óptica	5.9%	6.2%	6.6%	7.1%	7.6%
STP	28.7%	26.5%	23.6%	21.1%	18.0%
UTP	23.7%	28.8%	32.4%	36.5%	41.1%
Sin Cable	0.7%	1.6%	2.9%	4.2%	6.1%

1.11. CARACTERÍSTICAS DE LAS REDES DE ÁREA LOCAL

A nivel resumen, de lo anteriormente expuesto, puede deducirse que las características más significativas de las redes de área local son:

Area Moderada

El espacio fisico que abarca una RED local suele estar limitado a un edificio o conjunto de estos, pudiendo variar la distancia máxima entre sus nodos desde una decena de metros hasta varios kilómetros.

Canal Dedicado

El medio fisico (canal) está exclusivamente dedicado a la comunicación que se produce entre las distintas estaciones de la RED local. Existen medios alámbricos e inalámbricos para establecer el canal de comunicación.

Baja tasa de errores

Debido a las características de especial dedicación del medio y las distancias relativamente cortas en que se produce la comunicación, los errores serán escasos y fácilmente corregibles. En las redes locales industriales la fiabilidad de la transmisión de la información será un factor decisivo para garantizar la calidad de funcionamiento (ver recomendación 6.821 del CCITT y M1020).

Costo reducido

Uno de los principales objetivos que se barajan al planificar una RED local es el costo de la conexión entre los distintos sistemas informáticos sea notablemente inferior al precio del sistema informático propiamente dicho.

Modularidad

Las redes locales deberán ser muy flexibles, tanto para la incorporación de nuevos elementos como para su supresión. La razón estriba en que el entorno de aplicación de las redes locales suele ser muy cambiante.

Posibilidad de interconexión de equipos heterogéneos

Con frecuencia, en una oficina o planta de fabricación, debido fundamentalmente a la rapidez con que quedan obsoletos muchos equipos, esto suelen proceder de una amplia gama de proveedores, siendo necesario que la RED local sea capaz de solucionar el problema de interconexión de todos ellos. Esta característica está directamente relacionada con la necesidad de normalización.

CAPITULO 2. ARQUITECTURA DE REDES, TOPOLOGÍAS Y PROTOCOLOS

Compartir recursos y protegerlos son objetivos contradictorios. Los sistemas y programas pueden ser aislados completamente si se separan en computadoras diferentes, pero se evita que se compartan. De igual forma, programas que se encuentran en una red pueden ser compartidos por varios usuarios al mismo tiempo, pero esto acarrea problemas de seguridad. Normalmente interesa que una cantidad apropiada de información sea compartida entre los usuarios, pero no más de lo necesario. En una red, debe existir un mecanismo para evitar el acceso a personas no autorizada a la red o a ciertos archivos dentro de esta.

El nivel de seguridad que debe ser provisto en una red depende directamente del valor de los recursos que se desean asegurar. La información contenida en una red bancaria puede ser importante para algunas personas, pero inútil para otras. Un grupo de archivos específicos del sistema operativo deben ser vistos únicamente por el administrador del sistema y no por el usuario en particular. Un archivo personal de un usuario debe ser visto sólo por esa persona y nadie más.

2.1. REQUERIMIENTOS DE SEGURIDAD

Existen varios documentos que definen lo que es un "sistema seguro". Estos documentos no son más que un grupo de normas que indican los requerimientos de seguridad que debe poseer un sistema. La mayoría de estos documentos provienen de los cuerpos de defensa de los Estados Unidos de América, entre los más importantes destacan: La directiva DoD 5200.28, la cual especifica como debe ser manejada la información de los sistemas de procesamiento de datos y el Acto de Privacidad de 1.974, el cual requiere que las agencias federales norteamericanas aseguren la integridad y seguridad de la información de personas, esto debido al extenso uso que se hacen estas agencias de las computadoras.

El libro Naranja y el Libro Rojo son publicaciones del Ministerio de Defensa (DoD) de los Estados Unidos, y han servido como el estándar para la seguridad en redes de computadoras. Los sobrenombres provienen del color de las portadas de estos documentos.

El libro Naranja realmente se llama Trusted Computer System Evaluation Criteria (o el Estándar DoD85), lo que en castellano quiere decir Criterios para la Evaluación de Sistemas Confiables de Computación. Estos estándares fueron aplicados posteriormente a las redes y publicados en un documento que es el conocido Libro Rojo.

De acuerdo a estos documentos, se definen siete clasificaciones de seguridad para computadoras o redes. Estas clasificaciones definen progresivamente sistemas más seguros, donde tenemos que una computadora ejecutando sistema operativo DOS es considerado como un sistema clase D, debido a que posee protección mínima.

El proceso para certificar a un sistema de seguridad es largo y costoso, además debe ser conducido y supervisado por una agencia del gobierno de los Estados Unidos. Los sistemas operativos de redes más populares (ejemplo: Novell Netware y Windows NT Server) tienen un nivel de clasificación D (protección mínima) cuando son instalados por primera vez porque las funciones de seguridad no han sido activadas todavía. Posteriormente, una red debidamente configurada puede llegar hasta categoría C, donde el acceso a la misma es controlado.

Seguridad Total

Existen dos tipos de seguridad con respecto al acceso a redes de computadoras: Seguridad Externa y Seguridad Interna.

La seguridad externa se encarga de proteger y controlar el acceso a una instalación de computadoras de intruso y/o desastres tales como incendios e inundaciones. Los centros de computación de muchas empresas, sobre todo las grandes corporaciones, no permiten el acceso a la sala de computación sino a un pequeño grupo de personas. Por lo general estas instalaciones están resguardadas con puertas especiales que solo abren con una clave o al deslizar una tarjeta. Empresas más pequeñas colocan el servidor en un sitio seguro y lejos del alcance de la mayoría de los usuarios.

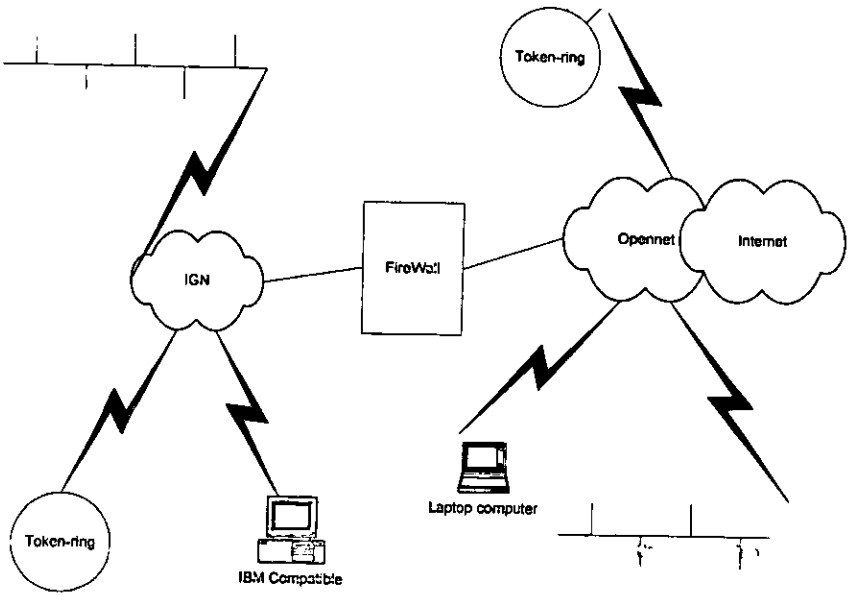
Una vez que el usuario tenga acceso físico a la computadora, entonces un sistema de identificación provisto por la red es el encargado de permitir el acceso al usuario. La seguridad interna no es más que una serie de controles diferentes a nivel de hardware y software encargados de garantizar la operación confiable de la red y velar por la integridad de los programas y los datos.

Muros de Seguridad

Estrictamente hablando un muro de seguridad puede ser definido como una colección de componentes que se colocan entre dos redes. Las siguientes

propiedades se cumplen: todo él tráfico en cualquier dirección debe pasar a través del muro de seguridad, únicamente al tráfico autorizado por las políticas locales de seguridad se le permitirá el paso y el muro de seguridad por si mismo es inmune a penetración.

A nivel de red encontramos esta tendencia de seguridad, los firewalls, que de una u otra forma necesitan una modificación de la infraestructura de Internet en la organización que se desea proteger. En términos generales este mecanismo de seguridad permite proveer un cierto grado de aislamiento entre dos redes; además, cuando se elige el muro de seguridad apropiado, se configura y se mantiene correctamente, puede proveer un determinado nivel de seguridad. Más específicamente y en teoría el fireWall sencillamente bloquea o restringe cierto tipo de comunicaciones no autorizadas entre computadoras en la organización y computadoras en las organizaciones externas. Para ver con mayor claridad el funcionamiento práctico de los muros de seguridad miremos una clase de muro de seguridad que existe, el de la compañía IBM.



IGN. Red Global IBM

2.2. MODELO DE REFERENCIA ISO – OSI

Las tecnologías que el hombre ha inventado, para comunicarse, siempre han seguido ciertas normas o reglas para su aceptación en un grupo social que puede ir desde una pequeña comunidad hasta todo una gran sociedad. En la época moderna las normas que rigen a las comunicaciones deben tener carácter universal. Hablando de comunicaciones digitales las normas o reglas universales están representadas por el modelo ISO – OSI[1].

El modelo OSI 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 encuadrase 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, ISA[2] u OSI se han convertido en una referencia obligada para todo lo relacionado con la intercomunicación de computadoras.

Estructura General del Modelo

Desde el punto de vista 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 esta 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 especificas de la maquina. Es decir, esta pensada para la interconexión de sistemas heterogéneos.

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

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

[1] International Estándar Organization – Open System Interconection
[2] Siglas en español

Las características del modelo podrían resumirse de la siguiente forma:

- Cada nivel estará representado por una entidad de niveles. Los niveles equivalentes en dos sistemas diferentes se comunican dé 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 él, 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 homologo en otro sistema informático, se la pasara al nivel inmediatamente inferior, el cual le añadirá información delimitadora propia y a su vez pasara esta información a su nivel inmediatamente inferior.

En el sistema receptor cada nivel separara la parte del mensaje que le corresponde y pasara 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 homologo 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 transición.

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: APLICACIÓN

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 originado y el receptor tuvieran versiones de datos sintáticamente 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 cambio de comunicación entre dos procesos del nivel de aplicación. Este nivel establece una sesión y se encarga de controlar la comunicación y sincronizar él dialogo.

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 que 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 validado.

En una sesión hay dialogo entre máquinas, entre procesos y el protocolo debe regular quien "habla", cuando y por cuánto tiempo.

Estas reglas necesitan ser acordadas cuando la sesión comienza. Este nivel también es responsable de dirigir él dialogo entre 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 la 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 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 HDLC[3] como protocolo del nivel de enlace.

NIVEL UNO: FÍSICO

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

Es muy importante recalcar que el modelo ISO – OSI es un estándar universal, pero más que un estándar tecnológico, representa un marco de referencia. Esto es, la mayoría de los fabricantes de hardware y software sus productos no cumplen con las funciones y límites de cada nivel, pero compararan sus productos con los niveles del modelo, argumentando sus ventajas y funciones respecto al modelo.

El modelo ISO – OSI, proporciona un lenguaje universal entre los especialistas del medio de la interconexión de equipo de cómputo, para que hablen un "mismo idioma" y puedan comparar cualquier producto o tecnología respecto a dicho modelo,

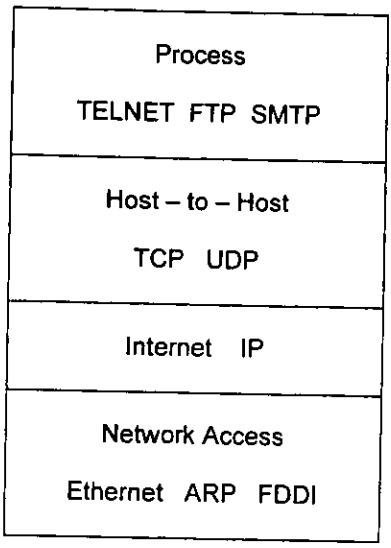
Los grandes centros de investigación de la industria están trabajando fuertemente para lograr una tecnología comercial que se apegue estrictamente al modelo, dicha tecnología es reconocida como OSI, pero en la actualidad no deja de ser un interesante proyecto, ya que la parte comercial tiene sus ojos puestos en tecnologías ya ampliamente probadas como TCP/IP y las nuevas tecnologías que manejan un gran ancho de banda como ATM, FAME-RALAY, etc.

[3] High Level Data Link Control

2.3. MODELO DoD (Cuatro – capas)

El Departamento de Defensa de los Estados Unidos de América creo en los años 70's, bajo el proyecto DARPA, el modelo DoD[4] cuatro capas basado en el modelo OSI de siete niveles.

Modelo DoD



Las cuatro capas del modelo DoD, de abajo hacia arriba, son:

1) La capa Network Access. Esta es responsable de entregar los datos atravez del hardware, ocupando diferentes protocolos para esta capa, dependiendo del tipo de red física que se tenga.
2) La capa Internet. Esta es responsable de entregar los datos a través de varias redes físicas que conectan a una máquina origen con una máquina destino. Los protocolos de ruteo son los más asociados con esta capa, como lo son: el protocolo IP.
3) La capa Host – to – Host. Maneja una conexión programada, el control de datos, la retransmisión de datos perdidos y manejadores de datos genéricos. El TCP y el UDP son los protocolos más importantes de esta capa.

[4] Departamento de defensa

4) La capa de Process. Esta capa contiene los protocolos a nivel de usuario, tales como: Correo electrónico, transferencia de archivos y acceso remoto.

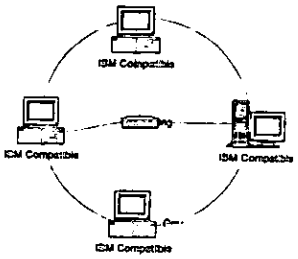
2.4. TOPOLOGÍAS

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 debe de considerar dos tipos:

- Física
- Lógica

La topología física se determina por la disposición de los elementos conectados a la red.



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; por ejemplo, se puede implementar un anillo lógico en una estrella física. El protocolo de comunicación es una RED es determinante para su rendimiento, para el análisis de éste no importará cual sea la topología física.

En el mercado actual existe una gran variedad de topologías físicas, la única forma de poder analizar todas ellas, es considerando primero su topología lógica y posteriormente entender como se estructura o conforma su topología física sobre la base de los elementos de conectividad.

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.

Los factores de análisis que se deben considerar para la elección de la topología son:

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

En el mercado actual existe una gran variedad de Topologías Físicas, para entender como funcionan todas estas, es importante conocer como funcionan lógica y físicamente los tipos básicos antes mencionados, con base en esto, entender las características que cualquier topología en el mercado pueda ofrecer.

Configuración en Estrella.

Antes que nada cabe mencionar que la topología de estrella lógica, no es un estándar, se origina o deriva de los métodos de comunicación utilizados en los equipos multiusuario tradicionales. El protocolo del que hace uso es el polling o poleo.

En una red de 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 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 recuperación en el comportamiento global de la red al presentarse una falla en uno de los nodos periféricos es muy baja y solo afectaría al trafico 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.

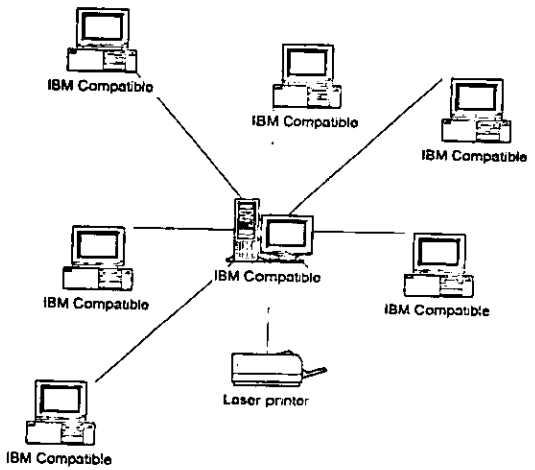
En el caso de que las comunicaciones se produzcan entre las estaciones, el sistema se vería restringido por la posible congestión del dispositivo central.

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

Por lo general, esta topología no es adoptada por las redes locales más importantes y no ha sido incluida dentro de las configuraciones normalizadas por la IEEE. No obstante, es de interés debido al auge que para las comunicaciones 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.

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 BUS

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

En las redes con esta configuración, a deferencia 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 de 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.

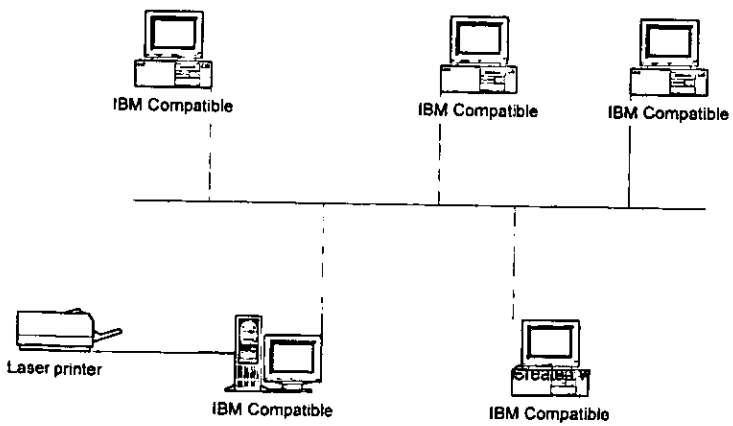
Las redes en esta configuración son sencillas de instalar y pueden tener dificultades para adaptarse a las características del terreno local.

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 dejara 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 términos técnicos es un anillo lógico.



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

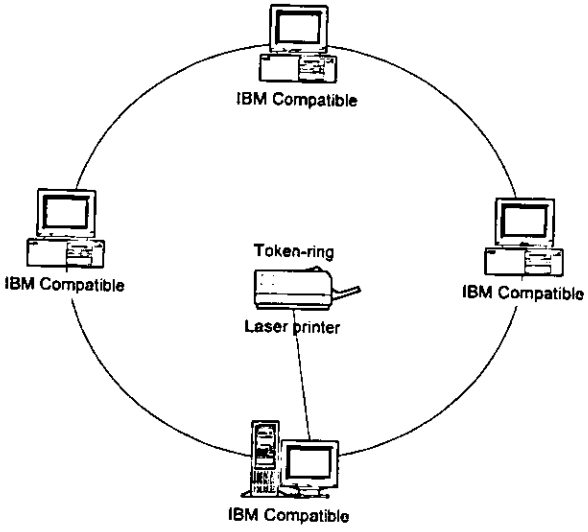
Una manera de evitar estos riesgos consiste en el uso de concentradores.

El concentrador es un dispositivo, fabricado con alta confiabilidad, al que se conectan las estaciones de trabajo de 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, restableciéndose el anillo.

A simple vista, la topología física parecerá de estrella, más la topología lógica continúa siendo de anillo. El protocolo de comunicación es Token Passing

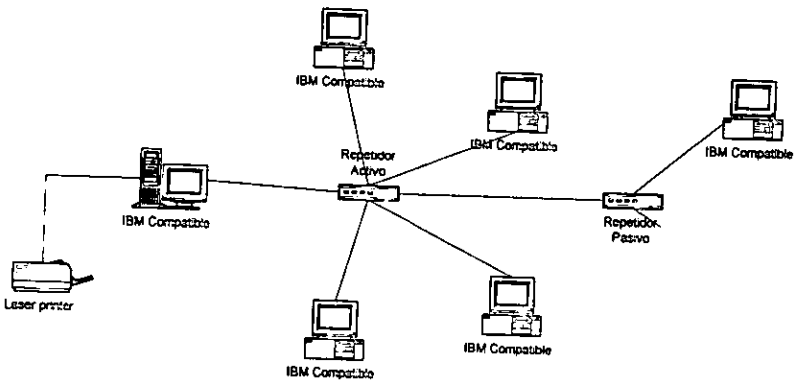
El concentrador acepta un número limitado de estaciones de trabajo, por lo que en caso de necesitar añadir alguna otra estación una vez agotado el espacio disponible para la conexión, se puede recurrir a conectar varios concentradores para ampliar la red. En el ámbito comercial, a estos concentradores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



TOPOLOGIA ÁRBOL

Desde el punto de vista físico, esta conexión como se dijo anteriormente, es combinada y es una opción más para implementar REDES, según las necesidades del usuario.

Trabaja el protocolo TOKEN PASSING, tarjeta ARCNET y repetidores tanto PASIVOS como ACTIVOS.



2.5. PROTOCOLOS

ETHERNET

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

La parte del estándar que entra en el estrato de enlace de datos consta del subestrato de control de acceso al medio y del control del enlace lógico, en lugar de compensar un protocolo de transmisión de datos completo.

Los servicios MAC[5] para Ethernet incluyen CSMA/CD[6] y el formato de frame básico. Existe flexibilidad en el formato de frames, en particular con respecto a las direcciones fuente y destino que pueden tener 16 ó 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 lógica	Bus
Topología Física:	Bus Estrella (Utilizando HUBS)
Medio de Comunicación	Cable coaxial grueso o delgado Cable UTP
Medio de transmisión	Banda Base
Método de acceso	CSMA/CD
Número máximo de nodos	1024
Velocidad máxima de transmisión	10 Mbps

Esta red constituye la especificación de los 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 activos entre dos nodos y libre de errores.

[5] Media Acces Control
[6] Carrier Sence Multiple Access / Coltion Detection

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 adopten a los niveles superiores.

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 transductores) 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 cuando otro esta 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 limites 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.

El controlador o interface de red, 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 la acción de interfaz con la conexión de la misma.

Actualmente, pueden encontrarse en el mercado circuitos integrados VSLI 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 interactuan 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 cuando usa como medio de transmisión el cable coaxial grueso (RG-11) el modo de transmisión es en banda base, lo que provoca la existencia de ciertas limitaciones en cuanto a la distancia máxima. La configuración estándar 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 estándar Ethernet soporta una opción más barata, denominada Thin Wire (cable delgado), que con un cable de inferior de calidad (RG-58) y con conexiones más sencillas puede lograr una cobertura máxima de 300 m. Actualmente la mayoría de las implementaciones Ethernet utilizan UTP como medio de comunicación, por la versatilidad en el cableado que ofrece.

Para la necesidad de una cobertura mayor, hay una oferta denominada Broadband. 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 módem especial llamado DECOM, y este a su vez, va conectado directamente al cable común. DECOM puede ser usado en los dos tipos de redes de banda ancha, simple o doble cable.

En las configuraciones de banda base, la conexión es completamente distinta en las redes estándar que en las Thin Wire. En el primer caso, la conexión del controlador de comunicaciones al cableado coaxial se hace por medio de un transeptor de comunicaciones al cable coaxial se hace por medio de un transeptor, como ya se vio. 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 unidos 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 transeptor por un cable de cuatro partes de hilos cruzados. Este cable tiene una longitud máxima de .50m.

TOKEN-RING

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

Comúnmente, las estaciones de trabajo se conectan con par trenzado blindado o no blindado, 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 de 72 estaciones que usaban cable UTP especial de IBM. Más tarde en 1989, se extendió hasta 16 Mb/s. Cuando se usa par trenzado blindado (STP) se puede 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 las versión de 16 Mb/s se requiere cable dúplex trenzado aislado, lo que eleva aún más los costos de instalación.

Características

Topología	Configuración de anillo
Medio físico	Cable par trenzado (UTP o STP)
Modo de transmisión	Banda Base
Método de acceso	Token Passing
Numero 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:

1. Token
2. 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 perdida. 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 las 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 la 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 campo FS. La trama continuará circulando hasta alcanzar de nuevo al emisor, el cual la retirara y emitirá otra vez el token.

Si durante el viaje de la trama de datos, ésta pasa por alguna estación que contenga 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 analizara 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 el 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 reinsertara 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, restableciendo 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, tienen 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 unidad 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 que la que existe un solo anillo, como se dijo anteriormente se pueden conectar en cascada varios MAU's, con lo que resulta un anillo de mayor número de estaciones.

La solución se basa en conectar dos o más MAU's, usando una toma de cada uno para conectarse al otro. Debido a que el número de estaciones está limitado en el anillo y 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 el Bridge pasarán los dos.

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 AECNET es anterior a la aparición de estándares de bus de señales, las 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 el bus de señales que se desarrollaron antes de la promulgación del estándar 802.4 de la IEEE. Y no es un estándar.

Control de Acceso al Medio de Comunicación

La forma en que las estaciones de la red accesan al uso del canal común de comunicación para depositar y recoger datos y 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 normalización[7] se han inclinado por adoptar sólo un número reducido de métodos de control de acceso, razón por la que solamente se comentarán des técnicas:

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

Técnica 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:

- Token Passing "token" en anillo (token ring)
- Token Passing en "bus" (token bus)

Token Passing "token" en anillo (token ring)

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

[7] Usualmente son IEEE y CCITT

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.

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 sea enviado el testigo o "token".

La estación que envío el mensaje, antes de poner en circulación al testigo, analiza la partición de reserva que fue anotada durante la circulación del mensaje y marca el testigo para que le sea entregada 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 monitora de proceso.

Token Passing en "bus"

El principio de fundamento es muy similar al anterior, como 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 o elimina alguna ya existente, obliga a reestructurar las direcciones de estacionamiento de las estaciones afectadas.

La información transmitidas por una estación es difundida por todo el bus, lo que hace posible que algunas estaciones pueden 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:

- 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 puede acortar 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 periodo 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.

Técnica de Contienda

La técnica de contienda o CSMA/CD[8] parte de la base de que, cuando una estación tenga que transmitir, deberá intentar competir con las restantes en el uso del canal.

[8] Acceso múltiple con detección de portadora

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

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

La estación segura 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 esta 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 perdida de tiempo ocasionada por los mecanismos antes mencionados, surge una mejora al método (es cuando se denomina CSMA/CD).

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. El trabajo conjunto con Digital, Xerox e Intel en el desarrollo de la red local Ethernet, en la que se uso 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.

2.6. 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.

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 expansión, permitiendo añadir en un futuro nuevos equipos y nuevos protocolos a la configuración existente.

Se citan algunos de los organismos encargados de la normalización:

ISO

Es una organización Internacional de Normalización, que presenta entre otras, el modelo de referencia OSI.

CCIT

Es un Comité Consultivo Internacional Telegráfico y Telefónico, este es un organismo de gran influencia en el entorno de las comunicaciones. Su recomendación para 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 ANSI[9] también ECMA[10] han puesto sus recomendaciones en concordancia con las de la IEEE.

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.

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).

[9] American National Estándar Institute
[10] European Computer Manufacturers Association

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 éste 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 es dos subniveles denominados control de enlace lógico[11] y control de acceso al medio[12].

El primero de ellos es común para redes locales, mientras que el segundo es especifico 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 este 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 esta 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.

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.

[11] Las siglas son LLC
[12] Las siglas son MAC

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 en 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 la red local, este nivel se comporta como un protocolo end-to-end, es decir, relaciona dos puntos de esta sin ayuda de intermediarios, siempre desde el 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 complicada por el subnivel superior del nivel dos.

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

La norma provee 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 secuencia.

La clase dos proporciona un servicio orientado a la conexión que soporta la secuencia 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 Mbps 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 costo 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 o 20 Mbps. 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 que existen múltiples versiones en cuanto a formato de tramas, existencia o no de prioridades, etc. La norma 802.5 regula una de estas 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 recomendación802.5 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.

Se pueden resumir las normas del comité 802 de la IEEE en una familia de estándares que esta orientada a las dos primeras capas del modelo OSI:

- **802.1**. - Que especifica la relación de los estándares IEEE y su interacción con el modelo OSI de la ISO, así como cuestiones de interconectividad y administración de redes.

- **802.2**.- Control lógico de enlace (LLC), que ofrece servicios de conexión lógica a nivel de capa 2.

- **802.3**.- Red de topología de "bus" lineal, con el método de acceso al medio CSMA/CD con raíces que se remontan hasta 1975, su primera edición es en 1985. Cuenta con varios adéndums, que ofrece variantes en el medio de transmisión como 10BaseT. Un nuevo adéndum define a Fast Ethernet de 100 Mbps, usando el mismo protocolo de CSMA/CD , que para la capa física propone el esquema usado por ANSI en FDDI, pero en su versión usando cable de cobre de par torcido (CDDI).

- **802.4**.- Define una red de topología usando el método de acceso al medio de Token Passing (paso de señal) que fue usado en procesos automáticos de manufactura (MAP[13]), para controlar robots en una línea de ensamble. Su primera edición es de 1985.

- **802.5**.- Red de topología no definida (tampoco definía el medio de transmisión), pero que usa el método de Token Passing para accesar el medio de comunicación edición de 1985. De está especificación, se desarrollo el IBM Token Ring que actualmente se usa. Mientras que un estándar de la industria fue adoptado como estándar oficial, en el caso de Ethernet 802.3 (Fueron adoptados los trabajos de Ethernet II, un estándar oficial fue modificado para crear uno de la industria el IBM Token Ring).

- **802.6**.- Red de área metropolitana (MAN), basada en la topología propuesta por la University of Western Australian, conocida como DQDB (Distribuited Queue Dual Bus; Canal Dual de cola distribuida). DQDB utiliza un bus de fibra óptica como medio de transmisión. Ambos buses son unidireccionables, y en contrasentido. Con esta tecnología el ancho de banda es distribuido entre los usuarios, deacuerdo a la demanda que exista, en procesos conocidos como "inserción de ranuras temporales". Puesto que puede llevar transmisión de datos síncronos y asíncronos, soporta aplicaciones de vídeo, voz y datos, IEEE 802.6 con su DQDB, es la alternativa de la IEEE para ISDN.

- **802.7 y 802.8**.- Son comités creados para apoyar y supervisar los desarrollos de tecnologías existentes, que pueden migrar hacia fibra óptica o tecnologías en banda ancha (broadband), que utiliza señales análogas y no digitales como los especificados anteriormente.

- **802.9**.- Se enfoca en arquitecturas e interfaces estándares que permitan aplicaciones de escritorio con servicios integrados de voz, video y datos. También se ha anunciado que este estándar sería compatible con ISDN (se tenía entendido que su ratificación se haría entre 1992 y 1993).

[13] Manufacturing Automation Protocol

- **802.10.**- Este grupo desarrolla estándares concernientes a seguridad en una red de área local, que incluyen mecanismos de seguridad en la transferencia de datos, administración y procesos de seguridad compatibles con el modelo OSI.

- **802.11.**- Redes inalámbricas (Wireless LAN's) que especifica un sistema de red de área local por medio de radiofrecuencias. Este estándar no ha sido ratificado, y el estándar de la industria norteamericana que persigue crear redes de área local o amplia, el CDMA (Code Divition Multiple Access; División Código de Acceso Múltiple), que pretende utilizar telefonia celular para transmisión digital.

- **802.12.**- Se prevé la posibilidad de que el Fast Ethernet, adéndum de 802.3, se convierta en el IEEE 802.12.

- **802.14.**- Es una propuesta no ratificada para Fast Ethernet pero que no utiliza CSMA/CD para la capa de MAC. Por ahora este proyecto sigue denominado como 100Base-VG. Y es la primera ocasión, en que se pretende ratificar dos estándares oficiales e internacionales, para una misma solución: Ethernet de alta velocidad (100Mbps sobre cable de cobre de par torcido).

Características	10BaseT	Ethernet	Token-Ring	Local Talk	FDDI
Transmisión Técnica	Baseband	Baseband	Baseband	Baseband	Baseband
Velocidad	10 Mbps	10 Mbps	4, 16 Mbps	230 Kbps	100 Mbps
Topología	Estrella	Bus	Star-wired ring	Bus	Anillo Dual
Método de Acceso	CSMA/CD	CSMA/CD	Token Passing	CSMA/CD	Token Passing
Estándar IEEE	802.3	802.3	802.5	———	802.8

CAPITULO 3. TECNOLOGÍAS DE VANGUARDIA

Hoy en día las tendencias de la industria informática muestran que la segunda gran revolución que están causando las computadoras será cuando todas ellas se integren en una sola RED. Cada vez es más común escuchar hablar de la Supercarretera de información y de usuarios, desde corporativos hasta estudiantes con las computadoras de sus casas, que se conectan a redes internacionales como Internet.

3.1. CONCEPTOS DE CONECTIVIDAD

Conectividad es la capacidad de interconectar equipos de computo, de igual o diferente naturaleza. Esto es, se puede conectar una computadora personal a otra, una Red LAN a otra, una Red Local a un Mainframe, Redes de computadoras a Redes de Computadoras, etc.

Para su estudio se harán dos divisiones básicas:

Conectividad por su entorno Geográfico

- Enlaces Locales
- Enlaces Remotos

Enlaces Locales. Son aquellos que, por la disposición física de los elementos a conectar, pueden enlazarse directamente por medio físico dedicado exclusivamente a dicha conexión.

Enlaces Remotos. Son aquellos en los que, los elementos a conectar están dispersos física y/o geográficamente, por lo que se requiere utilizar medios indirectos de comunicación como pueden ser líneas telefónicas privadas o conmutadas, canales de radiofrecuencia (microondas o señales de radio) y señales satelitales. Son enlaces indirectos.

Desde otro enfoque se podría decir, que en un enlace local el medio físico de comunicación pertenece a la misma compañía que desea establecer el enlace y en los remotos es necesario recurrir a medios pertenecientes a terceros (compañías telefónicas, empresas que proporcionan servicios satelitales y de microondas).

Otra característica general, es que en una conectividad local se alcanza altas velocidades, (hoy en día hasta 150 Mbits/s.), Ya que el medio de comunicación está dedicado exclusivamente al enlace. En las conexiones remotas, las velocidades que se alcanzan son bajas, (hasta 128 Kbits/s).

Soluciones de Conectividad

En conectividad existen diferentes necesidades a cubrir mismas que pueden solucionarse mediante:

- Puentes o Ruteadores (Conexiones entre Redes)
- Gateways (Conexiones de Redes con Mainframes)

Puentes y Ruteadores Locales

Para conformar un puente o ruteador se requiere de un componente en hardware y un componente en software. En la parte de hardware se requiere de las interfaces de Red convencionales, estas pueden ser de igual o diferente tecnología, (Arcnet, Ethernet, Token Ring, etc.) que serán instaladas en una sola computadora personal que se habilitara como servidor de comunicaciones. El servidor de comunicaciones se definirá como interno si el puente se establece en el mismo file server y externo si se establece en otro nodo. El componente en software consiste en un conjunto de programas que permiten la conversación de comunicación de protocolos (Toker Passing, CSMA/CD, etc.) de las diferentes interfaces que fueron instaladas. Sobra decir que dicho software se instala en el servidor de comunicaciones.

Algunos sistemas operativos ya tienen incluido el software necesario para establecer un puente o ruteador y es común que los sistemas operativos punto a punto no permitan estas facilidades de conectividad.

Los puentes cubren cuatro necesidades básicas:

1. ***Unir Redes***.- Por una parte, permiten que REDES LOCALES ya instaladas sean unidas entre sí, sin importar la tecnología de estas. Consecuentemente es posible tener dos o más redes con tipologías diversas trabajando entre sí mediante un puente o ruteador, dando la oportunidad de tener, por ejemplo, diferentes departamentos de una compañía interconectados.

2. ***Incrementar Rendimiento***.- Cuando se tiene la necesidad de aumentar el número de nodos de una RED, los puentes o ruteadores aseguran un mejor rendimiento que el crecimiento en una sola RED, ya que el puente o el

ruteador se encargará de dividir el tráfico de información entre cada RED conectada a el. Por ejemplo; si se requiere incrementar en 40 el número de nodos de una RED de 60, los tiempos de respuesta serán más satisfactorios con un puente o ruteador ya que él trafico de información se subdividirá en las secciones de 60 y 40 nodos. El rendimiento de una configuración como anterior (dos redes interconectadas) será mucho mayor al de una sola RED de 100 nodos.

3. ***Duplicar Distancias***.- El uso de un puente o ruteador permite también duplicar las distancias sin la necesidad de un repetidor, debido a que en cada extremo del puente o ruteador se tendrá una red que podrá cubrir la distancia máxima, según su medio de comunicación.

4. ***Alarga Vida del Hardware***.- La implementación de un puente o ruteador también alarga la vida útil de interfaces de RED con tecnologías en desuso, esto es; se puede hacer interactuar una pequeña RED de tecnología atrasada con otra tecnología más reciente mediante un puente o repetidor, ya que este se encargara de hacer la traducción de protocolos a efecto de que la comunicación entre las dos redes se lleve a cabo de manera óptima.

Los puentes y ruteadores hoy en día, también se pueden conseguir comercialmente como "cajas", esto es Hardware fabricado como puentes o ruteador que vienen en sus respectivos gabinetes, las ventajas de este otro tipo de servidores de comunicaciones es que no se depende del status apagado o prendido de una computadora personal.

Puentes y Ruteadores Remotos

Cuando se requiere conectar dos redes locales que por su dispersión geográfica son remotas entre sí, la solución es implementar un puente remoto.

Un puente remoto, también tiene un componente en hardware y un componente en software. El hardware consiste en una tarjeta especial que se conecta en una computadora de RED personal además de la interface de RED convencional, dicha tarjeta se comunica directamente a un modem para que, a través de una línea telefónica privada o conmutada, se conecte a la otra RED, la cual tiene una configuración similar.

El componente en software es un programa que permite transferir los datos de la interface de RED convencional a la tarjeta de puente remoto.

Existen comercialmente diversas configuraciones para puentes remotos que van desde comunicaciones asíncronas, X.25 etc.

El principal problema de este tipo de implementaciones es que las velocidades que alcanzan dependen principalmente del medio de comunicación y como este no es un canal dedicado las velocidades son relativamente bajas. Este problema se solucionara en un futuro inmediato con las nuevas tecnologías de comunicación que nos ofrecen las compañías telefónicas, como la RED Digital de Servicios Integrados (RDSI) y Comunicaciones en Banda Ancha, como son ATM y FRAME RELAY.

Gateway

Cuando se requiere conectar una RED LAN a un equipo central (Minicomputadora, Main Frame, o RED Pública de Datos), la solución es el establecimiento de un Gateway.

El objetivo de un "Gateway" es lograr la comunicación de una RED LOCAL a otro ambiente, a través de una sola línea. Lo anterior hace posible que desde cualquier estación de trabajo de la RED se pueda accesar a otro ambiente, que regularmente es un equipo mayor.

Existen dos razones de mucho peso para que si se desea enlazar una RED LOCAL a un "Host" (equipo central), se realice a traves de Gateways y no con tarjetas emuladoras clásicas.

1. Economía

Es mucho más económico adquirir las tarjetas Gateway y el software necesario para las Estaciones de Trabajo, que comprar una tarjeta emuladora para cada PC que necesite conectarse.

2. Facilidades de Líneas

Casi siempre es más sencillo conseguir una sola línea para Gateway, que una línea para cada PC que necesite conectar.

Existen actualmente, tres divisiones principales de Gateways en el mercado:

- Gateways que utilizan enlaces síncronos a computadoras IBM 43XX y 30XX, o bien IBM medianos (familias/34/36/38) a otros equipos mayores como UNIVAC.
- Gateways que utilizan enlaces asíncronos a computadoras medianos y grandes.
- Gateways que utilizan el protocolo X.25 para brindar conectividad a REDES públicas de datos como TELEPAC, BitNet, PEMEXPAQ, etc.

Para que se comprendan las principales características de los Gateways, es necesario definir el término de SESION.

Una sesión es el establecimiento de una conexión lógica entre un dispositivo y la computadora. En el lenguaje de IBM existe también el concepto de unidad lógica (LU), que en términos concretos puede ser una terminal o una impresora (un dispositivo con en cual se establece una sesión).

Los términos anteriores son importantes, porque normalmente las capacidades de los Gateways a equipos mayores, están medidas en su capacidad de LU's, lo cual es sinónimo del número de sesiones que pueden manejar.

Comentarios Generales acerca de los Gateways

Aunque los Gateways son una solución ideal para muchos casos, tienen ciertas limitaciones inherentes a su forma de conexión de igual forma que las tarjetas de emulación.

Cuando se desean transferencias continuas de archivos de volúmenes mayores, los tiempos de transmisión para pasarlos a la RED pueden ser considerablemente grandes, incluso de horas.

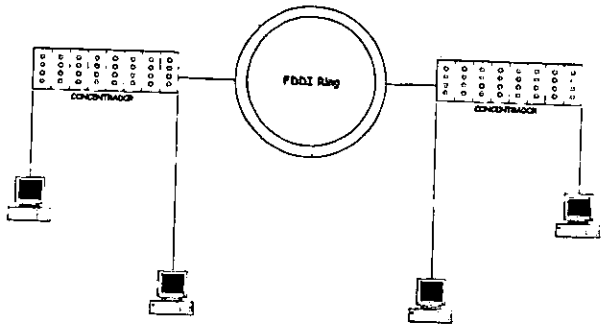
Por otra parte, vale la pena comentar que los Gateways regularmente platican de "igual a igual" entre las estaciones de trabajo de la RED (como enlaces "peer-to-peer"), lo cual significa que un Gateway pertenece a tipo de aplicaciones que no necesitan pasar por el server para realizar sus funciones, a menos que la tarjeta Gateway haya sido instalada en el propio SERVER, o que se tenga una RED de tipo estrella.

FDDI

La nueva 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 de 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 tipologías 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 (hasta de 100 Mbps).

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

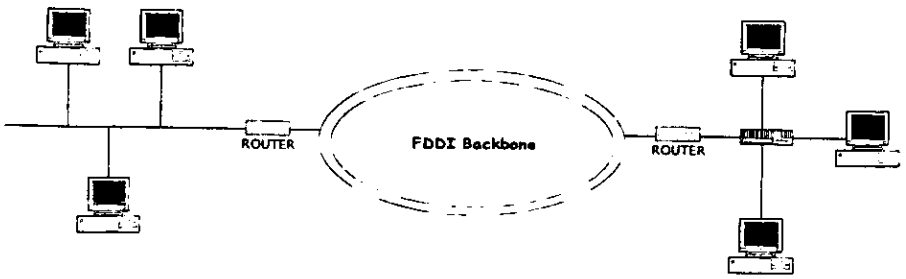
Además, la fibra óptica tiende a ser más segura que el cableado de cobre. Una red interconectada por medio de fibra óptica puede trabajar cerca de equipo eléctrico altamente sensible sin interferir uno con el otro. Un cable de fibra óptica entre dos edificios no atraerá rayos como el cable de cobre.

Al hablar de redes interconectadas por medio de la 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 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 otro, 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.

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, dando el alto costo 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).

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

Característica	10Base T	Ethernet	Token Ring	Token Bus	FDDI
Técnica de transmisión	Baseband	Baseband	Baseband	Baseband	Baseband
Velocidad	10 Mbps	10 Mbps	4, 16 Mbps	230 Kbps	100 Mbps
Topología	Estrella	Bus	Star-wire ring	Bus	Doble anillo
Método de acceso al medio	CSMA/CD	CSMA/CD	Token Passing	CSMA/CD	Token Passing
Estándar IEEE	802.3	802.3	802.5	_____	802.8

3.2. PUENTES, RUTEADORES Y CONCENTRADORES

Puentes o Bridges

Cuando las necesidades informáticas de una empresa u organismo crecen, se llega a la necesidad de interconectar redes locales de computadoras con otras redes. Esto es posible realizar por medio de una gran variedad de productos, como son los puentes, ruteadores y concentradores.

En término puente se usa para connotar el hardware y software que se necesiten 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 otra. De hecho son más que un repetidor, tiene suficiente información sobre los paquetes que maneja aunque no conoce la estructura propia de éstos. El trabajo de un puente solo se realiza en los niveles 1 y 2 del modelo OSI.

Un puente no hace diferencias sobre el tipo de protocolo que se usa 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.

La principal ventaja de utilizar puentes para la interconexión de redes locales, es que logran canales de alta velocidad. Su principal desventaja es que no se divide él trafico entre las redes a conectar, por el contrario se incrementa. Por ejemplo, si se tienen dos redes cada una de 25 nodos, se une a través de un puente, el resultado será de dos redes lógicas de 25 nodos y una red física de 50 nodos, el problema es que él trafico en la red es el generado por los 50 nodos.

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

Ruteadores o Routers

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

Un ruteador reduce en gran medida la cantidad de tráfico innecesario entre las redes locales conocidas, ya que solo 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 en aspecto de velocidad.

Los ruteadores manejan los niveles 1,2,3,4 del modelo OSI.

En los equipos modernos ya es común hablar de los BROUTERS, que son puentes y ruteadores simultáneamente.

Según algunos analistas clasifican a las redes lan's en generaciones. La segunda generación comienza con el surgimiento en el mercado de los ruteadores.

Concentradores

El término concentrador dentro del mercado se pueden dar dos acepciones generales. La primera se asocia con los "hubs" o con concentradores físicos. La segunda se analizara más adelante.

Un concentrador o "hub" 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 gabinete y ahí mismo es 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 confiables.

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.

La segunda definición que hoy en día se le da a los concentradores, es que además de simplificar el cableado y reducir sus fallas, tiene la función de Puentes, Ruteadores, Transductores, etc. Esto es posible gracias a la modularidad con la que son diseñados.

Todo concentrador que tiene estas funciones de modular, debe ir creciendo conforme a las demandas de la red. La filosofía de crecimiento varia de acuerdo a cada fabricante.

Puntos de consideración importantes:

- El concentrador hace las funciones de puente y ruteador, entre todas las tarjetas instaladas. Quizá esta sea la característica más importantes de este tipo de concentradores, para poder lograr esta comunicación entre los diversos protocolos de niveles físicos (Niveles 1 y 2 del modelo OSI), se requiere de un protocolo de mayor nivel que logre la interconectividad, dicho protocolo es TCP/IP[1]. Por lo cual es necesario que todo el hardware sea compatible con este protocolo.

- Se puede tener la administración de la red, gracias al modulo SNMP, pero se requiere de un software especial de administración compatible con este protocolo, el sistema debe correr en una estación de trabajo dentro de la red.

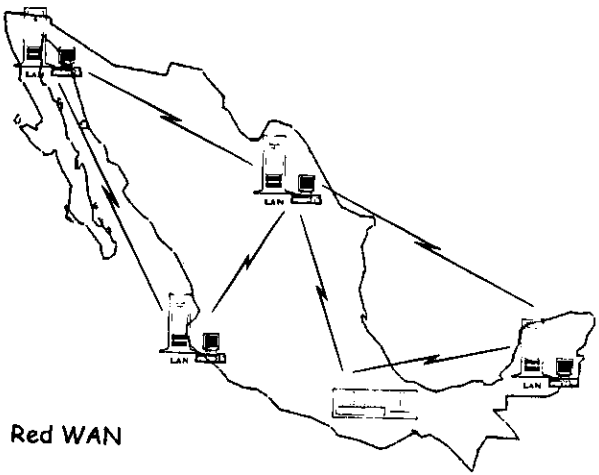
- La mayoría de los fabricantes ofrecen sistemas de redundancia en las fuentes de poder de sus equipos, además de UPS propios para los concentradores, estos aditamentos también siguen la filosofía modular y son opcionales.

- Otra característica interesante, es que las tarjetas del concentrador así como sus demás módulos, se pueden intercambiar, mientras el equipo esta encendido.

[1] TCP/IP.- Transmisión Control Protocol / Internet Protocol.

3.3. REDES WAN Y MAN

Además de las redes de área local LAN, existen las WAN[2] y las MAN[3]. 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.



Red WAN

Reconociendo las necesidades de contar con estándares de mayor alcance que los aplicables a las redes de área local, aunque sin llegar a redes de área basta estándar, en 1981 se estableció el Metropolitana 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 vídeo.

Como las MAN están diseñadas para redes que se extienden en distancias largas donde no es posible tener el canal de comunicación dedicado 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 cambio pronto a un protocolo de acceso múltiple con división de tiempo (TDMA).

[2] Wide Area Network
[3] Metropolitan Area Network

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.

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

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

Compañías, gobiernos locales, sistemas escolares, etc., han continuado con 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 redes de área amplia.

El comité describe varias metas para estándar MAN: debe dar cabida a esquemas de transmisión de señales rápidos y robustos, debe garantizar seguridad y privacia y hacer posible el establecimiento de redes privadas virtuales dentro de la 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 de describir estándares MAN es que estos todavía continúan en su proceso de desarrollo, sin embargo, el desarrollo de un estándar 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.

Se espera que el tráfico de 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.

Hoy en día con la tecnología de RDSI[4] o ISDN[5], ofrecen la infraestructura en cuanto al medio de comunicación, que las redes WAN y MAN requieran para cubrir sus objetivos.

[4] RDSI.- Red Digital de Servicios Integrados
[5] ISDN.- Integrated Services Digital Network

Velocidad de transmisión	LAN	WAN
Common	10 – 16 Mbps	9.6 – 56 Kbps
High Performance	100 Mbps	1.544 – 45 Mbps

Características	LAN	WAN
Network Owner Operator	Individual Company	Comunication Service Provider
Protocols	Ethernet, Token Ring, FDDI, TCP/IP	X.25, Frame Relay, TCP/IP

3.4. ENLACES TCP / IP

TCP / IP (Transmision Control Protocol / Internet Protocol) es una familia de protocolos para interconectar computadoras de diversas naturalezas. Lo que 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 uso 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 desarrollando, se fue estandarizando.

La forma en que se desarrolla hoy en día, es por medio de un Comité llamado IAB, que esta 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 penso para ser independiente del medio físico de enlace, esto precisamente lo que ha hecho que sea un protocolo ampliamente usado en enlaces de redes entre si, o bien, con redes amplias WAN.

Las ambientes que usa TCP / IP se basan en que cada elemento de la red tenga su dirección IP. El propósito de lo anterior es identificar de la forma única a cada elemento del conjunto.

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, pero no nos garantiza que éstos lleguen a su destino. Para remediar esto, está TCP.

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 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 base de datos, teniendo por un lado el equipo corriendo al manejador de base 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 estos están en la misma red o en redes distintas, las 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.

Protocolos, Pilas y Conjuntos

Un Protocolo es un conjunto de reglas que gobiernan las acciones de comunicación.

Una Pila de Protocolos es un conjunto subdividido de protocolos que interactúan con el fin de proveer comunicación entre diversas aplicaciones.

Un conjunto de Protocolos es una familia de protocolos que opera de manera conjunta a efectos de crear una plataforma consistente.

Acciones de IP

Si el destino de un Datagrama no se encuentra en la misma red como el Host fuente, el IP del Host direcciona el datagrama al ruteador local. Si éste no esta conectado a la red destino, entonces el datagrama debe ser enviado a otro ruteador. Esta secuencia de operaciones continúa hasta que el datagrama llega a la red destino.

El IP decide el ruteo de la información mediante la detección de un destino remoto en una tabla de ruteo. El IP busca una entrada en la tabla de ruteo que corresponda al destino con la identidad del siguiente ruteador al cual se le relevará el trafico de datagramas.

Información de la Tabla de Ruteo

En una Inter-Red pequeña y fija, las tablas de ruteo pueden ser introducidas y tener un mantenimiento en forma manual. En Inter-Redes más grandes, los ruteadores mantienen sus tablas actualizadas mediante el intercambio de información con los demás. Los ruteadores tienen la capacidad de descubrir dinámicamente hechos tales como:

- La conexión de una nueva red a la Inter-Red.
- La inhabilitación de un camino hacia una red destino.
- La conexión de un nuevo ruteador a la Inter-Red, mismo que determina la ruta más corta hacia ciertos destinos.

Arquitectura TCP

El TCP se implementa en el Hosts, la entidad de TCP en cada extremo de una conexión debe asegurar que los datos que se entregan a su aplicación local lleguen:

- Precisos
- En secuencia
- Completos
- Sin datos duplicados

El envío de una aplicación pasa una trama de bytes al TCP. Este se encarga de disgregar la trama en secciones y añadirle a cada sección una cabecera, formando segmentos. Posteriormente el TCP pasa cada segmento al IP para ser transmitido en un Datagrama.

Un TCP receptor debe mantener informado al emisor a cerca de la cantidad de información correcta que le ha llegado, mediante señales de reconocimiento (AKCs). Si el AKC de un segmento no llega en un intervalo de tiempo determinado, el TCP emisor vuelve a enviar ese segmento. A esta estrategia se le conoce con el nombre de Retransmisión con Reconocimiento Positivo.

Ocasionalmente una retransmisión provocará una reproducción en los segmentos entregados al TCP receptor.

El TCP receptor debe arreglar los segmentos que van recibiendo, en forma correcta, descartando todos aquellos que estén duplicados, De esta manera, el TCP entrega los datos a su aplicación de manera íntegra.

TCP es un protocolo completamente bilateral, es decir; los dos extremos de la conexión pueden enviar y recibir información al mismo tiempo, por lo que, de hecho se transmiten dos tramas de bytes.

El Software de Protocolo Inter-Red (IP) opera tanto en Hosts como en Ruteadores IP. En general, el Software IP permite a la computadora que lo ejecuta, funcionar como un Host IP, como un Ruteador IP, o como ambos a la vez.

TCP Y OSI

7 Aplicación	Servicios de Aplicación	SMTP
6 Presentación	Formateo de datos	FTP
5 Sesión	Regulación de Conversación	Telnet, etc.
4 Transporte	Integridad de datos de extremo a extremo	TCP, UDP etc.
3 Red	Ruteo y Conmutación	IP, ICMP, etc.
2 Enlace	Transmisión de Frames	Ethernet,
1 Físico	Acceso al medio	Arpanet, etc.

Nombres y Dominios

Tanto los nombres de la estructura de una Inter-Red como los de un sistema administrativo, son jerárquicos. Una Inter-Red está dividida en partes llamadas Dominios.

La responsabilidad de asignar nombres dentro de un dominio es tarea del administrador designado de ese dominio. Este administrador puede crear subdominios y delegar la autoridad de nombramiento a otro individuo de cada subdominio.

Ejemplos de Nombres de Inter-Red

Un nombre de Inter-Red puede describir a un sistema de manera muy apropiada ya que su estructura se basa en la concatenación de etiquetas que hacen referencia a cada subdominio. El nombre de una Inter-Red puede ser escrito en mayúsculas o minúsculas indistintamente:

EJEMPLO.ARAGON.ENEP.UNAM
ejemplo.aragón.enep.unam

Es fácil entender la estructura jerárquica de estos nombres. Todas las divisiones de la Universidad se encuentran en el Dominio UNAM de la Inter-Red. ENEP es el Dominio de segundo nivel justo abajo del nivel UNAM. ARAGON se encuentra como dominio de tercer nivel bajo de ARAGON. Finalmente el nombre del host que identifica un sistema individual, inicia la cadena que define el nombre. Las partes adyacentes del nombre se separan por medio de puntos (.).

El tamaño límite de cada etiqueta es de 63 caracteres pero el número máximo de caracteres por nombre es de 255 incluyendo los puntos separadores.

Formato de Direcciones

El IP utiliza direcciones para identificar a los Hosts y para enviarles información. Cada Host debe tener asignada una dirección IP que pueda utilizarse en comunicaciones reales. El nombre de un Host es traducido a su dirección IP mediante la tabla de relación de Nombres y Direcciones.

Una dirección IP es un valor binario de 32 bits que define el espacio total de direcciones que es un conjunto de números de direcciones. El conjunto total de direcciones IP contiene 232 números.

La notación punto es la forma más popular de expresar una dirección IP de tal forma que los usuarios finales pueden leerlas y escribirlas fácilmente. Cada octeto de las direcciones se convierte en un número decimal y cada número se separa por un punto (.). Por ejemplo, la dirección de UNAM.ENEP.ARAGÓN.EJEMPLO en notación de 32 bit binarios será:

10000010 10000100 00001011 00011111

130.132.11.31

Cabe hacer notar que el número más grande que puede aparecer en una notación separada por puntos es 255, que corresponde al número binario 11111111.

Una dirección IP se constituye de dos partes:

- Dirección de Red
- Dirección de Nodo o Dirección Local

La dirección de Red identifica la Red a la cual está conectado ese nodo, la Dirección Local a su vez, identifica al nodo de manera individual.

Direcciones Clase A, Clase B y Clase C

Las redes varían en tamaño. Existen tres formatos de direcciones diferentes para Inter-Redes que definen el uso dependiendo de su tamaño:

- Clase A para redes grandes
- Clase B para redes medianas
- Clase C para redes pequeñas

Además de las clases A, B y C existen dos formatos de direcciones especiales, esto son: Clase D y Clase E. Los formatos de clase D se utilizan para un Multicasting de IP que se emplea para distribuir un mensaje a un grupo de sistemas dispersos a través de la Inter-Red. La Clase E reserva su formato de direcciones para uso experimental exclusivamente.

Los primeros cuatro bits de cada dirección determinan su clase:

BITS INICIALES	CLASE
0XXX	A
10XX	B
110X	C
1110	D
1111	E

Sub-Redes

Cuando se implementa con una dirección de Red Clase A o Clase B se entiende la implicación de una complicada interconexión de Redes LAN y WAN. Es por eso que resulta práctico dividir en partes el espacio de direcciones, de tal forma que corresponde a la estructura de la Red como una familia de Sub-Redes. Para llevar a cabo esto, es necesario descomponer la parte local de la dirección de la siguiente manera:

Dirección de Red Dirección de Sub-Red Dirección de Host

La asignación de la dirección de Sub-Red frecuentemente se hace en un byte límite, cuando se implementa con direcciones Clase B como 156.33 debe utilizar su tercer byte para identificar las Sub-Redes, por ejemplo:

156.33.1
156.33.2
156.33.3

El cuarto byte será utilizado para identificar a los Host de manera individual dentro de una Sub-Red. Por otro lado cuando se implementa direcciones con Clase C solo se tiene un espacio de dirección de un byte y deberá utilizar cuatro bits para las direcciones de los Hosts.

Mascaras de la Sub-Red

Una máscara de Sub-Red es una secuencia de 32 bits que cubre con unos (1s) las zonas correspondientes a la red y a la Sub-Red, y cubre con ceros (0s) la zona que le corresponde a la dirección del Host. El tráfico de información sé rutea hacia un Host, considerando las partes de la Red y Sub-Red de su dirección IP. Es sencillo decir que tanto de una dirección correspondiente a la dirección de red debido a los formatos estrictamente definidos para Clase A, Clase B y Clase C.

A efecto de reconocer cualquier tipo de campo, con un tamaño arbitrariamente elegido para la Sub-Red, se creó un parámetro de configuración denominado Mascara de Sub-Red.

Identificación de Redes

Es muy recomendable conocer la forma en que se debe utilizar la notación punto para la dirección de IP, a fin de hacer referencia a la Red. Por convención, esto se hace llenando con ceros la parte correspondiente a la dirección local de la dirección IP. Por ejemplo, 5.0.0.0 identifica una red Clase A, 131.18.0.0 identifica a una Red Clase B y 201.49.16.0 identifica a una Red Clase C. La misma convención se sigue para la identificación de Sub-Redes con la desventaja de que nunca deben asignarse direcciones de este tipo a Hosts o a Ruteadores debido a que, por la notación empleada, es muy factible caer en una confusión.

3.5. 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 resto es poder manejarlas con una unidad.

La OSI (Organización Internacional de Standeres), ha categorizado las funciones de la administración de las redes como se vio anteriormente. Los dispositivos de interconexión entre 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 solo son tres: Get, Set y Trap). 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 comprende el marco de trabajo de SMNP.

3.6. B-ISDN: BroadBand – Integrated Services Digital Network

En la actualidad la tendencia en el mundo de las telecomunicaciones apunta hacia una red universal, conocida como B-ISDN, que soporte diferentes tipos de servicios, generalmente con requerimientos distintos. Una red de banda ancha multimedia, como la B-ISDN.

La concepción de la B-ISDN se debe tanto al gran avance tecnológico en el campo de la electrónica y la calidad de los medios de transmisión utilizados por las redes actuales (transmisión digital, fibra óptica, etc.) que permiten pensar en la

implementación de redes que efectúen la transmisión y conmutación de tráfico a altísimas velocidades de manera confiale, como a la transmisión de datos lo cual ha cambiado radicalmente los sistemas de transmisión. El concepto actual, es diseñar la red para que se pueda no-solo transmitir datos sino proporcionar servicios de otro tipo (incluso combinaciones de trafico: voz y datos, por ejemplo) a altas velocidades y con excelente calidad en el funcionamiento eficiente para cualquier tipo de servicio.

Una posible solución a esta tecnología de conmutación rápida de paquetes FPS (Fast Packet Switching), este concepto cubre todas las características básicas. Además es un concepto aplicable a todos los sistemas que operan a tasas de velocidad mucho más altas que los sistemas convencionales de conmutación de paquetes.

El FPS ha sido estudiado por la UIT-TS (antes conocida como CCITT) en los últimos años por ser la solución a B-ISDN. Esta tecnología tiene varias alternativas de implementación que se pueden clasificar en frame relays (paquetes de longitud variable) en el cual se encuentra FRAME-RELAY y cell relay (paquetes de longitud fija) en donde esta SMDS y ATM.

3.7. ISDN

El estándar de la red digital de servicios integrados (ISDN) tiene por objetivo el enlazar todo hogar y oficina con unos servicios digitales a alta velocidad utilizando líneas telefónicas, eliminando finalmente las líneas telefónicas analógicas. Una vez que, si se implantara el estándar, todo el sistema telefónico fuera completamente digital, lo que significa que no seria necesarios modems para interconectar las computadoras utilizando líneas telefónicas, los usuarios de las computadoras personales podrían aprovechar al máximo las ventajas de las ISDN. Estas ofrecerán conexiones para servicios de datos, base de datos y redes internacionales con velocidades de transferencia razonablemente rápidas. En la actualidad, ISDN sólo se encuentra disponible en ciertas áreas, aunque son más las que se están convirtiendo.

La conversión se ha de llevar a cabo sobre las líneas analógicas que van de la casa o la oficina a la central telefónica. LA mayor parte de las compañías telefónicas ya disponen de conexiones digitales con otras áreas telefónicas. Desde el lado de la casa, probablemente haya que recablear, siendo necesario un adaptador especial para adaptar los niveles de tensión del PC con los de la línea ISDN. Una velocidad de transferencia realista para los datos de la computadora personal sobre las líneas ISDN es de unos 150 Kb/s.

3.8. FRAME RELAY

La definición de frame relay fue hecha por el CCITT(UIT-T) (Recomendaciones 1.122, Q.922 y Q.933, así como las de la serie 1) y por ANSI, especialmente de TISI (estándares TI, 602, 206, 617 y 618). Además, se ha integrado un grupo de fabricantes, vendedores y operadores de la tecnología, el Frame Relay Implementors, como DEC, StrataCom y Bell Northern.

Frame Relay está diseñado para manejar el aumento de información en la carga de datos de área amplia y evitar retrasos, facilita la interconexión de las redes locales debido a los beneficios de eficiencia que representa, mejores tiempos de respuesta, calidad aceptable del servicio, transparencia y flexibilidad, las tecnologías de paquetes, como frame relay, ha comenzado a reemplazar a arquitecturas más tradicionales como las de circuitos (TDM Time Division Multiplexing) y X-25.

Frame Relay transporta únicamente datos. Elimina gran parte del control y detección de errores de X-25, por lo que requiere menos procesamiento que éste. Soporta velocidades hasta de canales T1, aunque cubre el rango de 256 kbps a 34 Mbps. La conmutación por células manejara de 34 Mbps hasta 155 Mbps en la interface del usuario y 600 Mbps entre nodos conmutados.

Como X.25, frame relay transporta datos dentro de frames y no maneja paquetes. Tiene la capacidad de realizar funciones, de enrutamiento a nivel de frame. En realidad constituye una versión simplificada del nivel de frame de X.25 con alguna semejanza con el LAPD, el nivel de frame de RDI (ISDN; Integrated Services Digital Network), (Red digital integrada) para el canal D. Este procedimiento de comunicación se ubica en la capa 2 del modelo OSI. Funciona al transferir datos mediante un nivel rudimentario de frames que se denomina él núcleo, el cual consiste, básicamente, en sobres de frame tipo (HDLC, High Level Data Link Control).

Frame Relay no posee funciones para control del flujo de datos, el frame contiene un campo que actúa como un identificador lógico del canal a nivel del frame (el DLCI, Data Link Connection Identifier; identificador de la conexión del enlace de datos). Este permite que los circuitos lógicos conmutados o permanentes se fijen en el nivel 2, lo que hace que las funciones de enrutamiento se lleven a cabo en éste último.

Entre los principales beneficios de la tecnología de frame relay, además de los que se describen antes, es que permiten al usuario aprovechar al máximo cualquier mejora cualitativa en la capa física.

Los enlaces de fibra óptica han cambiado radicalmente la calidad del servicio en los medios de transmisión, además de las mejoras continuas en los enlaces de

cobre. Por lo tanto, se elimina la necesidad de realizar controles y correcciones de errores frecuentes.

Frame Relay ofrece casi cinco veces más velocidad en la conmutación, dando a la simplificación del proceso. Sus usuarios también pueden compartir canales costosos, tales como T1, E1, T3 y E3. Es importante señalar que considera el rápido aumento en el poder de procesamiento de las estaciones de trabajo, que ahora pueden intercambiar grandes archivos y realizar funciones de telecomunicaciones que antes se llevaban a cabo en los nodos de la red.

Frame Relay maneja con eficiencia un tráfico irregular e impredecible y suministrar acceso de una sola línea a la red con conectividad lógica hacia cualquier otro destino. Lo que reduce los requerimientos de hardware, y simplifica el diseño de la red.

Aunque frame relay no corrija errores, debido a las recientes mejoras tecnológicas, tales como la introducción de la fibra óptica o los adelantos en la electrónica de repetidores en línea, los errores que detecta pueden corregirse extremo a extremo por X.25 o TCP / IP, por ejemplo. De esta manera se aligera al software de conmutación del nodo, lo que permite una conmutación mucho más rápida.

Este protocolo no incluye un mecanismo de control de flujo que reduzca las ventanas de transmisión. Si no que señala los problemas de conjestionamiento. Descarta los frames que provocan, y deja que un protocolo de nivel más alto retransmita los mensajes correspondientes.

A continuación se presentan, de manera general, los principales aspectos de Frame Relay:

- Orientado a conexión
- Paquetes de longitud variable
- Velocidad de 34 Mbps
- Servicio de paquetes en circuito virtual, tanto con circuitos virtuales conmutados como con circuitos virtuales permanentes
- Trabaja muy similar a una simple conexión de modo-circuito (en donde se establece la conexión entre el receptor y el transmisor, y luego se lleva a cabo la conmutación de la información), la diferencia esta en que la información del usuario no es transmitida continuamente sino que es conmutada en pequeños paquetes (frame – relays).
- Sigue el principio de ISDN de separar los datos del usuario de los datos de control de señalización para lo cual divide la capa de enlace en dos subcapas.
- Mínimo procesamiento en los nodos de enlace o conmutación
- Supone medios de transmisión confiables
- Funciones implementadas en los extremos de la subred.
- Maneja el protocolo HDLC de igual manera que X.25.
- El protocolo de transferencia es bidireccional entre las terminales

- La capa inferior detecta pero no corrige los errores, se deja para las capas más altas, lo cual lo hace más rápido y transparente.
- Ideal para interconectar LAN y WAN por sus altas velocidades y transparencia a las capas de red superiores
- Se pueden cargar múltiples protocolos de LAN sobre Frame Relay

3.9. ATM

ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) es una tecnología de comunicaciones de datos de conmutación de paquetes de banda ancha diseñada para combinar las características de los multiplexores por división de tiempo con retardo dependiente (TDM) y redes locales de retardo variable.

- Una red de banda ancha es aquella, en que las señales viajan como señales de radiofrecuencia por canales separados. Se soporta la transmisión simultanea de datos, voz y vídeo por varios canales.

- La conmutación de paquetes es la capacidad de enviar pequeñas unidades de información (paquetes) por canales ATM. Un mensaje es dividido en paquetes de 48 bytes (llamados celdas en ATM), y se le añade una cabecera de 5 bytes, lo que da un tamaño de celda de 53 bytes. Los paquetes son situados en un canal ATM, y generalmente son mezclados con otros paquetes (multiplexados).

- En el extremo receptor, los paquetes son reensamblados. La multiplexación por división de tiempo es un método para combinar señales separadas en una única transmisión de alta velocidad. Con ATM, se transmiten celdas provenientes de muchas fuentes. Pueden mezclarse, pero cada una tiene su dirección de destino específica. En la multiplexación por división de tiempo regulares. En otras palabras, todas las celdas son del mismo tamaño, tanto en bytes como en tiempo.

El retardo variable es habitual en las redes locales, debido a que cada método de red puede utilizar un tamaño de paquete distinto. ATM divide los paquetes largos para adoptarlos a su tamaño de celda y los envía por el canal de datos; éstos son reensamblados en el otro extremo.

ATM ofrece un método para enviar simultáneamente información en paquetes procedentes de varias fuentes sobre una línea a alta velocidad, donde es reensablada y enviada a cada sistema de destino. La característica más interesante de ATM es que se aplica a un amplio rango de comunicaciones de datos, desde el bus de datos de una central de cableado hasta un sistema internacional de comunicación de datos. ATM no debe infravalorase como posible estándar para integrar todos los sistemas de comunicaciones y computadores.

Los fabricantes están comercializando hubs de cableado con backplanes ATM y conexiones ATM para redes de gran alcance.

ATM combina la multiplexación y conmutación de paquetes en un método universal de transferencia de datos. Soporta redes locales, voz y vídeo. Las celdas (paquetes de ATM) son procesadas rápidamente, debido a su pequeño tamaño. Hay muy poco retardo en la conmutación de paquetes. Esto es importante para las transferencias de voz y vídeo, que son sensibles al tiempo.

ATM es un protocolo de transporte que funciona básicamente en el subnivel MAC de la jerarquía de protocolos. Debido a esto, puede trabajar sobre muchas tipologías a nivel físico. ATM no se basa en ningún protocolo determinado. Puede convertir tipo de paquete en celdas de 53 bytes y transportarlo sobre un backbone o WAN.

ATM está definiendo el futuro de las comunicaciones en redes de gran alcance. Suprimirá la barrera entre las LAN y WAN. Esta barrera es la caída en rendimiento asociada con las transferencias de datos sobre redes públicas. Los puentes o routers de LAN a WAN convierten los datos LAN en datos WAN, e introducen retardos al hacerlo. ATM puede utilizar SONET (Synchronous Optical Network, Red óptica síncrona) como medio físico para las redes de gran alcance. SONET es un estándar de cable de fibra óptica que las empresas telefónicas están implementando en la red pública de teléfonos y comunicaciones.

Las velocidades de transmisión de ATM son escalables, dependiendo de la capacidad del nivel físico. Con ATM, no existe un estándar que límite la velocidad de transmisión como en FDDI (100 Mbps). El pequeño tamaño de celda no exige utilizar un procesamiento especial, que es necesario en FDDI. Las celdas ATM son fáciles de construir, mientras que FDDI requiere conversiones de protocolo que originan retardos. Actualmente, ATM puede utilizarse en las líneas T1, T1 secundarias y T3 existentes. Para hacer lo mismo en FDDI, se necesita una conversión. ATM utiliza caminos independientes para los usuarios de la red cuando se implementa en una red local. FDDI es un medio compartido; cuantos más usuarios accedan al cable, más se reducirá el ancho de banda.

A continuación se presentan, de manera general lo principales aspectos de ATM:

- Técnica de conmutación de paquetes, intrínsecamente orientado a conexión
- Manejo de celdas de tamaño fijo (53 octetos)
- Transmisión a altas velocidades (51.84Mbps, 155.52Mbps, 622.08Mbps)
- Retardos bajos en la transmisión de los paquetes
- Soporta todo tipo de servicios
- ATM "adapta" todos los servicios ofrecidos para transportarlos como celdas
- Diferentes conexiones pueden soportar diferentes tipos de servicios
- Se acomoda a diversas ratas de velocidad
- Aceptable a cambios en el futuro

- En ATM se tiene una división de la capa física en dos subcapas para que el manejo del control de errores sea más simple y rápido en los enlaces de transmisión (realiza un chequeo mínimo), pues el control fuerte se hace en los extremos de la comunicación. (Funciones implementadas en los extremos de la red).
- Control de flujo a nivel de enlace
- Modo de transferencia ATM (Asynchronous Transfer Mode o Asynchronous Time Division Multiplexing). Esta técnica de multiplexamiento por división de tiempo y asincrónica, que se convirtió en la mejor innovación en cuanto al multiplexamiento se refiere y que hace uso del estado avanzado de la electrónica es el modo de transferencia utilizado por ATM. Está técnica es digital, cualquier información análoga que se quiera transmitir es primero convertida en información digital (a datos de computador) antes de llevar a cabo la transmisión, así dicha información puede ser transmitida a arbitrarias distancias y convertidas nuevamente a señales análogas en los sitios de destino.
- Modo de conmutación dinámica, basada en principio de conmutación de Banyan.
- La red no conoce el tipo de la información de la celda: conmutación universal
- Las celdas tienen información de prioridad, el tipo de servicio, controles de acceso al medio y de códigos de chequeo de errores en el encabezado
- Se lleva a cabo un contrato de tráfico de las distintas conexiones en donde el usuario especifica la prioridad y requerimientos del servicio. Este contrato se utiliza para decidir aceptar nuevas conexiones con lo cual se evita congestión en la red, de igual manera se utiliza para tomar decisiones –la red- de lo que el usuario solicito y se puede por ejemplo perder una celda (celda con baja prioridad)
- ATM puede soportar frame-relay y SMDS

Tipo	Velocidad	Uso
ArcNet	2,5 Mbps	Redes Locales
Token Ring	4-16 Mbps	Redes Locales
Ethernet cable delgado	10 Mbps	Redes Locales
Ethernet cable grueso	10 Mbps	Redes Locales extendidas

Líneas conmutadas	2.400-19.200 bits/s	Conexiones remotas monousuario
Conmutación de paquetes	Menor de 64 Kb/s	Bajo o medio en enlaces WAN
Fractional T – 1	64 Kb/s	WAN y enlaces redundantes
T – 1	1,544 Mbps	Alto en enlaces de WAN
T – 3	44,184 Mbps	Alto en enlaces de WAN
Fibra óptica	1 o 100 Mbps	Alto en enlaces de MAN

3.10. FAST ETHERNET

Para redes de área local que utilicen Token Ring (de 4 – 16 Mbps) o Ethernet (10 Mbps). Fast Ethernet es la mejor solución para aquellas redes de área local que quieran extender su desempeño mientras mantienen la compatibilidad con todo lo que existe.

Esta tecnología es fundamental en la extensión del método de acceso al medio CSMA/CD (Carrier Sense Multiple Access with Collision Detection), este método usado en las redes de área local define la forma como se transmiten la información a través del bus de transmisión (medio físico).

Uno de los problemas de Fast Ethernet es que no se ha definido aún un estándar que permita que no haya incompatibilidad entre cada uno de los productos de los distintos proveedores. Sin embargo, debido a la relativa simplificada de esta tecnología se espera que su desarrollo sea rápido.

Ventajas de Fast Ethernet:

- Alto rendimiento
- Tecnología basada en estándares

- Migración a costo aceptable con máximo aprovechamiento del equipo ya existentes (infraestructura de cableado, sistemas de administración de red etc...)
- Soporte de los principales vendedores en todas las áreas de productos de red
- Costo óptimo

Como el protocolo natural de 10 base-T, virtualmente no cambia en fast ethernet, este puede ser introducido fácilmente en ambientes de ethernet estándar, la migración es simple y económica en muchos aspectos importantes.

- Las especificaciones del cableado para red 100 base-T permite a fast ethernet corre en la mayoría de cableados comunes en ethernet, incluso categorías 3, 4 y 5 de utp, stp y fibra óptica.
- Experiencia administrativa. Los administradores pueden relevar en ambientes 100 base-T con herramientas de análisis de red familiares.
- La administración informática se traduce fácilmente de ethernet a 10Mbps a redes fast ethernet lo que significa recapacitación mínima del personal de administración y mantenimiento de la red.

Alternativas de cableado:

- 100 Base-T soporta 3 especificaciones físicas
- 100 Base Tx: cable UTP o STP de un par trenzado eia 568 o categoría 5 para datos
- 100 Base T4: cable UTP de 4 pares trenzados para voz y dato categoría 3, 4 o 5
- 100 Base Fx: sistema estándar de 2 fibras ópticas

3.11. 100VG

100VG para grado de voz, es una tecnología de redes de área local de alta velocidad que extiende el tráfico Ethernet a 100Mbps. Esta tecnología extiende la tecnología Ethernet pero no se fundamenta en el método CSMA/CD de control de acceso al medio.

100VG no es una arquitectura de red para todo, es una arquitectura de conexión de circuitos. Se traslada la responsabilidad para dirigir él trafico de datos de las tarjetas adaptadoras de la red a Hubs inteligentes, que están dedicados a administrar la red.

En esta arquitectura no hay posibilidad de colisiones ya que el Hub controla permanentemente cual estación esta enviando datos, de igual manera el Hub puede decidir el orden y la prioridad en que se aceptan los datos desde la

estación. El retardo indeterminado de acceso al medio que se presenta utilizando CSMA/CD es eliminado, pero los problemas de rendimiento debidos a retardos ocacionados por factores eléctricos continúan.

Al igual que con Fast Ethernet, no se ha definido aún un estándar que permita que no haya incompatibilidad entre cada uno de los productos de los distintos proveedores. Adicionalmente debido al cambio de protocolo de control de acceso al medio se hace indispensable el empleo de un nuevo tipo de hardware (como el de tarjetas adaptadoras de red y de Hub), lo cual coaccionaría costos adicionales.

PROPIEDAD	FAST-ETHERNET	100VG	FDDI	ATM
Método de Acceso	CSMA/CD	DPAM: Método de acceso por demanda de prioridad	Esquema de doble anillo con token	Acceso Conmutado a través de Canales y Caminos Virtuales
Servicios de Red	Tráfico Asíncrono	La prioridad permite optimizar el uso del medio para voz e imagen (comparado con Fast-Ethernet)	Trafico Asincrónico y Sincrónico	Todo tipo de tráfico
Medida de Marcos	64 – 1500 bytes	64 – 1500 bytes	64 –4500 bytes	53 bytes
Madurez de estándares	Aproximadamente cuatro años de madurez	Aproximadamente cuatro años de madurez	Cera de 14 años de madurez de estándares para redes de este tipo (100Mbps)	Madurez de estándares en redes WAN. Aún se trabaja en estándares para redes LAN
Escala	Principalmente para redes LAN	Principalmente para redes LAN	Como Backbone de alta velocidad	Para redes WAN, MAN y en el futuro en redes LAN

Costo	Predica ser la tecnología menos costosa ya que mantiene la infraestructura de 10Mbps Ethernet	Costo alto, ya que requiere de nuevos equipos especializados	La existente infraestructura (ya montada) y la proliferación de vendedores la hacen que tenga un costo aceptable	Costo alto, debido a la nueva infraestructura que requiere
Cableado UTP3	Posible	Sí	No	No
Cableado UTP4	Posible	Sí	No	No
Cableado UTP5	Sí	Sí	Sí	Sí
Cableado STP5	Sí	Sí	Sí	Sí
Cableado IBM T1 UTP	Sí	Sí	Sí	Sí
Fibra Óptica	Sí	Sí	Sí	Sí

CAPITULO 4. DEFINICIÓN DEL PROTOCOLO SNA Y SU AMBIENTE DE TRABAJO

4.1. SNA

SNA (arquitectura de redes de sistema, ARS), es una arquitectura de red que permite que los clientes de IBM construyan sus propias redes privadas, tomando en cuenta a los host y a la subred. Un banco por ejemplo, puede tener uno o más CPUs en su departamento de procesos de datos, y numerosas terminales en cada sucursal. Con el uso de SNA todos estos componentes aislados pueden transformarse en un sistema coherente.

Antes de la aparición de SNA, IBM tenía varios cientos de productos de comunicación, utilizando tres docenas de métodos de acceso de teleproceso, con más de una docena de protocolos de enlace. La idea de crear la SNA, consistió en eliminar este caos y proporcionar una infraestructura coherente para el proceso distribuido débilmente acoplado. Debido al deseo de varios clientes de IBM de mantener la compatibilidad de todos estos programas y protocolos (mutuamente incompatibles), la arquitectura SNA resulta más complicada de lo que debiera haber sido, de no existir estas limitaciones. La SNA efectúa también un gran número de funciones que se encuentran en otras redes, las cuales, aunque resulta muy valiosas para ciertas aplicaciones, tiende a elevar la complejidad total de su arquitectura.

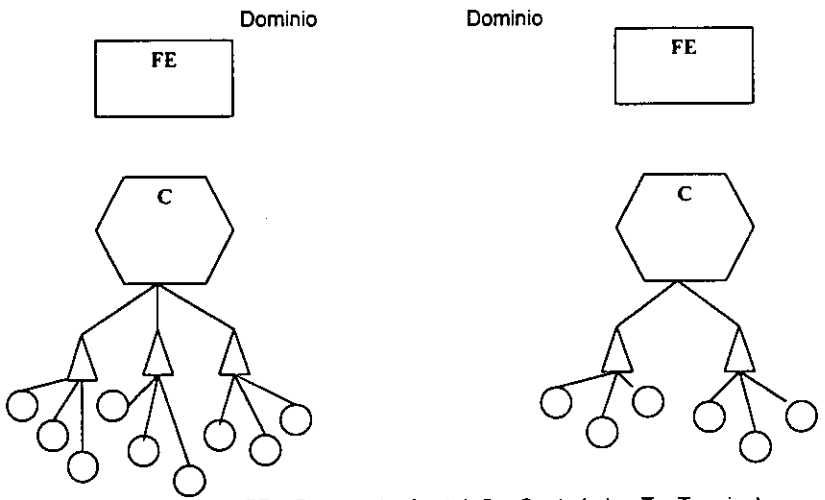
La SNA ha evolucionado considerablemente con el paso de los años y, en la actualidad, sigue evolucionando. Su primera versión en el año 1974 sólo permitía redes centralizadas, es decir, redes en forma de árbol con solo un host y sus terminales. Desde nuestro punto de vista, esto no puede considerarse en absoluto como una red. Su versión posterior, de 1976, ya permitía tener múltiples host con sus respectivos árboles, con la posibilidad de tener comunicación entre árboles, solamente a través de sus raíces. La versión de 1979 elimino esta restricción, teniendo ahora la capacidad de comunicarse de manera más general. Por último, en 1985, incluyo la aparición de topologías arbitrarias de host y LAN.

Una red SNA está constituida por una colección de máquinas denominadas nodos, de los cuales hay cuatro tipos, que se caracterizan aproximadamente de la manera siguiente. Los nodos tipo 1 son las terminales. Los nodos tipo 2 son los controladores, es decir, son las máquinas que supervisan el funcionamiento de las terminales y otros periféricos. Los nodos tipo 4 son los procesadores frontales, es decir, aquellos dispositivos cuya función consiste en reducir la carga del CPU principal y realizar el manejo de interrupciones asociadas con la comunicación de datos. Los nodos tipo 5 son los mismos host principales, aunque, con la aparición

de los microprocesadores de bajo costo, algunos controladores han adquirido algunas propiedades de los host. Curiosamente, no hay nodos del tipo 3.

Cada uno de los nodos contiene uno o más NAU (unidad direcionable de red, UDR), que son una pieza de software a través del cual se permite que un proceso utilice la red; puede considerarse como un SAP (punto de acceso del servicio), más las entidades que proporcionan los servicios de las capas superiores. Para usar la red, el proceso debe conectarse directamente a una NAU y, a partir de ese momento, puede dereccionarse y direccionar otras NAU. Las NAU son, por consiguiente, los puntos de entrada a la red para los procesos de usuarios.

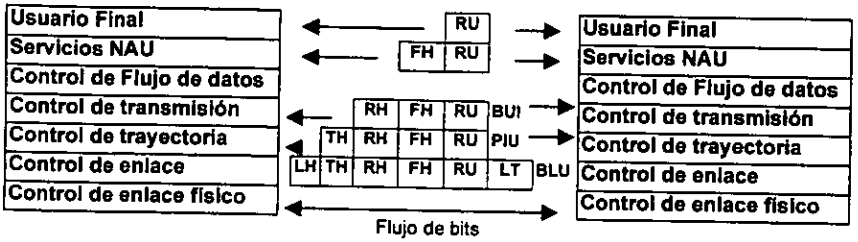
Hay tres tipos de NAU: el LU (unidad lógica, UL), es la variedad más común a la que se unen los procesos de usuario, el PU (unidad fisica, UF), es una NAU administrativa especial asociada con cada uno de los nodos. La red utiliza un PU para poner el nodo en línea, dejarlo fuera de línea, probarlo y ejecutar funciones parecidas a la administración de redes. Mediante el PU se proporciona una forma de direccionar en la red un dispositivo fisico, sin tener en cuenta los procesos que la están utilizando. El tercer tipo de NAU es el SSCP (punto de control en los servicios de sistema, PCSS), del que normalmente hay uno por cada nodo tipo 5 y ninguno en los otros. El SSCP tiene un conocimiento completo de, y a su vez control sobre, todos los procesadores frontales, controladores y terminales unidos o ligados al host. Se conoce como dominio al conjunto de hardware y software manejado por un SSCP; él la siguiente figura se describe una red SNA simple de dos dominios.



Una red SNA de dos dominios. FE = Procesador frontal, C = Controlador, T = Terminal

Aunque es posible llevar a cabo una correspondencia aproximada de las capas SNA con las capas del modelo OSI, si se observa con detalle, se puede apreciar que los dos modelos no tienen una correspondencia completa, especialmente en las capas 3, 4 y 5. A continuación se presenta un resumen de las capas de SNA.

La capa SNA localizada en la parte más baja de la arquitectura, mostrada en la siguiente figura, tiene a su cargo el transporte físico de los bits de una máquina a otra. Los protocolos que se utilizan en esta capa, generalmente son conforme a las normas industriales apropiadas.



LH = Cabecera de enlace
LT = Cola de enlace
TH = Cabecera de transmisión
RH = Cabecera de pregunta / respuesta
FH = Cabecera de función

BLU = Unidad de enlace básica (= trama)
PIU = Unidad de información de ruta (= paquete)
BIU = Unidad de información básica (= mensaje)
RU = Unidad de pregunta / respuesta

La siguiente capa, la capa de control de enlace, construye tramas a partir del flujo de bits original, detectando y recuperando errores de transmisión de una manera transparente para las capas superiores. Muchas redes han copiado, ya sea en forma directa o indirecta, su protocolo de capa 2, del protocolo de comunicación de datos de la capa 2 de la SNA, es decir, el SDLC (control de enlace de datos síncrono, CEDS). En particular, la configuración del HDLC (control de alto nivel para enlace de datos, CANED) de la ISO es muy parecido al SDLC. La SNA tambien soporta el mecanismo de acceso de paso de testigo en anillo de una LAN, en esta capa.

El objetivo de la capa 3 de la SNA, denominado por IBM como control de ruta, consiste en establecer una trayectoria lógica de la NAU frente a la NAU destino. Muchas redes SNA se encuentran divididas en subredes, denominadas subáreas, cada una de las cuales tiene un nodo especial de subárea que actúa como una pasarela. Con frecuencia, una subárea corresponde a un dominio. Este diseño conduce a una estructura jerárquica, con los nodos de subárea conectados conjuntamente para formar una red dorsal y cada uno de los nodos conectado a un nodo de subárea.

El control de la ruta está constituido por tres subcapas: la capa localizada en la parte superior, realiza el encaminamiento total, decidiendo que secuencia de subáreas deberá ser utilizada para ir de la subárea fuente a la subárea destino. A esta secuencia se le conoce como ruta virtual. Dos subáreas pueden quedar conectadas a través de diferentes tipos de líneas de comunicación (por ejemplo, utilizando una línea alquilada o satélite), de tal forma que la siguiente capa elige que línea especifica usar, generando así una ruta explícita. La capa localizada en la parte inferior, divide él trafico entre varios enlaces paralelos de comunicación, del mismo tipo, con objeto de alcanzar un mayor ancho de banda y una mayor fiabilidad.

La información relacionada con la determinación de rutas virtuales y explícitas, así como el manejo de la congestión de la red, se pasa en la cabecera de transmisión, como se muestra en la figura anterior. Con objeto de tener una mayor eficiencia, el control de ruta también puede agrupar paquetes de información que no tienen ninguna relación, en unidades más grandes.

La capa de control de transmisión, que esta localizada encima de la capa de control de ruta, tiene bajo su responsabilidad la creación, el manejo y la liberación de las conexiones de transporte (sesiones). Todas las comunicaciones en SNA utilizan sesiones y no soporta comunicaciones sin conexión. El propósito de la existencia de una sesión en la SNA, como en el caso del modelo OSI, consiste en proveer a las capas superiores con un canal libre de error que sea independiente de la tecnología del hardware de las capas inferiores.

En SNA se distinguen cinco tipos diferentes de sesiones:

1. SSCP – SSCP: para el control entre dominios y gestión de mensajes.
2. SSCP – PU: para permitir que el SSCP inicie, controle y pare al PU.
3. SSCP – LU: para hacer que el LU maneje sesiones.
4. LU – LU: para transmitir los datos del usuario.
5. PU: para la administración de redes.

En el modelo OSI, cualquier proceso puede enviar un mensaje a otro proceso que haya solicitado establecer una sesión. Si la parte solicitada acepta, envía una respuesta que establece la sesión. La situación en SNA es mucho más compleja y difiere para cada uno de los diferentes tipos de sesión. Aquí solo se considera el tipo de sesión usuario a usuario (es decir, LU – LU), como se muestra enseguida.

Para establecer una sesión, un proceso debe decírselo al gestor de control de sesiones de su dominio. Si el destino es local (en el mismo dominio), ésta se puede establecer directamente.

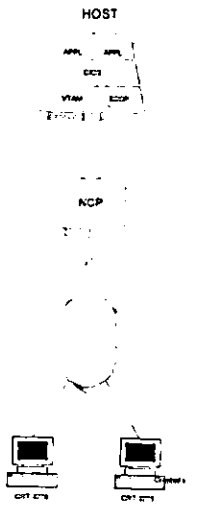
Sin embargo, si el destino está en un dominio remoto, el SSCP deberá contactar primero al SSCP correspondiente que controla el dominio distante. Las rutas virtuales y explícitas también se deberán seleccionar. Este mecanismo resulta ser bastante tedioso en su manejo, pues requiere el intercambio de alrededor de una docena de mensajes de control. Una vez que se establece la sesión, la capa de control de transmisión se encarga de regular la velocidad del flujo entre los procesos, de controlar las asignaciones de memoria, de administrar las prioridades de los mensajes, de manejar la multiplexión y demultiplexión de datos de mensajes de control, en beneficio de las capas superiores, así como de efectuar el cifrado y decodificación de mensajes, siempre que así se solicite.

El control de flujo de datos, que no tiene nada que ver con el control de flujo de datos en el sentido usual, se encuentra localizado encima del control de transmisión. En lugar de esto, el control de flujo de datos tiene como objetivo el seguimiento de que extremo de la sesión le corresponde hablar a continuación, suponiendo que el proceso quiere ese tipo de servicio.

Esta capa esta muy relacionada también con la recuperación de errores. Una característica que resulta poco común pero que es propia de la capa de control de flujo de datos, es la ausencia de una cabecera específica para comunicarse con el software correspondiente del otro extremo. En lugar de dicha cabecera la información, que normalmente se comunicara a través de ella, se pasa al control de transmisión como parámetros y se incluye en la cabecera de transmisión.

La sexta capa dentro de SNA, los servicios NAU, provee dos clases de servicios a los procesos de usuario. Primero, están los servicios de presentación, como la compresión de textos. En segundo lugar se encuentran los servicios de redes, que están relacionados con la operación de la red como un todo.

THE SNA NETWORK



4.2. ARQUITECTURA EN CAPAS DE SNA

System Network Architecture (SNA) es todo un diseño que permite la comunicación entre diversos productos desarrollados por IBM. SNA da las reglas para que diversos dispositivos, protocolos, funciones y conceptos dentro de la red puedan comunicarse y sean compatibles entre sí.

SNA se encarga de distribuir los mensajes generados por un dispositivo a través de la red, además de distribuir datos, SNA define direcciones, rutas y la secuencia de la información para que esta llegue a su destino.

SNA no es un producto de software, ya que su diseño esta basado en una variedad de software y hardware hechos por IBM.

1. Capa Transacción de Servicios

Contiene todos los servicios que las aplicaciones necesitan accesar (Bases de Datos, Intercambio de Documentos, etc.), la capa de transacción de servicios puede estar implementada en programas aplicativos o específicamente en servicios que son accesados por programas aplicativos.

2. Capa Servicios de Presentación

Formatea los datos de diferentes aplicaciones, para que puedan viajar a través de la red. Coordina los recursos compartidos, la capa de presentación corre dispositivos independientes para formatear datos, maneja interfaces para comunicaciones entre programas.

3. Capa Control de Flujo de Datos

Controla la dirección del flujo de datos, maneja niveles de sesiones en la red, maneja y controla errores y asigna números de secuencia a los paquetes de datos.

4. Capa Control de Transmisión

Da secuencia a los paquetes de datos, mide el intercambio de datos entre puntos de la red para determinar y dar confianza a la capacidad de procesamiento de datos, también encripta datos si la seguridad es requerida.

5. Capa Control de Ruteo

Rutea los datos entre el emisor y receptor, controla él trafico a través de la red, las funciones de enrutamiento van desde pasar datos de un nodo a otro en la red

hasta tener una ruta punto a punto de aplicaciones, también se encarga de segmentar y poner en bloques la información, respetando el tamaño de bloque que el protocolo requiera.

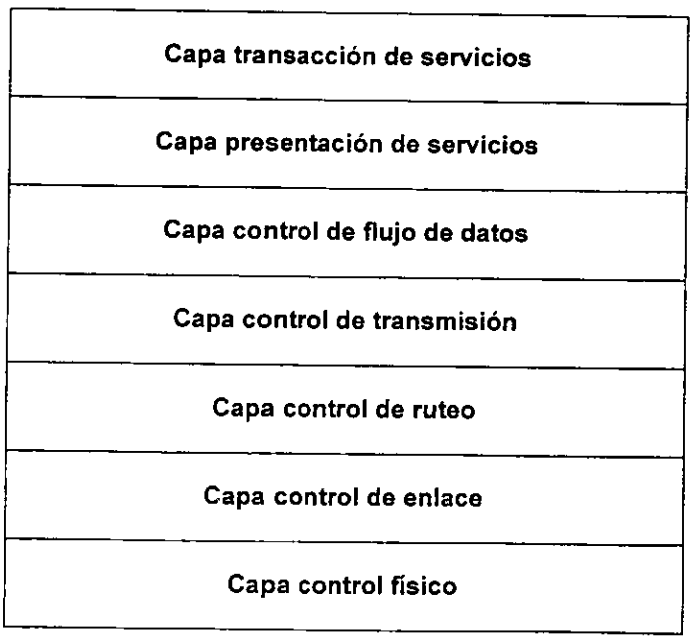
6. Capa Control de Enlace

Transmite los datos entre nodos adyacentes. La capa de enlace se encarga del control de flujo de datos, detecta y corrige errores con ayuda de los protocolos.

7. Capa Control Físico

Conecta física y eléctricamente nodos. La capa física define los estándares mecánicos de conectores, los estándares eléctricos de los conectores y la señalización.

Arquitectura en capas de SNA



4.3. COMPONENTES DE LA RED SNA

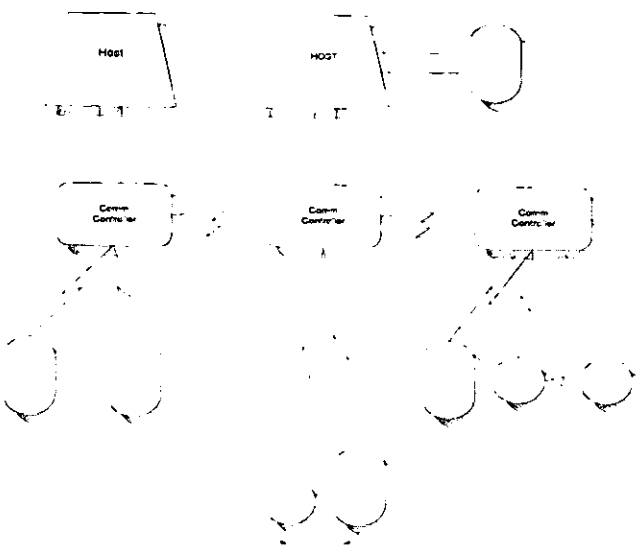
Host. Las redes SNA están constituidas por los host, que son los procesadores de datos. Los Host soportan métodos de acceso de comunicación, puntos de control de red y a los usuarios finales.

Usuarios finales. El término usuario final hace referencia a una terminal de la computadora, al operador de la misma o a un programa de aplicación. En los tres casos se hace referencia a una entidad que interactua con la red, que usa los servicios de la misma con un propósito definido, principalmente, el intercambio eficiente de datos con otro usuario final. El usuario final no forma parte de la red sino que se sirve de ella; es emisor y receptor de datos.

Controladores. Hay dispositivos que soportan la comunicación con las redes SNA y dan acceso al usuario final de la red. El más común es el cluster o controlador 3270 el cual da conexión a la red a impresoras y terminales, también puede dar acceso a programas o aplicaciones corriendo desde los Host. La función de los controladores de comunicación es administrar el flujo de datos entre un Host y terminales remotas. En una red SNA los datos pueden pasar a través de uno o varios controladores antes de llegar a su destino final.

La función de los controladores de comunicación es administrar el flujo de datos entre un host y terminales remotas. En una red SNA los datos pueden pasar a traves de uno o varios controladores antes de llegar a su destino.

CHARACTERISTICS OF THE SNA NETWORK



4.4. CLASIFICACIÓN DE NODOS

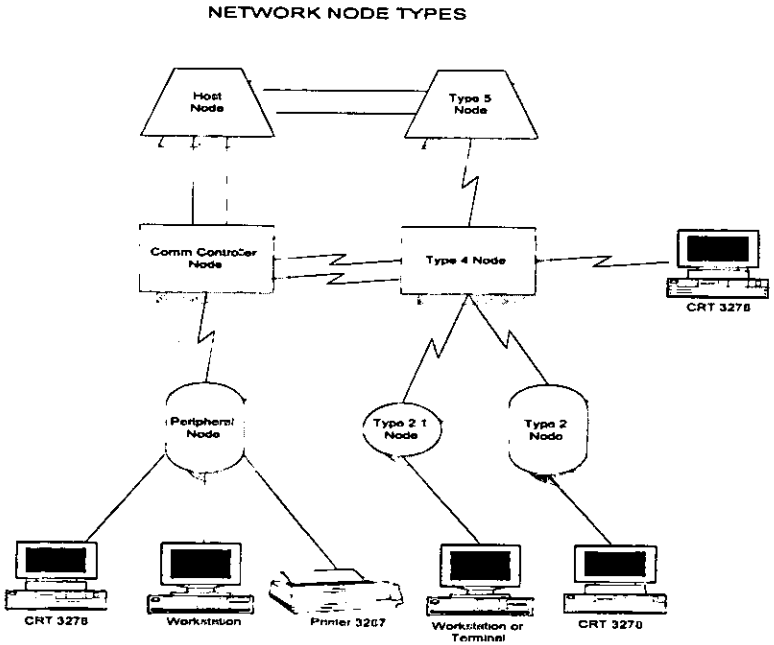
Una red SNA esta constituida por una conexión de máquinas denominadas nodos que son una colección de uno o varios puntos de liga de la red de los cuales hay cuatro tipos que se caracterizan de la manera siguiente:

Nodos tipo uno son los terminales.

Nodos tipo dos son los controladores, es decir, son las máquinas que supervisan el funcionamiento de los terminales y otros periféricos.

Nodos tipo cuatro son los procesadores frontales, es decir, aquellos dispositivos cuya función consiste en reducir la carga del CPU principal y realizar el manejo de interrupciones asociadas con la comunicación de datos.

Nodo tipo cinco o nodo HOST, las principales funciones del nodo host son el control de recursos de red, correr aplicaciones de otro sistema, además de dar al usuario final acceso a las comunicaciones de red.



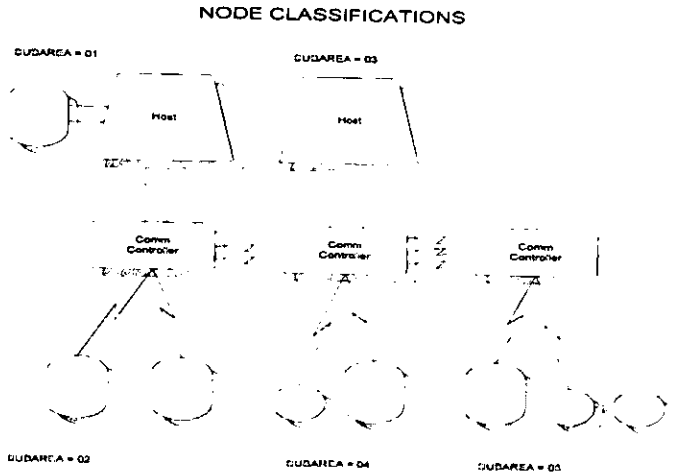
SNA define como una subarea al conjunto que forman un host y todos los periféricos y dispositivos conectados a este, también una subarea puede ser un controlador de comunicaciones y todos los periféricos conectados al mismo.

El concepto de subarea se utiliza para asignar una única dirección por nodo y así facilitar la administración y el ruteo en la red.

Un Host subarea node, es un procesador que contiene un método de acceso por telecomunicaciones (ACF/VTAM). La función del host subarea node es administrar una porción o toda la red SNA.

Un Nodo Controlador de Comunicaciones, contiene un programa de control de red (ACF/NCP). Su función es controlar y rutear al flujo de datos en la red.

Los elementos restantes de una red SNA son llamados nodos periféricos, los nodos periféricos pueden ser dispositivos o terminales, tales como: cluster de control, departmet processors, estaciones de trabajo e impresoras. El propósito de los nodos periféricos es dar servicio o soportar a los usuarios finales.

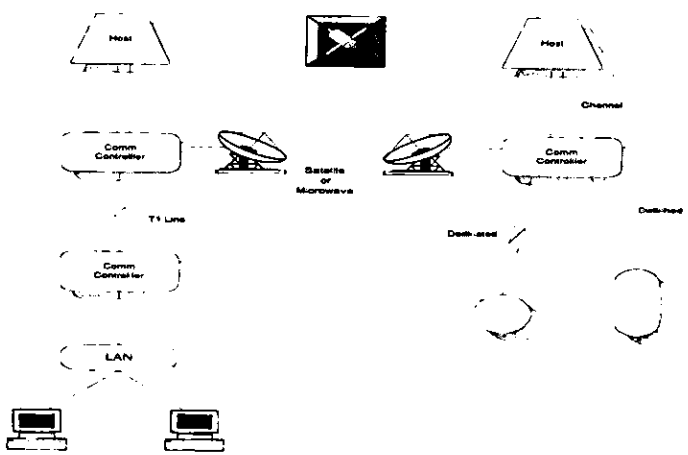


Ligas de Datos. Una liga física conecta 2 nodos adyacentes en la red. Una liga es el medio físico de transmisión de datos entre nodos. Los protocolos asociados a una liga de datos sirven para la transmisión de datos, el manejo de flujo de datos, además de detectar y corregir errores.

Hay 3 tipos de Protocolos de liga de Datos

- Synchronous Data Link Control (SDLC): Es un protocolo serial bit a bit y es independiente del medio de transmisión, medios como las líneas telefónicas, satélite o microondas pueden utilizar SDLC.
- Sistema de Canal 370 I/O. Es un sistema de transmisión en paralelo de alta velocidad. Este es usado para conectar los host con los controladores de comunicación. Mientras el canal da una alta velocidad de transmisión, la liga física entre componentes esta limitada en la distancia.
- La red Token Ring: Es una LAN de alta velocidad, la cual permite conectar dispositivos de una red LAN a una SNA pasando por los controladores de comunicación, como es de alta velocidad, la restricción es de distancia.

SNA DATA LINKS

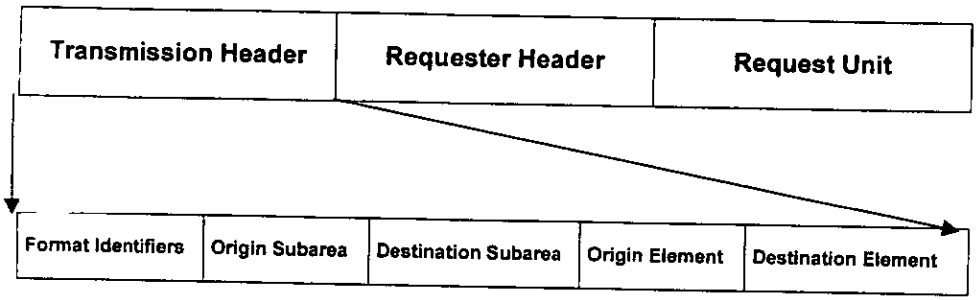


* Synchronous Data Link Control (SDLC)
* System/370 I/O channel
* Token ring network

4.5. DIRECCIONES EN LA RED

Para el control y el correcto ruteo de información a través de la red, se debe asignar a cada elemento una única dirección. Los recursos asignados a esa única dirección son llamados Network Address Units (NAU's), que son una pieza de software a través del cual se permite que un proceso utilice la red; para usar la red el proceso debe conectarse directamente a una NAU y a partir de ese momento, puede direccionarse a otra NAU, por esto son consideradas los puntos de entrada a la red para los procesos de usuario.

La comunicación entre NAU's se realiza con la ayuda de un formato de mensaje llamado Path Information Unit (PIU). Los PIU están formados por un Header de transmisión, un Header de requerimiento/respuesta y la unidad de requerimiento, la información de dirección de red esta contenida en el Header de transmisión del PIU, un ejemplo del PIU se muestra a continuación:



NAU (Network Addressable Units).

- Habilita a los usuarios para enviar datos
- Se utiliza para identificar el destino de los datos
- Se utiliza para controlar y administrar funciones
- Se asignan cuando el sistema es arrancado

Network subarea address

- Identificador único en la red
- Suelen ser la dirección para todos los recursos de toda la subarea
- Se utilizan para rutear datos entre subareas

Element address

- Identifica cada recurso en la subarea
- Se utiliza para rutear datos dentro de las subareas

Local address

- Identifica recursos dentro de los nodos periféricos
- Identifica origen/destino de los datos

Los recursos de la red están identificados por NAU's que son asignadas cuando el sistema es generado. Las direcciones son usadas para rutear datos desde un origen hasta un destinatario final en la red.

Hay tres niveles de direccionamiento:

- ***Dirección de Subárea***. Son asignadas a todos los Host y a todos los controladores de comunicación. Los campos de origen y destino de subáreas son de cuatro bytes de longitud, las direcciones de subárea son usadas por todos los recursos de la red dentro de la subárea, así que, esta dirección sirve para referenciar recursos entre subáreas.

- ***Dirección de Elemento***. Identifica recursos dentro de una subárea el campo de dirección de elemento tiene 16 bits y permite definir hasta 65536 elementos dentro de una subárea. Cada recurso es identificado por su dirección de subárea y su dirección de elemento. La dirección de elemento solo se usa para rutear datos dentro de la misma subárea.

- ***Dirección Local***. Únicamente identifica recursos en un nodo periférico. La dirección local es solo utilizada por el nodo periférico para rutear datos de usuario desde la red hacia el recurso local.

Cada NAU puede dar servicios a uno o más usuarios finales, los cuales pueden ser programas, operadores en terminales o una combinación de ambos. Hay tres tipos de NAU's:

- ***Logical Units (LU)***. Dan al usuario final acceso a los recursos de la red, y administran la transmisión de información entre usuarios finales. Una LU puede ser un subsistema de aplicación (los llamados CICS, IMS) o la programación lógica asociada con un dispositivo independiente o un subsistema terminal.

El tipo de unidad lógica define un subconjunto de protocolos en capas soportadas por programas de aplicación durante una sesión, así las características de cada tipo de LU son:

- ***LU tipo cero***. Se le llama de extremo abierto porque es definida por el producto que vincula. Su función es la de interconectar dos programas o aplicaciones que intercambien datos entre si, la característica principal es que los programas pueden o no estar dentro de los estándares de SNA.

- ***LU tipo 1***. Se refiere al flujo de datos entre una terminal y un programa.
- ***LU tipo 2***. Une un programa con una terminal que despliega mensajes.
- ***LU tipo 3***. Permite que un programa se comunique con una impresora.
- ***LU tipo 4***. Permite que un programa se comunique con uno o varios workstation, transfiriendo datos en línea o batch.
- ***LU tipo 6.2*** Permite la transferencia de datos entre dos aplicaciones. Las aplicaciones pueden corren en 2 nodos tipo 5 (procesos host), en un nodo tipo 5 y en otro nodo tipo 2.1 (nodos periféricos).

Los LU 6.2 están conformados por una serie de servicios, protocolos y formatos para comunicarse entre LU´s, la comunicación se basa en un software llamado Advanced Program-to-Program Communication (APPC). Los LU tipo 6.2 están desarrollados para procesar transacciones en línea, distribuir en toda la red accesos a las bases de datos y también a la transferencia de archivos y aplicaciones.

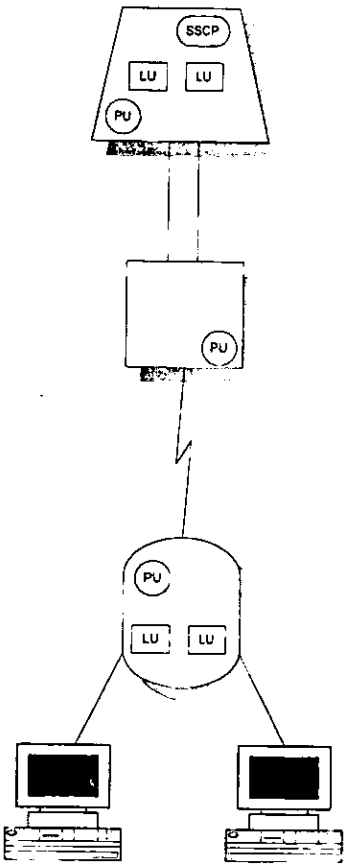
Para poder comunicar aplicaciones con el LU 6.2 se requieren dos pares de estos, más de una aplicación o programa pueden compartir la conexión de LU 6.2.

- ***Physical Units (PU)***. Representa las propiedades físicas que tiene el producto respecto a la red. Un PU no es un dispositivo físico, sino que es un conjunto de componentes SNA que provee servicios para controlar enlaces, terminales, controladores y procesadores de la red. Los PU están localizados en los nodos y administran los recursos de los mismos, activando y desactivando a la propia máquina y a cada enlace proveyendo acceso a otros nodos SNA. Los PU son implementados como una combinación de software y hardware, por ejemplo, en un Host existe un software llamada CM (Comunication Access Method) y necesita de un hardware de administración de red.

  - ***PU tipo 5***. Representa un nodo central (Host) y debe contener un PU, un LU y un SSCP
  - ***PU tipo 4***. Hace referencia a un nodo que contiene un software de control de encaminamiento (PC), una PU y LU's opcionalmente.
  - ***PU tipo 2.*** Se refiere a un nodo final con funciones de ruteo limitadas, generalmente es un dispositivo que controla un grupo de terminales, debe contener una PU y varias LU's.
  - ***PU tipo 1***. Son dispositivos simples, de dirección única y de bajo costo ya que contienen un PU y opcionalmente un LU, se les conoce como dispositivos pre-SNA.

- ***System Services Control Point (SSCP).*** Es el punto central de control en una red SNA. El SSCP solo puede residir en el Host Subarea Node.

NETWORK ADDRESSABLE UNITS



*Logical Units

4.6. TIPOS DE SESIONES EN LA RED SNA

Una sesión es una conexión lógica entre NAU's , el propósito de una sesión es el intercambio de datos y el control de información. Antes de que una NAU pueda comunicarse con otra se deben seguir ciertas reglas de conexión y de sesión. Hay cuatro tipos de sesiones para poder intercambiar datos en SNA:

- ***Sesión SSCP-SSCP.*** System Services Control Point ejecuta funciones de administración en la red, es responsable de arrancar y detener la comunicación en la red y principalmente de establecer sesiones con LU's y PU's, están configurados en la porción de red bajo su control. La función de red bajo el control de un SSCP se le llama dominio, a lo largo de la red pueden existir uno o más SSCP compartiendo la responsabilidad de controlar y supervisar operaciones de la red, a esto se le llama múltiple dominio de la red. La sesión SSCP - SSCP se establece entre dos SSCP para empezar o detener sesiones entre LU's en diferentes dominios o en diferentes redes. Un ejemplo puede ser un usuario final introduciendo datos o pidiendo acceso a una aplicación que se encuentra en un diferente Host al suyo.

- ***Sesión SSCP-PU.*** Esta sesión se establece entre un SSCP y un PU permitiendo que el SSCP envie requerimientos, reciba respuestas y pida información del estatus de los nodos de la red. Una vez que el nodo ha sido activado por el NCP (Network Control Program), el SSCP establece la sesión con el PU del nodo. El nodo se activa cuando la sesión SSCP - PU ha sido establecida. Una vez que el nodo ha sido activado el resto de la sesión puede ser establecido.

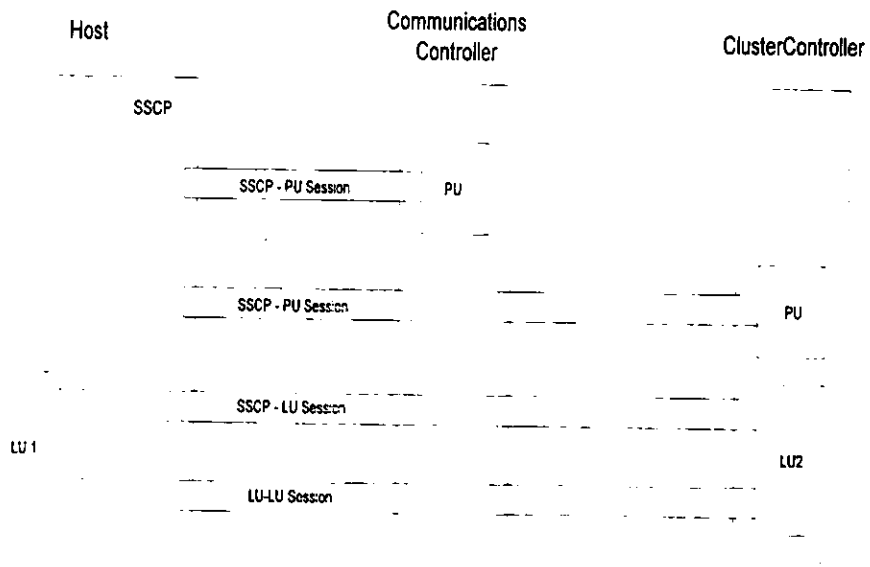
- ***Sesión SSCP- LU.*** El SSCP establece una sesión con el LU Para habilitar al LU a enviar requerimientos de inicio de sesión con otro LU.

- ***Sesión LU - LU.*** Las sesiones entre dos LU's permite la comunicación entre dos usuarios finales. Un usuario final puede ser un operador introduciendo datos en la red para actualizar una base de datos, o bien también el usuario final puede ser un programa que este actualizando la base de datos. La sesión LU - LU que interactua con uno de estos usuarios finales es llamada half session. Cuando la sesión es establecida una de las half session es designada la PLU (Primary Logical Unit) y la otra es la SLU (Secundary Logical Unit). Cuando la sesión LU - LU es establecida esta se regirá por una serie de reglas (protocolo) que definirá los parámetros de la sesión, esta serie de reglas es enviada en un comando BIND desde el PLU hasta el SLU; la sesión comienza a operar cuando la SLU envía de regreso una respuesta positiva hacia el PLU.

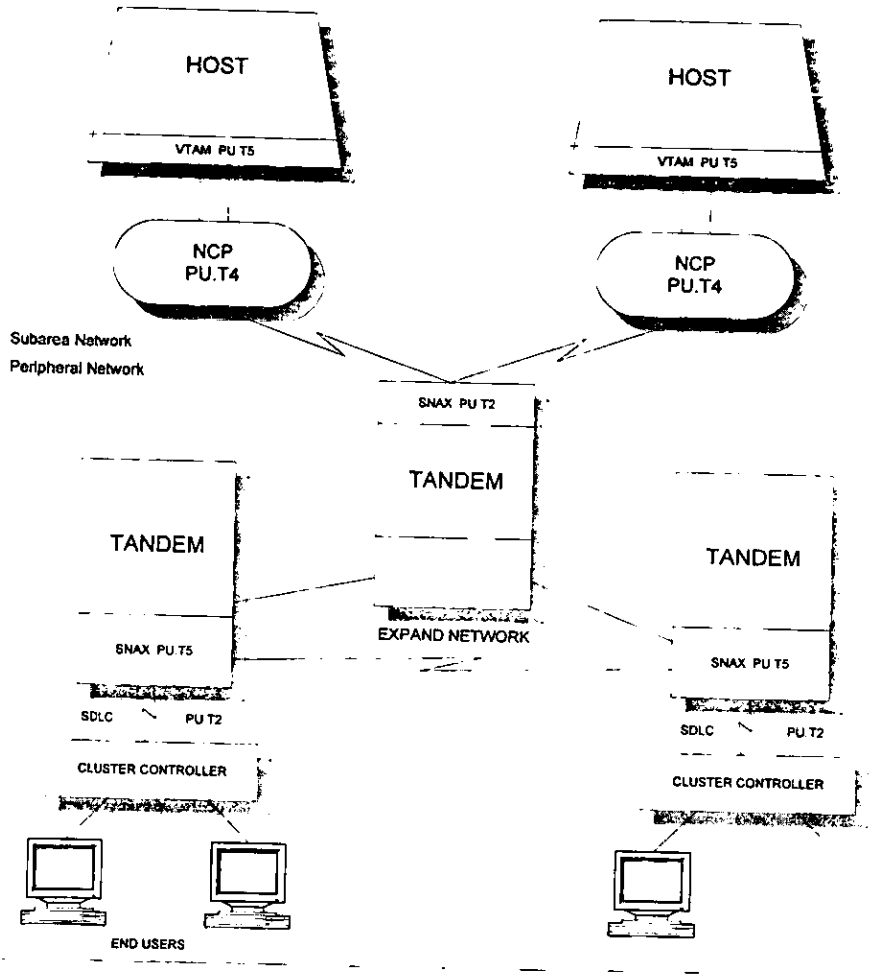
Para establecer una comunicación que permita intercambiar datos en una red SNA se deben seguir ciertos pasos de manera jerárquica.

1. El SSCP debe activar el PU del Host en el cual reside.
2. Se debe establecer una sesión SSCP - PU con el control de comunicaciones local.
3. Se hace una liga con el PU del nodo periférico remoto quedando establecida una sesión SSCP - PU remota.
4. La LU del remota del nodo periférico establece una sesión SSCP – LU.
5. Cuando la LU remota responde al SSCP, la PLU se conecta con SSCP.
6. La PLU le envía a la SLU las reglas que gobernaran la sesión LU - LU en un comando BIND.
7. Si la SLU acepta las reglas la sesión LU - LU se establece y el trafico de datos empezara a fluir a través de la red.

SESSION ESTABLISHMENT HIERARCHY



TANDEM IN AN SNA NETWORK



Capitulo 5. SNAX/APC

Para que un usuario pueda tener acceso a una red SNA debe estar provisto de un proceso que lo atienda y actué como intermediario entre las peticiones que este requiera y el acceso a procesos que atiendan sus peticiones. Los TP's (Transaction User) son aplicaciones o programas que ejecutan operaciones para los usuarios finales. Pero también estos usuarios pueden requerir hacer uso de aplicaciones fuera de la red de SNA. SNAX/APC permite que aplicaciones corriendo fuera de SNA (ejemplo TANDEM) puedan comunicarse con los recursos de la red SNA, para esto solo se requiere que SNA soporte LU's (Logical Units) del tipo 6.2.

SNAX/APC nos permite hacer conexiones entre TP's corriendo en una red TANDEM y TP's corriendo en una red SNA, para esto SNAX provee a los TP de protocolos para la comunicación en las capas inferiores, pero a la vez mantiene los beneficios de estos protocolos disponibles para la programación de aplicaciones dentro de la red de TANDEM dando una interface de alto nivel.

Por ejemplo. Un TP corriendo en una red Tandem puede hacer uso de SNAX para pedir acceso aun TP corriendo en un sistema IBM. SNAX busca alojarse en una LU disponible en la TANDEM, estableciendo la conexión con la LU 6.2 que se encuentra remota, una vez establecida la comunicación se puede ejecutar todas las ventajas que proporciona la red SNA, incluyendo el administrador de errores y la función de terminación de sesión.

SNAX da servicios asociados con las capas inferiores de SNA como son: La capa de Transmisión y control, la capa de control de flujo de datos, la de servicios de presentación, la que se encarga de administrar los LU y la de control de puntos de servicios.

5.1. CONCEPTOS BÁSICOS

Cuando un programa empieza a comunicarse con una red SNA, lo primero que debe hacer es establecer comunicación con un dispositivo lógico dentro de la red SNA, este dispositivo es llamado logical Unit (LU); Una sesión LU-LU es establecida cuando el programa emisor indica que esta buscando comunicarse con otro programa dentro de la red SNA. El programa receptor también debe estar conectado a su propio LU. Los LU son identificados así: el LU que pide conexión es llamado LU primario y el otro es el LU secundario, un LU primario puede

establecer una sesión LU-LU emitiendo un requerimiento a la red SNA llamado BIND, y el LU secundario debe responder que acepta la petición contestando con un INIT-SELF. Cuando el BIND es reconocido positivamente la sesión LU-LU esta lista para comunicarse.

Después de establecer una sesión LU-LU entre cada par de TP's que necesitan comunicarse, LU 6.2 crea una LU-LU sesión entre los dos sistemas para posteriormente intentar crear una LU-LU sesión que pueda ser reutilizada por cada TP, a este tipo de conexión compartida se le denomina conversación. Los dos TP's que se encuentran en conversación tiene el uso exclusivo de su sesión LU-LU, y una vez que terminan de utilizarlo lo liberan dejándolo disponible para otro par de TP's.

5.2. ELEMENTOS DE COMUNICACIÓN DE SNAX/APC

Los TP's se comunican con SNAX/APC usando una herramienta propia del sistema Tandem que esta hecha basado en mensajes orientados, llamada message-oriented aplication program interface. La unidad básica de este sistema se le denomina IPC (Interprocess Comunication), cada mensaje IPC empieza con un IPC header el cual contiene información acerca del mensaje, seguido del header un IPC contiene uno o más UOWs (SNAX/APC Units of Work).

Los UOW son estructuras de mensajes que identifican el requerimiento de una operación y dan la información necesaria para este requerimiento. Por ejemplo un UOW se usa para pedir acceso a una aplicación del Host, o para recibir algún mensaje desde el Host, o también para confirmar la que una transacción se completo exitosamente. Los UOW pueden ser verbos para petición de tareas o para contestar requerimientos.

Varios UOW pueden ser concatenados en un solo mensaje IPC, reduciendo con esto el tráfico de mensajes en la red y subir la eficiencia del sistema. Todos los UOW que estén dentro de un IPC son validados antes de que sean procesados. Por ejemplo Un mensaje IPC puede estar conformado de la siguiente manera:

ALLOCATE	SEND-DATA	SEND-DATA	CONFIRM

En este ejemplo se muestra una serie de UOW que en conjunto harían la petición de WRITE-READ (leer-escribir).

Las respuestas desde SNAX/APC son manejadas en forma similar que las peticiones, basándose en UOW. Un IPC de respuesta contiene un UOW de respuesta por cada UOW de petición. SNAX procesa los UOW de petición en el orden en que aparezcan en el IPC, y por lo tanto los UOW de respuesta aparecerán en el mismo orden.

Cada UOW de respuesta tiene un header estándar que indica un código de respuesta. El código de respuesta identifica el estado que le corresponde a cada UOW de petición. Por ejemplo el código RC_OK (0) indica que el requerimiento dado fue completado satisfactoriamente.

Para la administración de los UOW se han clasificado en tres:

UOW de servicio
UOW de control de operación y
UOW de conversación.

UOW de servicio. Sirven para inicializar, limpiar y distribuir funciones entre los componentes de SNAX. No son parte del set de funciones de LU 6.2.

DISPLAY - STATUS	Obtienen información acerca de los LU locales que están controlados por algún proceso de SNAX/APC. Por ejemplo información sobre sesión y conversación de algún verbo que se este ejecutando
TP -READY	Inicializa la comunicación con el SNAX/APC local y algún LU local, esto para establecer una instancia al TP
TP -END	Libera todos los recursos que un TP-READY le asigno a un TP, en resumen cancela la operación de TP-READY. Un TP local debe invocar un TP-END cuando ha completado la ultima conversación asociada a un TP-READY, y con esto se destruye la instancia del TP.

UOW de control de operación. Estos UOW si se encuentran incluidos en el protocolo LU 6.2. Los UOW de control y operación sirven de ayuda para el control de los LU. A continuación se enlistan los verbos básicos de conversación.

ACTIVATE-SESION	Activan una sesión LU-LU entre un LU local y un LU vecino especificado. Un TP puede utilizar este verbo para establecer todas las sesiones entre LU´s antes de que la aplicación del TP empiece a requerir servicios de SNAX/APC.
DEACTIVATE-SESION	Desactiva una sesión LU-LU.

UOW de conversación. Los TP's utilizan los verbos de conversación para comunicarse con SNAX/APC. SNAX procesa los verbos de petición y regresa el estado del verbo de petición en mensaje de respuesta.

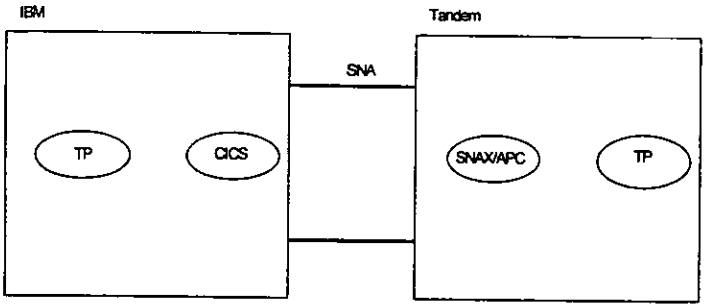
ALLOCATE	Establece comunicación con un TP remoto. Un TP que invoca un ALLOCATE es llamado TP origen y siempre iniciara en estado de send. El otro TP es llamado TP receptor y siempre empezara en estado de receive.
CONFIRM	Es un requerimiento que el TP remoto envía para la confirmación de algún evento o acción, por ejemplo el de recepción de datos.
CONFIRMED	Es la respuesta a un CONFIRM, indicando que el evento o la acción ha sido ejecutado.
DEALLOCATE	Termina una conversación con el TP remoto.
FLUSH	Transmite el contenido de los LU's locales, enviando su buffer al TP remoto.
GET-ATTRIBUTES	Consultas para el SNAX/APC local pidiendo información acerca de los atributos de conversación.
PREPARE-TO-RECEIVE	Prepara al TP local para recibir datos, además de cambiar el TP local de un estado de send a un estado de receive.
RECEIVE-AND-WAIT	Espera y recibe información del TP remoto.
RECEIVE-INMEDIATE	Recibe cualquier información que este disponible del TP remoto sin esperar que otra información llegue.
REQUEST-TO-SEND	Se indica al TP remoto que el TP local tiene datos a enviar
SEND-DATA	Envía datos al TP remoto.
SEND-ERROR	Reporta un error del TP local al TP remoto.

5.3. TIPOS DE CONVERSACIÓN

Una conversación puede ser iniciada por el TP local o por el TP remoto. Con SNAX/APC, los TP's pueden iniciar la conversación o esperar hasta que sus servicios sean requeridos por un TP remoto.

A continuación se exponen tres ejemplos para comprender el inicio de conversaciones.

El sistema Tandem es conectado al Host de una IBM que cuenta con una red SNA. Un TP es arrancado por Tandem, y una aplicación CICS es arrancada por IBM.

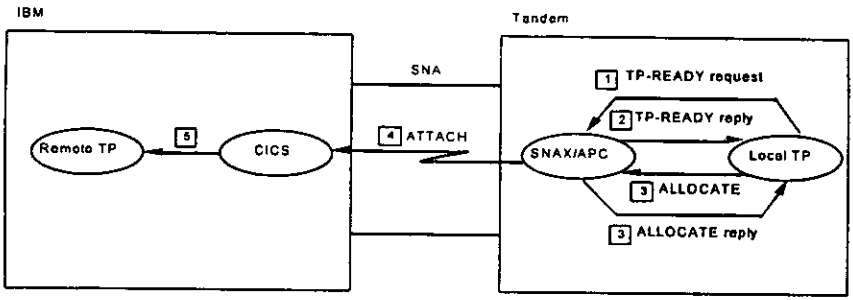


Ambiente inicial de SNA

En nuestro primer ejemplo un TP local (sistema Tandem) necesita tener acceso a una base de datos que se aloja en el CICS de IBM; por tanto el TP local es el que inicia la conversación.

1. El TP local envía un requerimiento TP-READY hacia el proceso de SNAX/APC. Este TP-READY le indica al LU de SNAX/APC que TP esta arrancando la comunicación
2. SNAX/APC contesta con un TP-READY en el cuál indica la creación de una instancia TP.
3. EL TP envía un requerimiento ALLOCATE hacia SNAX/APC, especificando hacia que TP remoto es la petición. Si la sesión LU-LU no existe, SNAX/APC la puede inicializar.
4. Cuando el proceso de SNAX/APC esta listo para transmitir datos hacia el TP remoto, envía un requerimiento llamado SNA ATTACH hacia el LU 6.2 remoto. (Un ATTACH es un comando de SNA el cual se envía al LU, indicando el nombre del TP remoto con el cual el TP local quiere comunicarse).
5. El LU remoto recibe el ATTACH y lo asocia con el TP remoto.
6. Después el LU remoto envía la respuesta ATTACH a SNAX/APC, y este a su vez envía la respuesta del ALLOCATE al TP remoto.

Cuando el TP local recibe la respuesta del ALLOCATE, este puede seguir enviando datos hacia el TP remoto usando el verbo SEND-DATA. El SEND-DATA puede ser enviado en el mismo mensaje IPC donde se envió el verbo ALLOCATE.



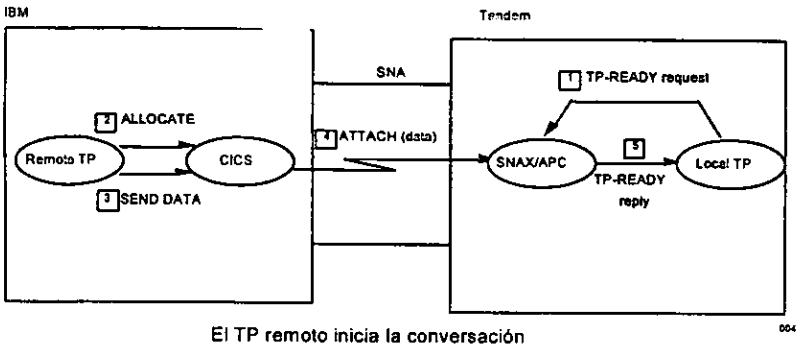
Iniciando Conversación

Para nuestro segundo ejemplo el proceso de SNAX/APC puede recibir un ATTACH desde un TP remoto de dos maneras.

a) Que el TP local exista y espere por un ATTACH desde el TP remoto.
b) Que el TP local no exista pero pueda ser creado por un DISPACHER una vez que se reciba el requerimiento ATTACH del TP remoto.

La siguiente figura ilustra la situación cuando el TP local ya existe.

1. SNAX/APC recibe un TP-READY desde el TP local indicando que espera un ATTACH desde el TP remoto. EL proceso de SNAX/APC verifica si ya había recibido la petición de ATTACH, si no ha recibido aun la petición pone el requerimiento de TP-READY en una pila de requerimientos interna.
2. SNAX/APC recibe un ATTACH del LU que recibió la petición, en este se especifica el TP destino; en este momento SNAX/APC saca de la pila el TP-READY de requerimiento y envía un TP-READY de respuesta el TP local. Si por alguna causa SNAX/APC recibe el ATTACH remoto antes de que el TP local le envie su TP-READY, se guarda el ATTACH en la pila de requerimientos hasta que el TP-READY sea invocado.
3. El TP local invoca un verbo RECEIVE-AND-WAIT para los datos del TP remoto.
4. El verbo RECEIVE-AND-WAIT es completo cuando SNAX/APC recibe los datos del TP remoto.

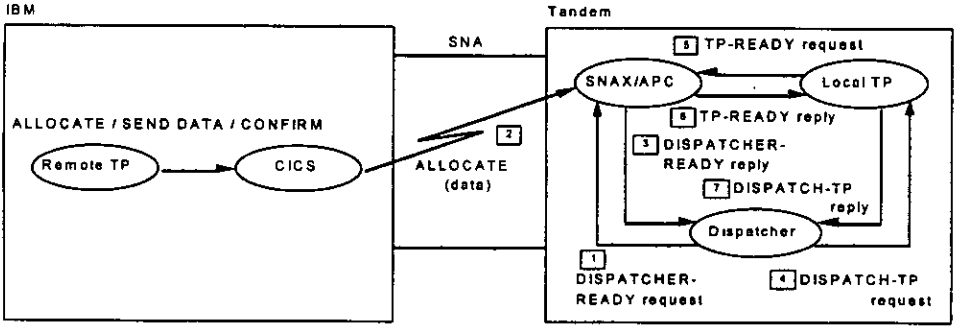


El TP remoto inicia la conversación

En el tercer ejemplo SNAX/APC entablara la comunicación con la ayuda de un administrador de procesos llamado DISPATCHER dentro de un ambiente PATHWAY. Este tipo de comunicación solo funciona cuando el requerimiento proviene del TP remoto.

1. En este caso el que inicia una parte de la comunicación es el propio SNAX/APC, ya que este arranca la parte del despachador. Una vez que el DISPATCHER se arranco este envía un DISPATCHER-READY hacia SNAX/APC, esto le permite a SANX/APC conocer que dispatcher esta disponible para arrancar un TP server. SNAX/APC guarda la petición de DISPATCHER-READY hasta que recibe un ATTACH desde el server remoto para el TP local.
2. Cuando SNAX/APC recibe el ATTACH por parte del LU buscando comunicarse con el TP local (El TP local aun no existe). SNAX/APC guarda el requerimiento ATTACH hasta que recibe un TP-READY del TP local.
3. SNAX/APC saca el requerimiento DISPATCHER-READY y envía una respuesta de DISPATCHER-READY hacia el DISPATCHER, esta respuesta lleva como información el nombre del TP que fue invocado.
4. EL DISPATCHER usa la información para crear un verbo de requisición DISPATCH-TP, el cual es enviado hacia el TP local. Si el TP existe y además tiene alguna liga disponible, el TP recibe el DISPATCH-TP, de lo contrario, PATHWAY crea un nuevo TP para que pueda recibir el DISPATCH-TP.

5. Cuando el TP local recibe el DISPATCH-TP, utiliza la información de este para abrir una sesión correcta de SNAX/APC y formar un requerimiento TP-READY. Este TP-READY sirve para indicar que no se trata de un ATTACH local y que el TP que envió el TP-READY fue creado por el DISPATCHER.
6. Cuando SNAX/APC recibe el TP-READY, saca el ATTACH que tenia en espera y envía una contestación de TP-READY al TP local. En este momento el TP local debe invocar el verbo RECEIVE-AND-WAIT para estar listo de recibir información desde el TP remoto.
7. Cuando la conversación llega a su fin, el TP local debe enviar un DEALLOCATE para liberar su parte de la comunicación, a la vez de enviar la respuesta del DISPATCH-TP al DISPATCHER.

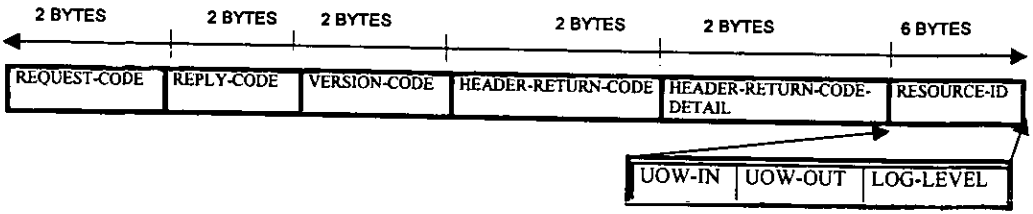


Comunicación con ayuda de un despachador

5.4. ESTRUCTURA DE LOS MENSAJES IPC

La unidad elemental de comunicación entre un TP y SNAX/APC es el Inter-Process Comunication (IPC). Los IPC contienen un header y uno o varios SNAX/APC Units of Work (UOW), solo en peticiones como TP-READY y el DISPLAY-STATUS los IPC solo pueden contener estos UOW.

El header del IPC es una estructura de datos que contiene información que identifica el requerimiento de un TP hacia el proceso de SNAX/APC.



Estructura del header de un mensaje IPC

REQUEST-CODE. Este campo indica las condiciones de procesamiento del requerimiento del TP. Solo es permitido el valor -2 (stop-on-error), que le indica a SNAX /APC que detenga el procesamiento si encuentra error en algún UOW.

REPLY-CODE. Indica las posibles respuestas que SNAX/APC da al TP.

Posible Valor	*Significado*
0 (All-Uows-ok)	Todos los UOW fueron procesados correctamente. Las respuestas de los IPC incluyen un Header IPC de respuesta, los header de las respuestas de los UOW y los datos de respuesta de los UOW.
2 (Uows-With-Error)	SNAX/APC detecto una condición de error mientras procesaba una petición de un UOW. La respuesta del IPC se conforma por el header del IPC, los header de respuesta de cada UOW y los datos de respuesta (incluyendo la información del UOW con error).
3 (Request-error)	SNAX/APC detectó un error en: el header del IPC, algún header UOW, el procesamiento de algún mensaje IPC. Ningún UOW es procesado. La respuesta del IPC trae solo el header de respuesta.

VERSION-CODE. En la petición como en la respuesta este campo contiene la versión de SNAX/APC usada. Este campo debe contener el valor de S1. Para futuras versiones de SNAX/APC este campo debe usarse para indicar capacidades de la nueva versión.

HEADER-RETURN-CODE. En un verbo de petición hacia SNAX/APC este campo es ignorado. En una respuesta SNAX/APC lo llena solo cuando el campo REP-CODE tiene el valor de 3 (request-error).

Posible Valor	*Significado*
0 (Ipc-ok)	SNAX/APC regresa este valor si el valor del REPLY-CODE es 0 o 2
1 (Invalid-version-code)	Este código indica que el valor del campo VERSION-CODE no fue reconocido por SNAX/APC.
2 (Invalid-resource-id)	SNAX/APC no reconoce el RESOURCE-ID en el momento. Esto es porque tal vez se invoca un verbo TP-READY cuando no hay conversación aun.
3 (Service-denied)	Se niega el procesamiento del verbo de petición.
4 ((Invalid-uow-header)	Se detecto un header UOW en el verbo de petición, si este código es regresado, OUW-OUT indica el UOW que fallo.
5 (Req-too-long)	El mensaje IPC fue demasiado largo para el tipo de respuesta dado o la longitud del mensaje excede el máximo configurado por SNAX/APC.
6 (Req-too-short)	El mensaje IPC fue demasiado corto para el tipo de respuesta dado
7 (Rep-too-long)	La respuesta es más grande que la configurada en el TP
8 (Invalid-req-code)	El valor del campo REQUEST-CODE es invalido
9 (Snax-file-error)	SNAX/APC recibe un error del sistema operativo en el cual esta montado mientras procesaba el verbo de petición. Si esto sucede se asume que SNAX/APC aborta la comunicación.
10 (Out-of-resources)	El TP local invoca un verbo ALLOCATE o un TP-READY cuando el LOCAL-ATTACH aun no es terminado, o aun no hay recursos disponibles para la comunicación.

HEADER-RETURN-CODE-DETAIL. Cuando se requiere de una mayor información acerca del header-return-code, se auxilia del valor del header-return-code-detail. La siguiente tabla muestra los valores posibles.

HEADER-RETURN-CODE		HEADER-RETURN-CODE-DETAIL	
VALOR	SIGNIFICADO	VALOR	SIGNIFICADO
2	Invalid-resource-id	310 (Config-Error)	Uno o más de los valores de configuración en la base de datos para el LU local tienen error.
3	Service-Denied	401 (Process-Reset)	El cpu primario donde corre SNAX/APC falló. El TP local debe parar y volver a arrancar para hacer posible un nuevo llamado TP-READY.
		402 (Mult-UOW-Not-Allowed)	Un mensaje IPC contiene varios UOW y uno de esos UOW es un TP-READY.
		403 (Previous-IPC-Not-Complete)	El TP local envió un mensaje IPC a SNAX/APC, pero anteriormente un mensaje del mismo TP no se completo o no a llegado a su fin.
		404 (Mult-Alloc-not-Allowed)	EL TP local invoco dos verbos ALLOCATE después un solo verbo TP-READY. Solo es permitido un ALLOCATE por cada TP-READY
4	Invalid-UOW-Header	302 (Invalid-Indicator)	Un UOW de petición contiene un indicador invalido
		303 (Invalid-Tpname)	El nombre especificado del TP no esta registrado en la base de datos o algún TP no autorizado invoca un TP-READY al TP en cuestión.
		304 (Invalid-Luname)	El LU especificado en la petición no esta registrado en la configuración de la base de datos.
		305 (Invalid-Send-Length)	El tamaño total del mensaje IPC excede el valor del parámetro MAXAPPLIOSIZE declarado en la configuración.
		306 (Invalid-Type)	El tipo de requerimiento solicitado es erróneo
		307 (Invalid-APC-Verb)	SNAX/APC detecto un verbo invalido
		308 (Too-Many-UOWS)	SNAX/APC detecto más UOWs en el mensaje IPC que los especificados en el campo UOW-IN del IPC-Header.
9	Snax-File-Error	Número de error del File-System	Contiene el error de GUARDIAN-90.

RESOURCE-ID. Este campo indica los recursos específicos dentro de SNAX/APC para los cuales este mensaje IPC tiene significado. En el primer mensaje IPC, el TP pone ceros en el campo RESOURCE-ID; pero para los requerimientos subsecuentes, el TP debe usar el RESOURCE-ID que regreso el primer mensaje de IPC.

UOW-IN. Este campo indica el número de UOWs que contiene el mensaje IPC. En un verbo de petición, este campo debe ser llenado por el TP.

UOW-OUT. Indica el número de UOWs de respuesta que vienen en un IPC de respuesta de SNAX/APC. Si el REP-CODE indica Uows-with-error (valor 2), el campo UOW-OUT regresa el numero de UOW que causo el error.

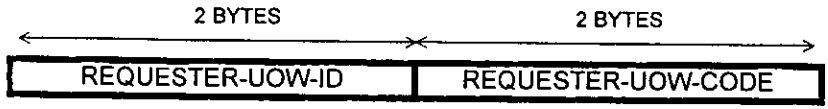
LOG-LEVEL. Este campo debe estar en ceros, se usara para futuras versiones.

5.5. ESTRUCTURA DE LOS MENSAJES UOW

Los TP´s se comunican con SNAX/APC utilizando verbos de petición o verbos de respuesta denominados Units of Work (UOW´s). Los mensajes IPC pueden contener múltiples UOW siempre y cuando sean de la misma conversación. Concatenando varios UOW en el mismo IPC disminuye el tráfico entre procesos y por consiguiente la eficiencia aumenta. Los UOW que conforman en el mismo IPC son procesados en el orden de aparición dentro del mensaje IPC.

Antes de procesar cualquier UOW de un mensaje IPC, SNAX/APC revisa todos los UOW y checa posibles UOW no validos para SNAX/APC, si encuentra algún UOW invalido regresa todo el mensaje IPC como invalido sin procesar ningún UOW.

El header de un UOW de petición tiene la siguiente estructura:



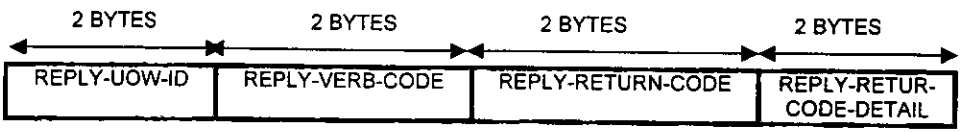
Estructura del header de petición de un mensaje UOW

REQUESTER-UOW-ID. Este campo debe contener el valor "ST", el cuál indica el comienzo de cada UOW.

REQUESTER-UOW-CODE. Identifica el requerimiento especifico. Por ejemplo 1001 (Allocate), 1006 (Receive-and-Wait) etc.

Posible Valor	*Significado*
2001	ACTIVATE-SESS-REQ-CODE
1001	ALLOCATE-REQ-CODE
1002	CONFIRM-REQ-CODE
1003	CONFIRMED-REQ-CODE
2002	DEACTIVATE-SESS-REQ-CODE
1004	DEALLOCATE-REQ-CODE
3003	DISPATCHER-READY-REQ-CODE
3002	DISPATCH-TP-REQ-CODE
3001	DISPLAT-STATUS-REQ-CODE
1012	FLUSH-REQ-CODE
1005	GET-ATTRIBUTE-REQ-CODE
1010	PREP-TO-RECEIVE-REQ-CODE
1006	RECEIVE-AND-WAIT-REQ-CODE
1011	RECEIVE-IMMEDIATE-REQ-CODE
1007	REQUEST-TO.SEND-REQ-CODE
1008	SEND-DATA-REQ-CODE
1009	SEND-ERROR-REQ-CODE
3006	TP-END-REQ-CODE
3005	TP-READY-REQ-CODE

Cada mensaje de respuesta de SNAX/APC contiene la siguiente estructura:



Estructura del header de respuesta de un mensaje UOW

REPLY-UOW-ID. Este campo contiene el valor "ST" para identificar el inicio de un UOW.

REPLY-VERB-CODE. Contiene un valor que identifica el tipo de verbo al cuál SNAX/APC esta respondiendo. Ejemplo DEALLOCATE-REP-CODE

REPLY-RETURN-CODE. Este campo indica si fue o no exitoso el verbo de petición.

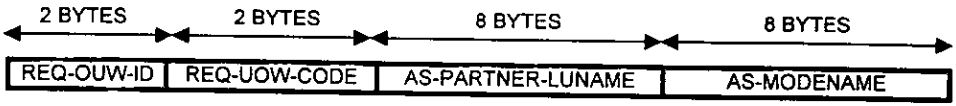
5.6. DEFINICIÓN DE LOS VERBOS DE SNAX/APC

A continuación se describen los verbos más importantes con los que SNAX/APC logra establecer comunicación entre aplicaciones.

ACTIVATE-SESSION.

Como su nombre lo indica se utiliza para activar una sesión especifica. Este verbo no arranca una conversación, simplemente comienza una sesión LU-LU, enviando o pidiendo un BIND.

Antes de usar el verbo ACTIVATE-SESSION un TP debe tener un control de sesión autorizado, el cuál esta declarado en el campo de SESSION-CONTROL-PRIVILEGE de la configuración del TP.



Estructura del verbo ACTIVATE-SESSION

REQ-UOW-CODE. Debe contener el valor 2001 el cuál identifica el verbo activate-session.

AS-PARTNER-LUNAME. Este es el nombre del LU remoto en donde se hará la conexión LU-LU. El nombre del LU remoto debe estar dado de alta en la base de datos de arranque de SNAX/APC, este nombre debe estar en letras mayúsculas.

AS-MODENAME. Este campo indica el nombre del modo que el LU remoto usara para accesar al BIND.

El verbo ACTIVATE-SESSION puede ser usado solo para activar una sesión con el LU local usado el verbo TP-READY. Un TP puede utilizar este verbo para obtener todas las sesiones con las que trabajara, antes de arrancar las

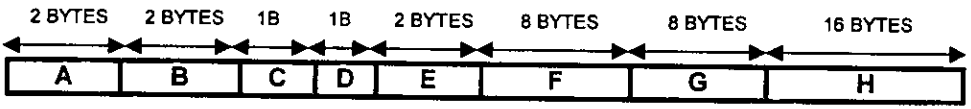
conversaciones e intercambio de datos: para lograr esto el TP debe seguir la siguiente secuencia de verbos por cada LU:

TP-READY (local)
ACTIVATE-SESSION
TP-END

ALLOCATE.

Un TP utiliza el verbo ALLOCATE para establecer conversación con un TP remoto. El verbo ALLOCATE debe ser el primer verbo invocado después que el TP se ha comunicado con el SNAX/APC local (después del TP-READY). EL verbo ALLOCATE se complementa cuando el TP local toma el control de la conversación.

Un verbo ALLOCATE provoca que SNAX/APC cree un attach (FMH-5) que es una instrucción propia de SNA.



A.- REQ-UOW-ID
B.- REQ-UOW-CODE
C.- AL-PARTNER-TP-TYPE
D.- AL-SYNC-LEVEL
E.- RESERVERD-2
F.- AL-PARTNER-LUNAME
G.- AL-MODENAME
H.- AL-PARTNER-TPNAME

Estructura del verbo ALLOCATE.

AL-PARTNER-TP-TYPE. Indica el tipo de conversación que el TP remoto utiliza. Si el campo es llenado con la letra B significa que el TP utiliza los verbos básicos de conversación.

Si por el contrario el campo tiene la letra M utiliza verbos mapeados de conversación.

AL-SYNC-LEVEL. Indica el nivel de sincronización de la conversación. la letra N significa que no se utilizara sincronización, y la letra C confirma la sincronización.

RESERVERD-2. Campo reservado para futuras versiones, debe tener el valor de cero

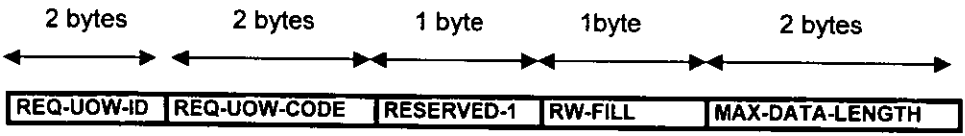
AL-PARTNER-LUNAME. Contiene el nombre del LU remoto que soporta el TP remoto. Este nombre debe estar dado de alta previamente en la base de datos de arranque de SNAX/APC. El registro en la base de datos de be ligar el LU remoto con el LU local.

AL-PARTNER-TPNAME. Contiene el nombre del TP remoto. Este nombre es utilizado cuando SNAX/APC envía un Attach al LU remoto.

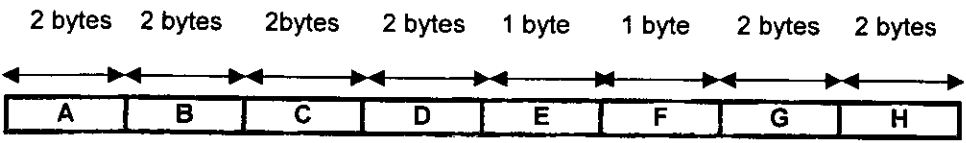
RECEIVE-AND-WAIT

El TP Local invoca al verbo Receive-and-wait cuando esta listo para recibir datos o información de control desde el TP remoto. El TP Local puede invocar este verbo mientras tenga en estado de send y el resultado exitoso cambia su estado de send a receive.

Petición:



Respuesta:



A.- REP-UOW-ID
B.- REP-VERB-CODE
C.- REP-RETURN-CODE
D.- RETURN-CODE-DETAIL
E.- RESERVED
F.- REQUEST-TO-SEND-IND
G.- WHAT-RECEIVED
H.- DATA-LENGTH

REQ-UOW-CODE. Debe tener el valor de 1006, que identifica al verbo Receive-and-wait.

RW-FILL. Bandera que indica dos estados:

"L". Indica que el TP Local esta esperando el registro lógico de datos, el registro lógico de datos puede estar completo o solo tener una parte del registro completo, el tamaño del registro debe ser igual al especificado en el campo Max-data-length.

"B". Indica que el TP Local reciba datos independientes del formato lógico del registro. El tamaño de este debe ser menor o igual al especificado por el campo Max-data-length.

MAX-DATA-LENGTH. Indica el tamaño máximo del registro que el TP Local recibirá.

REQUEST-TO-SEND-IND. Indica cuando el TP invoca al verbo Request-to-send, solo puede tener dos valores "Y" o "N".

WHAT-RECEIVED. Sirve para saber que fue recibido por el TP remoto, un TP en estado de Recive debe involucrar un verbo Receive-and-wait hasta que el valor de What-receive indique una transición del estado de receive.

Los datos válidos son:

0. El Rw-fill del Uow de petición indica que el buffer esta lleno y el TP Local esta recibiendo datos.
1. El TP Local esta recibiendo la parte complementaria del registro de datos.
2. El TP recibió incompleto el registro de datos (ya que el registro fue mayor que el campo Max-data-length). El TP debe invocar otro Receive-and-wait para recibir el resto de los datos.
3. EL TP remoto avisa que esta en estado de recive y por consecuencia el TP local se pone en estado de send, el TP Local puede ahora invocar el verbo Send-Data.
4. EL TP remoto invoca un Confirm, el TP aviso del Confirm y puede responder con Confirmed o Send-error. No se recibe ningún dato en esta respuesta.
5. El TP remoto invoca un Prepare-to-receive seguido de un verbo Confirm o un Sync-level, el TP Local recibe el estado de Confirm.

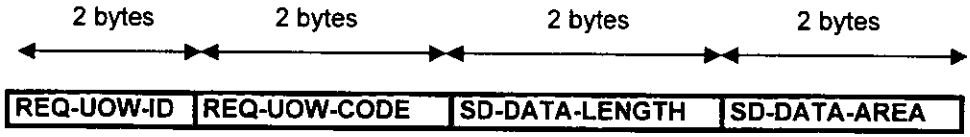
6. El TP remoto a invocado a un verbo Deallocate del tipo Confirm o con tipo Sync level, y la sincronización es confirmada. El TP puede responder con un confirmed, este cambiará al estado Deallicate, cuando tenga este estado, el TP local debe invocar un verbo Deallocate.

DATA-LENGTH. Indica el número de bytes de los datos recibidos por el TP local.

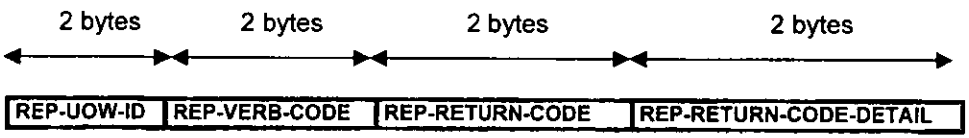
SEND-DATA

Este verbo envía datos al TP remoto, el TP local mueve datos dentro de SNAX/APC enviando su buffer a través del verbo Send-data.

Petición:



Respuesta:



REQ-UOW-CODE. Debe tener el valor 1008 que identifica el verbo Send-data

SD-DATA-LENGTH. Indica el tamaño, en bytes, de los datos que se están enviando.

SD-DATA-AREA. Contiene los datos que van a ser enviados.

TP-READY

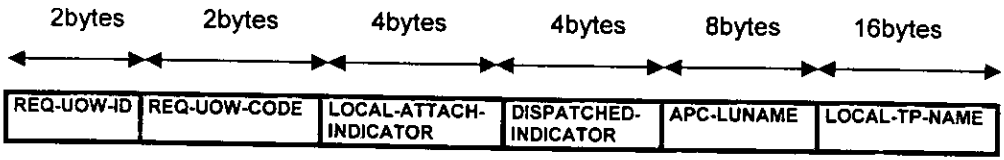
Un TP local utiliza el verbo Tp-ready para indicar comunicación con el proceso de SNAX/APC. El verbo Tp- ready debe ser el único Uow en el mensaje Ipc, no se puede concatenar con otro Uow.

Cuando el TP local invoca un Tp-ready, el campo Resource-id del Ipc de petición debe estar en ceros, ya que la contestación del Ipc contendrá en este campo los recursos utilizados mientras dure la sesión activa.

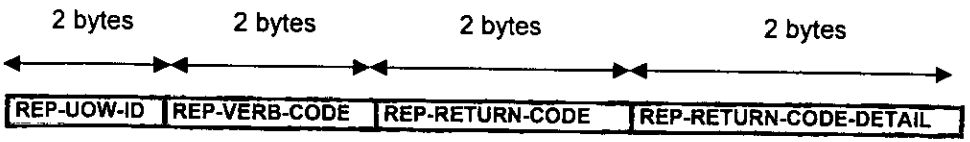
Hay dos diferentes formas de involucrar un TP-READY:

a) Si el TP local quiere comenzar una conversación. Para esto se debe especificar que el TP-READY hará un Local-attach que significa que el Tp local es el indicador de la conversación.
b) Si el TP local espera que un Tp remoto inicie la conversación, para esto debe indicar un Not-local, el cual se complementará hasta que un TP remoto se aloje en la dirección del Tp-local.

Petición:



Respuesta:



REQ-UOW-CODE. Debe llevar el valor 3005 que identifica al verbo TP-READY

LOCAL-ATTACH-INDICATOR. El valor "Y" indica que el TP esta inicializando un attach al SNAX/APC local. El valor "N" indica que el TP esta preparado para recibir un attach del TP remoto.

DISPATCHED-INDICATOR. El valor "Y" indica que el requerimiento TP-READY es inicializado por un despachador. El valor "N" indica que no utiliza ningún tipo de despachador.

APC-LUNAME. Es el nombre del LU local, debe estar en mayúsculas y con una longitud máxima de 8 caracteres.

LOCAL-TPNAME. Es el nombre del TP local. Debe estar en mayúsculas y con longitud máxima de 16 caracteres.

Capitulo 6. Desarrollo de una aplicación con el protocolo SNAX/APC para la transferencia de información entre redes.

El porque de este trabajo tiene que ver con el funcionamiento de una Casa de Bolsa. El estudio se centra principalmente en el área que administra el efectivo, pero para entender con mayor facilidad el objetivo del tema explicaremos algunos conceptos bursátiles.

6.1. CONCEPTOS BÁSICOS DE FINANZAS

Finanzas, término aplicado a la compraventa de instrumentos legales cuyos propietarios tienen ciertos derechos para percibir, en el futuro, una determinada cantidad monetaria. Estos instrumentos legales se denominan activos financieros o títulos valores e incluyen bonos, acciones y préstamos otorgados por instituciones financieras.

El primer emisor de un título valor se denomina prestatario, mientras que a la persona que compra el título valor se le conoce como prestamista. Los prestatarios necesitan dinero en efectivo, mientras que a los prestamistas les sobra liquidez. Cuando un prestatario emite un título valor que adquiere un prestamista ambas partes se ven beneficiadas; el prestatario obtiene el efectivo que necesita y el prestamista el derecho a obtener en el futuro el valor monetario prestado, así como una taza justa de beneficios (como pago de intereses).

Mercados Financieros, Las transacciones realizadas entre el primer emisor (prestatario) y el primer prestamista son transacciones del mercado primario. El primer prestamista puede vender los activos financieros adquiridos en el mercado primario a otras personas, en lo que se conoce como mercados secundarios. La compraventa de títulos, valores negociables en los mercados secundarios no tiene consecuencias para el emisor del título, es decir, el primer prestatario; sólo se produce una variación en la titularidad (propiedad legal) de los títulos valores. Ejemplos de mercados secundarios son la Bolsa de Valores, como la Bolsa de Nueva York, la Bolsa de Londres y la Bolsa de Tokio. Puede haber un mercado fuera de la cotización oficial del mercado secundario.

Clases de Títulos Valores, Casi todos los títulos valores que se negocian en los mercados secundarios pertenecientes a uno de estos grupos: Bonos o Acciones. Los bonos son instrumentos crediticios: A cambio de cierta cantidad de dinero, proporcionan un rendimiento fijo. Las características más importantes de los bonos son su valor facial (o a la par), su fecha de vencimiento y la taza de cupón. El valor

facial refleja la cantidad de efectivo total que se pagará al propietario del bono a la fecha de vencimiento, que va desde los tres meses a los treinta años. Antes del vencimiento, cada año se paga el cupón, que es la taza de cupón multiplicada por el valor facial. Este cupón es el beneficio que obtiene el poseedor del bono. Cuando el cupón es igual al tipo de interés medio que se está pagando en ese momento, el precio del mercado del bono será igual a su valor facial. Cuando el cupón es mayor a los tipos de interés que se están pagando, el bono se venderá a un precio superior al valor facial. Cuando el cupón que se paga es inferior al tipo de interés del mercado, el bono se venderá con descuento. El pago del cupón constituye una obligación legal, por lo que el impago, puede provocar la quiebra.

Las acciones preferentes son parecidas a los bonos, ya que tienen un valor facial y proporcionan un dividendo predeterminado (parecido al cupón de los bonos). La diferencia estriba en que las acciones preferentes, a diferencia de los bonos, no tienen un plazo de vencimiento, y en que se puede no pagar los dividendos anualmente durante varios años, sin que ello implique la quiebra del emisor. Las acciones ordinarias no tienen ni plazo de vencimiento ni dividendos anuales estipulados. Estos títulos valores tienen un periodo de vida ilimitado, y sólo se pagarán dividendos si el emisor obtiene algún beneficio satisfactorio. Dado que los rendimientos de los bonos son los más seguros, los bonos son inversión menos arriesgada, pero a su vez tienen un menor rendimiento. Las acciones preferentes comportan mayores riesgos que los bonos, pero menores que los que comportan las acciones ordinarias. Éstas son las más arriesgadas, por lo que su taza de rendimiento esperada es también la más elevada.

Los agentes que emiten títulos valores pueden dividirse en públicos y privados. Los emisores privados pueden ser individuos, sociedades y corporaciones. Los emisores públicos pueden ser distintas instituciones gubernamentales.

Las finanzas en el sector privado, Tanto los individuos, como las sociedades y las corporaciones pueden emitir títulos valores financieros para pagar diferentes activos que quieran adquirir. Puesto que las corporaciones son la principal fuerza financiera del sector privado, el siguiente análisis se centrará en la financiación de las corporaciones. Estas pueden adquirir más capital vendiendo acciones y bonos, o pueden financiar sus necesidades temporales obteniendo préstamo de los bancos.

El responsable financiero de la corporación debe decidir qué activos ha de comprar la empresa y cómo hay que financiar esta adquisición. Las decisiones de inversión en activos dependen de dos factores: Las tasas de retorno esperadas y el riesgo. Para poder estimar los rendimientos esperados de un proyecto se realizan análisis detallados sobre las previsiones de ventas potenciales, gastos y beneficios esperados de la inversión. El riesgo depende de la incertidumbre que tenga la empresa respecto a los beneficios anuales que pueda obtener.

Las decisiones financieras dependen únicamente del tipo de contrato financiero que minimice los costos para la empresa. Al igual que ocurre con las decisiones de inversión en activos, los costos financieros se expresan en función de la taza de interés anual. Los costos financieros de una emisión de nuevas acciones vienen dados por los dividendos mínimos más la apreciación del precio de las acciones que el comprador espera recibir.

Financiación a corto plazo, Deudas. Su financiación se divide en deudas a corto plazo y deudas a largo plazo. La emisión de deuda a corto plazo debe amortizarse en menos de cinco años. Los préstamos concedidos por bancos comerciales son el ejemplo más común de deudas a corto plazo. Las líneas de crédito de los bancos permiten a una empresa pedir préstamo un máximo predeterminado, pero se exige que el saldo esté a cero durante uno o más meses al año. Estas líneas de crédito no suelen estar respaldadas por una garantía. Los bancos también ofrecen préstamos a dos o tres años, pero éstos suelen estar avalados por los inventarios o los activos exigibles de la empresa si no se devuelven en el plazo determinado.

Existen otros tres tipos de financiación a corto plazo, que son: ***los pagarés de empresas, las pignorancias y el factoring.*** Los pagarés de empresas son una deuda emitida por una empresa que tiene un plazo de vencimiento inferior al año. Sólo los emiten grandes empresas, financieramente solventes, y tienen un costo en intereses ligeramente inferior al de los préstamos bancarios concedidos para las inversiones con menores riesgos. La pignoración y el factoring son utilizados por empresas más pequeñas, con menor solidez financiera. El factoring es la venta física de las cuentas a cobrar a los clientes. La pignoración es un préstamo garantizado con las cuentas a cobrar a clientes de la empresa. Dado que comportan un mayor riesgo, la pignoración y el factoring obligan a la empresa a pagar mayores intereses que los que se pagan por los pagarés de empresa.

Antes de mediados de los años 60, todas las emisiones de deuda se vendían dentro del país en el que la corporación que los emitía residía. Desde entonces, la financiación internacional se ha incrementado de manera espectacular. La mayor parte de esta financiación en el orden internacional es a corto plazo, y tiene lugar en lo que se denomina mercado de eurobonos, estando su mercado principal en Londres. El mercado de eurobonos permite que las empresas emitan deudas en divisas extranjeras (principalmente en dólares) al tiempo que evita las regulaciones y restricciones de los mercados financieros nacionales. En el mercado de eurobonos se emite deuda tanto a corto como a largo plazo. En los últimos años se han llegado a emitir bonos con un plazo de vencimiento de hasta 50 años.

Financiamiento a largo plazo, Normalmente, la financiación a largo plazo se lleva a cabo mediante la emisión de bonos o mediante arrendamientos con opción de compra. Los bonos que no están avalados por algún activo se suelen

denominar obligaciones. Dado el riesgo que comportan, las obligaciones implican una mayor tasa de rendimiento. Las emisiones de bonos garantizados implican que éstos estan avalados por algún activo, por lo que rinden menores intereses. El arrendamiento con opción de compra es parecido a la emisión de una deuda, con la diferencia de que el título de propiedad del activo no se cede a la empresa que efectúa el arrendamiento. Este tipo de financiación está aumentando gracias a sus mayores ventajas impositivas, que no poseen los demás medios de financiación.

En algunas ocasiones, la emisión de bonos a largo plazo permite al comprador adquirir posteriormente acciones ordinarias de la empresa. Estos bonos convertibles permiten que el poseedor de los bonos los intercambie por un determinado número de acciones ordinarias. Algunas obligaciones permiten que el poseedor de los bonos compre acciones ordinarias a un precio inferior. Desde el punto de vista de la corporación, los bonos convertibles dan lugar, a su vencimiento, a una ampliación de capital, mientras que las obligaciones preferentes seguirán siendo una deuda, pero también supondrán una ampliación de capital en el futuro.

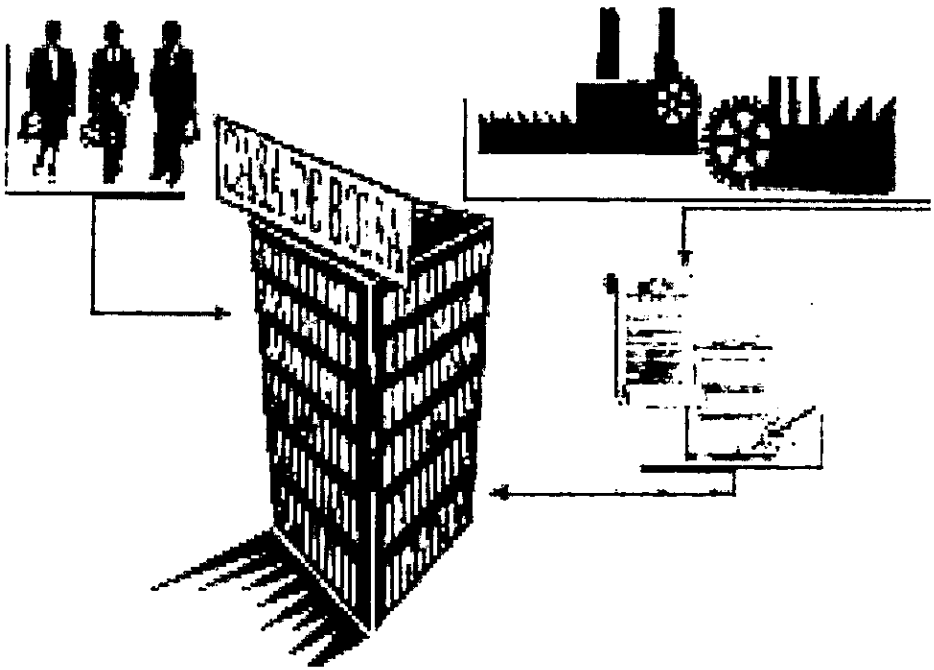
Las acciones preferentes son, de alguna manera, parecidas a los bonos. Se venden con un determinado valor, se paga una cantidad determinada anualmente y en caso de quiebra, otorgan el derecho de acudir a liquidación de los activos por delante de los propietarios de acciones ordinarios. En otros aspectos son análogas a las acciones ordinarias: No hay que pagar dividendos si la empresa no tiene suficiente efectivo, y los dividendos que se pagan pueden ser mayores en caso de que los beneficios de la empresa aumenten. Por su parte, los bonos rinden un cupón fijo y obligatorio todos los años. Los compradores de acciones preferenciales obtienen ventajas fiscales que no tienen los que compran bonos. Estas ventajas fiscales hacen que las empresas emitan acciones preferenciales, que además comportan menores costos para el emisor.

Los auténticos propietarios de una corporación son los tenedores de acciones ordinarias; reciben la totalidad de los beneficios, descontados los pagos de intereses de las deudas y el pago de dividendos de las acciones preferentes. Estos beneficios se distribuyen en dos formas: como efectivo, en forma de dividendos a los accionistas, y como incremento del valor de las acciones ordinarias. Este aumento del precio de las acciones ordinarias puede tener dos causas:

1. La reinversión de los beneficios, para aumentar el crecimiento de la corporación o permitir el logro de otros objetivos, aumenta el valor total de los activos de la empresa, y por tanto, el valor de sus acciones. Si por ejemplo, se retiene una determinada cuantía de los ingresos por cada acción de la empresa, el valor de cada acción debe aumentar en la misma cuantía.

2. El cambio en las expectativas de los accionistas sobre los beneficios potenciales futuros de la empresa hará que el precio de las acciones varíe. El rendimiento obtenido por un accionista viene dado por el dividendo percibido más las ganancias (pérdidas) del valor de las acciones.

Intermediarios financieros, Son aquellas instituciones que obtiene recursos de un prestamista y los ofrecen a los prestatarios. Por ejemplo, un banco comercial obtiene dinero de los depósitos de sus clientes, las cuentas de ahorro y la venta de bonos. Después presta éste dinero a individuos, corporaciones o gobiernos. Existen más intermediarios financieros, como las sociedades inmobiliarias, los fondos de inversión mobiliaria, las compañías de seguros y los fondos de pensiones. Estas instituciones permiten que los pequeños ahorradores junten sus fondos y puedan diversificarlos en varias inversiones. Además, la experiencia financiera de los gestores de éstas instituciones permite que los ahorradores obtengan mayores rendimientos.



Financiación del sector público, Mediante el gasto público los países realizan servicios demandados por los ciudadanos. A lo largo del siglo pasado el gasto público aumentó considerablemente en todos los países, independientemente del sistema político. Esto se debió, en parte, a la tendencia casi universal de ampliar los servicios gubernamentales en áreas que antes estaban reservadas a la iniciativa privada, pero también fue debido al crecimiento de la población, a una mayor riqueza general y a la elevación de los niveles de vida.

El gasto público se puede dividir en tres grandes grupos*: **defensa, obras públicas y programas que favorezcan el bienestar social**.* Las obras públicas incluyen servicios como la creación de carreteras, ferrocarriles, el teléfono y los telégrafos. Los programas que fomentan el bienestar social incluyen gastos en el sistema sanitario, la educación y la ayuda a personas discapacitadas. El principal ejemplo de la intervención estatal en la economía es el de la antigua Unión Soviética, donde casi todas las industrias pertenecían al Estado o estaban bajo su control.

Cuando el gasto público es superior a los ingresos de los impuestos, el déficit resultante puede financiarse de dos maneras: ***mediante la emisión de obligaciones respaldadas por el gobierno, o mediante la creación de dinero.***

Imposición, El gasto público se financia, principalmente, mediante los impuestos. Éstos pueden ser de varios tipos, impuestos indirectos, impuestos sobre las importaciones, impuestos sobre la renta, impuestos sobre el valor añadido, y otros mecanismos que permiten obtener ingresos. Este es el principal medio de obtención de recursos del sector público.

Financiación de los déficits, Los gobiernos pueden financiar los déficits emitiendo deuda pública. En el ámbito nacional suele existir un departamento del tesoro, con poder para emitir títulos valores a corto y a largo plazo. En Gran Bretaña, las obligaciones del tesoro tienen un periodo de vencimiento igual o superior a los tres meses; Los bonos de gobierno tienen un plazo de vencimiento que oscila entre 1 y 20 años. Los bonos emitidos por un gobierno están considerados como los títulos valores con menor riesgo.

En muchos países ha aumentado la emisión de deuda por parte de las administraciones locales y los municipios. Estas emisiones son muy parecidas a las de los gobiernos centrales, pero comportan mayores riesgos. Por ello, tienen rendimientos, después de impuestos, superiores a los de la deuda del gobierno central, incluso cuando el plazo de vencimiento es el mismo. Además de mayor riesgo que comportan, estas emisiones de deuda tienen otra característica esencial: sus ventajas fiscales. Aunque los ingresos derivados del aumento del precio de los bonos estan totalmente sometidos a gravamen, el cupón pagado esta exento de los impuestos sobre la renta del gobierno central, y tampoco pagan impuestos en la administración local que los emite. Debido a este trato de favor fiscal, los rendimientos de las emisiones de las administraciones locales suelen ser inferiores a los de la deuda pública del gobierno central.

Creación de dinero, En última instancia, el gobierno puede financiar sus gastos creando más dinero. Esta fuente de financiación sólo está al alcance de los gobiernos centrales. Si el gobierno de la nación desea gastar determinada cantidad para pagar varios proyectos, puede, por ejemplo, crear la cantidad de dinero necesaria para sus gastos. Sin embargo, en la práctica este proceso es más complicado; la creación de dinero depende normalmente del banco central. Por ejemplo, en España el Banco Central es el Banco de España, que es el responsable de la oferta monetaria del país. La oferta monetaria a menudo varía en función de las necesidades de financiación del déficit público, o para controlar los tipos de interés, o el nivel de la inflación, y también para aumentar el nivel de empleo. Desgraciadamente, los procesos necesarios para lograr éstos efectivos suelen entrar en conflicto. Por ejemplo, el objetivo de tener bajos tipos de interés en un momento dado suele implicar mayores tipos de interés y mayores tasas de inflación a largo plazo.

Finanzas internacionales, Los movimientos de capital entre países, pueden dividirse entre pagos corrientes e inversiones de capital. Los pagos corrientes se refieren a los pagos entre países por exportaciones e importaciones, así como el pago de intereses y dividendos. Durante un año cualquiera, un determinado país tendrá déficit o superávit en sus transacciones corrientes. Las inversiones de capital se refieren a la compraventa de títulos valores de un país por parte de otro. Estas transacciones también pueden dar lugar a un déficit o a un superávit. Un déficit neto de las transacciones corrientes y de las inversiones de capital refleja el flujo neto de recursos financieros que han salido de un país; Un superávit neto refleja los recursos financieros que han entrado en el país.

Cada país tiene su propia unidad monetaria, en la que exigirá que se le paguen los superávits netos. El valor de una moneda en términos de otra depende de qué país de los dos tiene un déficit neto frente al otro. Por ejemplo, si Estados Unidos tiene un déficit neto en sus relaciones con Francia, el valor del franco Francés aumentará en relación con el dólar. Este valor relativo es el reflejo de tipo de cambio, que expresa el costo de una unidad de una determinada moneda en términos de otra. El aumento del valor del franco Francés hace que las exportaciones francesas a Estados Unidos sean más caras y que las exportaciones de Estados Unidos a Francia sean más baratas. Por lo tanto, el déficit tendría que equilibrarse automáticamente. Por ello, el tipo de cambio es muy importante dado su papel a la hora de reequilibrar los déficits y superávits entre los distintos países.

Los movimientos de capital han venido cobrando importancia a lo largo de las décadas de los 80 y los 90, a medida que se liberalizaba el sistema financiero internacional y se suprimían los controles sobre los tipos de cambio. Por ello, los especuladores monetarios y los inversores, ayudados por los adelantos en las telecomunicaciones, pueden mover fuertes cantidades de dinero por todo el mundo a una velocidad vertiginosa. El poder de este sistema financiero

Internacional se hizo patente en 1992, cuando las presiones especulativas organizadas rompieron el sistema monetario europeo de la Unión Europea, y de nuevo a principio de 1995, cuando las finanzas internacionales perdieron la confianza que tenían en México, provocando el pánico financiero en este país, lo que obligó a Estados Unidos a concederle un paquete de ayudas financieras.

6.2. PANORAMA GENERAL DE LA PROBLEMÁTICA

Como ya se ha mencionado, una Casa de Bolsa es un intermediario para realizar operaciones bursátiles, es decir, es el enlace entre las empresas que necesitan capital y los individuos que les sobra liquidez. Para que la Casa de Bolsa funcione adecuadamente necesita tener toda una infraestructura dividida en diferentes áreas entre las que se destacan:

Area de promoción. Que se encarga de atraer clientes que deseen invertir su capital.

Area bursátil. Gente especializada en flujos bursátiles.

Area de administración de efectivo y valores. Se encarga de controlar los flujos de efectivo y valores que se efectúen en Casa de Bolsa.

Para el buen funcionamiento y aprovechamiento de los recursos de una empresa, se debe contar con una Tesorería, que es la que se encarga de administrar los flujos de efectivo, esto es, tener liquidez oportunamente, distribuir el dinero eficientemente, pagar oportunamente a clientes y proveedores, administrar las chequeras del negocio, así como de centralizar el efectivo a final del día.

El asunto no lo es del todo fácil, para esto la Tesorería se auxilia de otras instituciones bancarias y de crédito. También es necesario contar con herramientas electrónicas para que el flujo de efectivo sea más eficiente.

Para poder liquidar (pagar o cobrar) una operación bursátil los clientes y la Tesorería cuentan con diferentes métodos a los que llamaremos medios de liquidación, estos medios de liquidación son los siguientes:

Liquidación en efectivo. Es la forma más antigua de liquidación, se ha quedado en el pasado aunque muchos clientes siguen ocupando este medio.

Tiene más desventajas que ventajas ya que no es un medio que utilice las ventajas electrónicas actuales, también representa un riesgo recibir o dar dinero en efectivo. Actualmente este medio de liquidación ya no se utiliza en la Casa de Bolsa.

Emisión de cheques. Este medio de liquidación es muy utilizado cuando los clientes no cuentan con algún servicio electrónico proporcionado por su Banco, o por que el cliente aun no confía plenamente en los medios electrónicos.

Ventajas.

- Seguridad de liquidez sin que se tenga dinero en efectivo en las manos
- Respaldo de una institución bancaria
- Se pueden personalizar los pagos

Desventajas.

- Para hacer valido el cheque se debe de presentar solo en el banco que emite el cheque
- El uso de papel para los cheques suele ser muy costoso
- La falsificación de cheques es frecuente

Listado de cargo abono (RMC). Es el primer intento de liquidación electrónica, consiste en cargar y/o abonar a diferentes cuentas de efectivo en una sola transacción sin que el cliente o la Casa de Bolsa se tengan que presentar en el Banco respectivo. La mecánica de liquidación comienza desde que el cliente abre una cuenta de efectivo en un Banco, si el cliente desea que sus transacciones sean vía RMC lo notifica al Banco y a Casa de Bolsa para que el permiso de abonar o cargar sea dado de alta. Cuando Casa de Bolsa tenga que abonar o cargar a la cuenta de efectivo por concepto de alguna operación bursátil, se genera un listado que contiene información de cuentas de cargo y abono (este listado puede contener la información de varias operaciones a realizar de diferentes clientes), el listado se lleva al banco y allí un capturista liquida todas las operaciones del listado.

Ventajas.

- Se empieza a aprovechar las ventajas electrónicas
- El cliente no necesita presentarse en el Banco
- El cliente puede ordenar sus operaciones por teléfono
- La seguridad se incrementa notablemente
- No hay comisión por el uso del medio

Desventajas

- El dinero no esta disponible en línea (Al momento de cerrar la operación)
- La liquidación es por lotes
- Se depende de un capturista

Liquidación por líneas electrónicas. Este medio de liquidación aprovecha todas las ventajas de los avances en comunicaciones. Consiste en hacer transferencias de efectivo desde el lugar mismo en que se generan, para nuestro caso, desde la misma Casa de Bolsa. Existen dos caminos para que la transacción se efectúe, una es que se genere información electrónica de varias operaciones en lotes y se transmitan desde una terminal instalada en la Casa de Bolsa. La otra manera es que exista una conexión física con el sistema del banco y las operaciones se realicen en línea y en tiempo real.

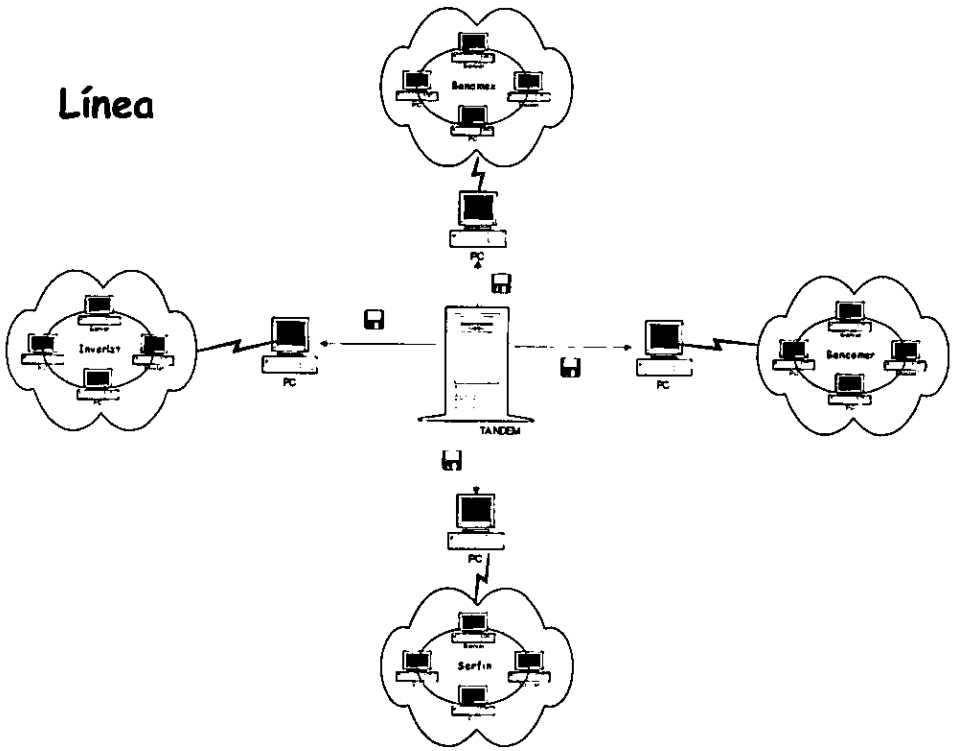
Los trámites para que el medio de liquidación sea válido es que el cliente autorice a Casa de Bolsa para poder cargar o abonar en sus cuentas de efectivo.

Ventajas.

- Se aprovechan las ventajas electrónicas
- El cliente no necesita presentarse en el Banco
- El cliente puede ordenar sus operaciones por teléfono
- La seguridad se incrementa notablemente
- Rapidez en el traspaso de efectivo
- Mejor servicio por parte de Casa de Bolsa

Desventajas.

- Comisión por el uso el servicio
- Sólo se tiene el servicio con algunos bancos
- La transferencia de fondos debe ser en cuentas del mismo banco
- Se depende totalmente de la infraestructura dada por el banco



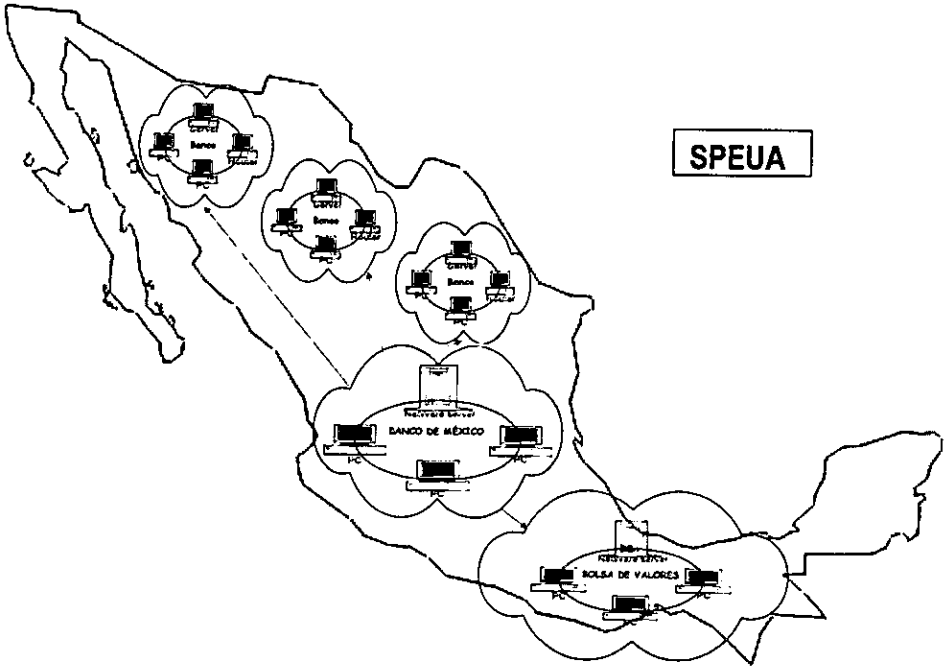
Servicio de Pagos Electrónicos de Uso Amplio (SPEUA). Este medio de liquidación es un servicio que ofrece Banco de México a todos los bancos del país, y consiste en poder hacer transferencias de efectivo por el sistema de Banco de México. Esto se hizo con la finalidad de un eficiente flujo de efectivo entre bancos.

Ventajas.

- Las transferencias de efectivo tienen el respaldo del Banco de México
- Se pueden realizar operaciones entre diferentes bancos
- El servicio esta disponible para cualquier banco, y en cualquier lugar del territorio nacional
- Se aprovechan las ventajas electrónicas
- El cliente no necesita presentarse en el Banco
- El cliente puede ordenar sus operaciones por teléfono
- La seguridad se incrementa notablemente
- Rapidez en el traspaso de efectivo
- Mejor servicio por parte de Casa de Bolsa

Desventajas.

- El monto mínimo actual por transacción es de cincuenta mil pesos
- Opera bajo un esquema de financiamiento entre bancos
- Se cobra una comisión a cada Banco por el uso del servicio



6.3. ANALISIS DE LA PROBLEMÁTICA

Los entes principales en una transacción bursátil son:

1. **Clientes**. Personas físicas o morales que desean invertir capital en el ambiente financiero.
2. **Contratos**. Es el documento oficial de acuerdos entre el cliente y la Casa de Bolsa.
3. **Chequeras**. Es el enlace con los Bancos, donde el cliente y Casa de Bolsa tienen el dinero en efectivo.
4. **Medios de liquidación**. Son los servicios que da un banco a clientes y Casa de Bolsa para hacer más fácil el traslado de efectivo.

Al realizar una operación de compraventa de títulos en Casa de Bolsa se disparan dos eventos de naturaleza distinta, uno que es el movimiento de títulos y por otra parte el movimiento o flujo de efectivo.

Para nuestro estudio veremos a detalle el flujo de efectivo en una operación bursátil.

Cuando un cliente abre su contrato de intermediación bursátil, esta listo para invertir su dinero en instrumentos bursátiles. Una vez que el contrato se abre, el cliente tiene que especificar los medio por los cuales sus operaciones serán liquidadas (pagadas o cobradas), para esto, el cliente informa a Casa de Bolsa los nombres de Bancos y números de chequeras donde tiene su dinero. Cuando Casa de Bolsa da de alta esta información activa los medios de liquidación válidos para el contrato del cliente. La manera más común con la que un cliente liquida sus operaciones es teniendo una cuenta de cheques en un Banco y dar permiso para que Casa de Bolsa pueda cargar o abonar efectivo de esa cuenta, con esto el cliente puede ordenar sus operaciones por teléfono y evita pérdida de tiempo al ir al Banco o a Casa de Bolsa.

De las premisas más importantes dentro de Casa de Bolsa esta la de dar a sus clientes el mejor servicio, y para esto ponen énfasis en tres conceptos:

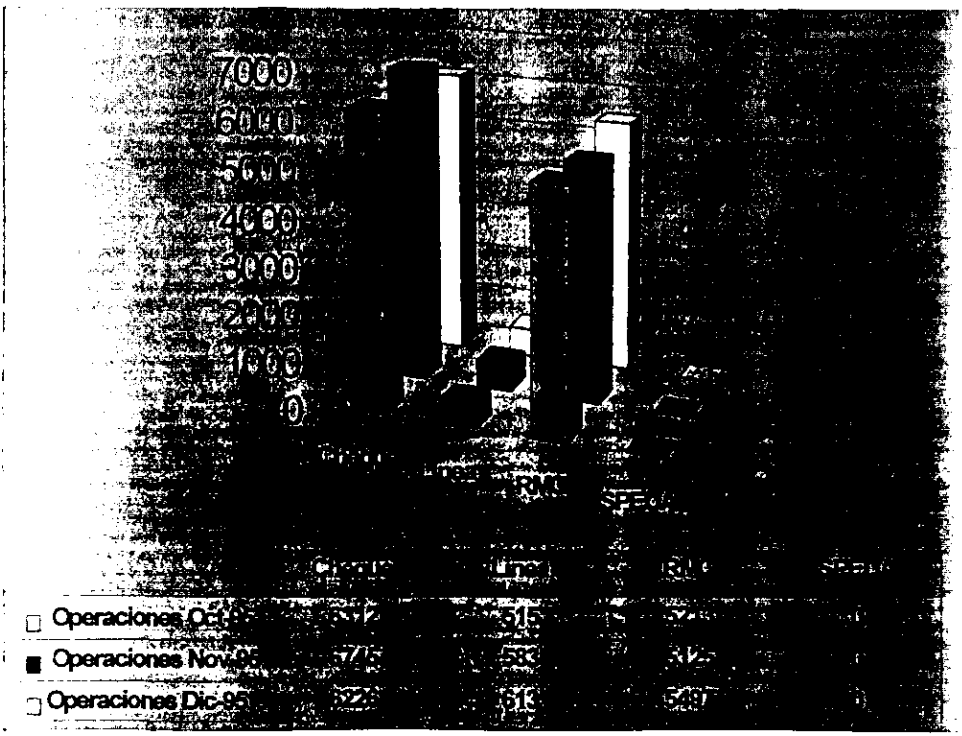
1. Calidad en el servicio a clientes y proveedores
2. Rapidez y oportunidad en inversiones
3. Liquidez inmediata de efectivo

Para poder lograrlo se debe de contar con herramientas de trabajo tecnológicamente avanzadas y con propuestas de mejoras en áreas de servicio a clientes.

En un esfuerzo por mejorar ineficiencias que existían en el área de Administración de Efectivo, se detectó que la rapidez con la que se efectuaban pagos, cobros o traspasos de efectivo tanto en chequeras de clientes como en las chequeras propias, era muy baja. El área de Administración de Efectivo quería vender a sus clientes el servicio de liquidación de operaciones en línea, esto es, poder tener liquidez en su chequera de efectivo en el instante mismo que su operación bursátil estuviera lista.

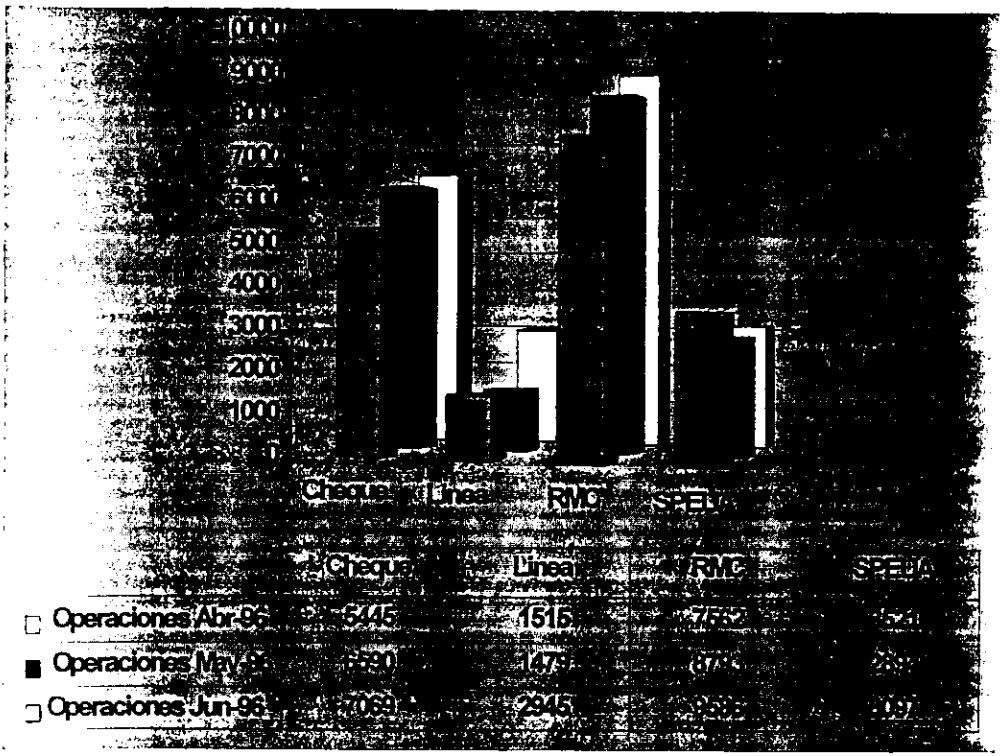
Es en este punto que el área de Sistemas de Cómputo, el área de Comunicaciones y el área de Administración de Efectivo empiezan a trabajar en conjunto. El presente trabajo narra las etapas de desarrollo que se siguieron para poder resolver el reto que propone Administración de Efectivo.

Lo primero que se investigó era saber la tendencia de liquidación que había, es decir, si los clientes tendían a utilizar ya los medios electrónicos disponibles en los bancos. Para esto se armó un estadístico histórico de los diferentes medios de liquidación.



En un principio la manera más común de liquidar operaciones era con dinero en efectivo, pero para mayor seguridad tanto de clientes como de la Casa de Bolsa se tomó la política del no manejo de efectivo. Por esta causa la emisión de cheques es una practica común aún en estos días de liquidación de operaciones Bursátiles.

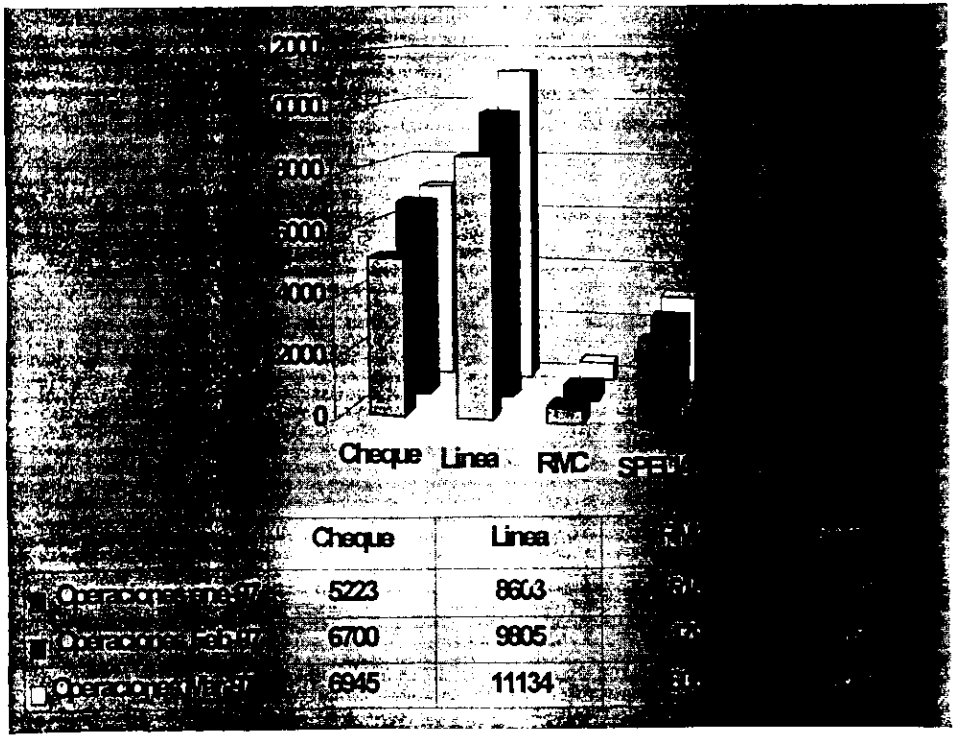
El siguiente estudio fue un estadístico de operaciones diarias en el cual se observara el medio de liquidación mas utilizado por los clientes, ésto para saber la preferencia de los clientes en cuanto a su medio de liquidación preferido.



En este resultado se observa que los clientes preferían utilizar el medio de liquidación RMC, aún sabiendo que ya existía la liquidación por líneas electrónicas, esto causó extrañeza y se pidió al área de Administración de efectivo que indagara las causas por las cuales los clientes preferirían un medio de liquidación semiautomático. Los resultados de la encuesta llegaban a tres conclusiones básicas:

1. El medio RMC no tiene costo adicional, y aunque mínimo, las líneas, tienen un costo extra.
2. Pueden realizar operaciones de cualquier monto.
3. Desconocimiento de que existan otros medios de liquidación.

El medio de liquidación RMC tal vez sea el menos costoso para los clientes, pero por el contrario para la Casa de Bolsa el costo operativo es muy alto. Por esto se decidió promover el uso de medios electrónicos en los clientes. Para esto se realizó una campaña de información sobre las ventajas de los médios de liquidación en línea, el resultado fue muy bueno como se observa en la siguiente gráfica.



Ya para esta época se difundió el medio de liquidación por SPEUA, pero como era totalmente nuevo los clientes desconocían su uso, además de que el monto mínimo por operación debía ser de 100,000 pesos.

Como siguiente paso, el área de Comunicaciones en conjunto con el área de Desarrollo de Sistemas de Cómputo, investigaron el flujo electrónico que seguían las operaciones liquidadas por líneas, las herramientas con las que actualmente se liquidaban y cómo era su funcionamiento.

Esto se hizo con el objeto de poder mejorar las herramientas con las que se cuenta actualmente.

6.4. PROPUESTA DE SOLUCIÓN CON SNAX/APC

Con la información recabada anteriormente se diseñó una propuesta de solución que contiene los siguientes puntos:

- La solución debe de bajar los costos operativos por cada transacción liquidada. Para que nuestra propuesta de solución baje los costos operativos, se pretende eliminar pasos intermedios entre la generación de la orden de liquidación y la liquidación misma en el banco. Esto se logra creando una herramienta de liquidación que no dependa de áreas de administración para que la orden llegue al Banco correspondiente.

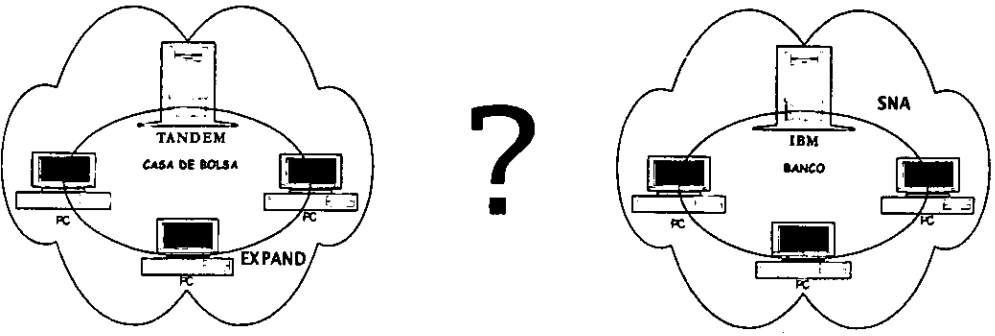
- Ya que no se cuenta con un medio de liquidación totalmente automático, el esfuerzo se centrará en obtener una herramienta de liquidación de operaciones totalmente automática. También se puede lograr reducir el tiempo de disponibilidad de efectivo para los clientes.

- Como existe un Banco que es parte del grupo financiero se propone dar impulso para que los clientes de Casa de Bolsa también sean clientes del Banco del grupo. Para obtener una herramienta de liquidación de operaciones totalmente automática se necesita tomar en cuenta los siguientes puntos:

  - ✓ El Banco con el cual se liquidará debe ser el Banco del grupo, ya que a diferencia de otros Bancos, se puede tener acceso a su base de datos casi sin restricciones. Así la orden de liquidación (cargo/abono) se armará desde Casa de Bolsa y se enviará a la base de datos del Banco.

- Explotar al máximo las herramientas electrónicas con las que se cuentan actualmente, esto es, si hay que resolver algún problema de hardware o software, hay que investigar primero si las herramientas actuales pueden resolver dicho problema.

Para lo anterior se investigó la actual topología de red con que se cuenta en Casa de Bolsa, así como los medios de comunicación actuales.

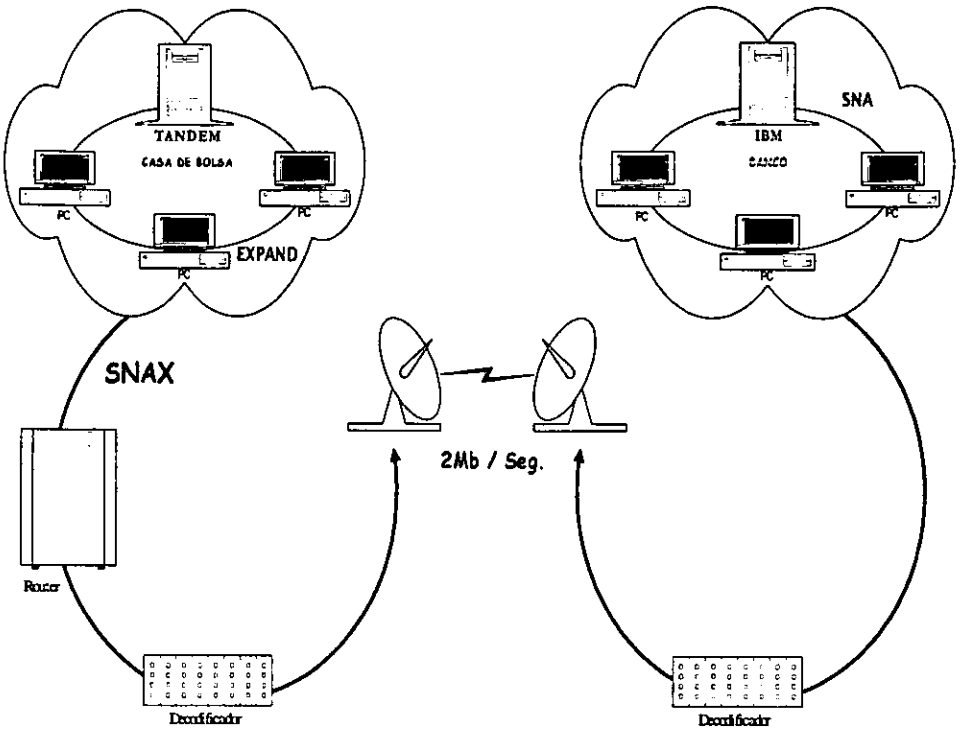


Analizando la tipología de red con que cuenta Casa de Bolsa y Banco se pueden deducir algunos problemas:

- La infraestructura informática de Casa de Bolsa esta montada principalmente sobre un mainframe TANDEM, por el contrario, la infraestructura informática del Banco esta montada sobre Main Frame de IBM.

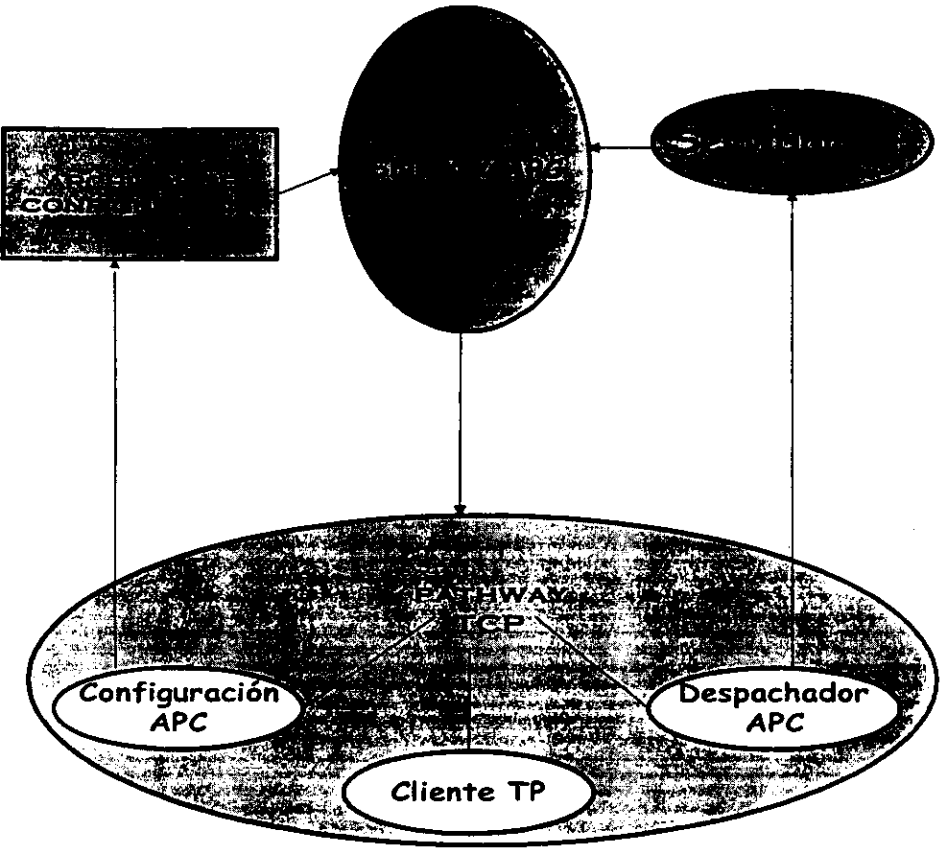
- La arquitectura de red de TANDEM se le conoce como EXPAND y la arquitectura de red de IBM es SNA, redes totalmente distintas y que no se pueden comunicar sin tener un intérprete.

Tomando en cuenta los puntos anteriores debemos resolver el problema de comunicación entre redes diferentes. Con el protocolo SNAX/APC se puede lograr la comunicación entre estas dos plataformas diferentes, ya que este protocolo corre sobre el TANDEM y emula como si fuera un LU de la red IBM (SNA).



Para implementar la solución de comunicación con SNAX/APC se realizaron los pasos siguientes:

- Como SNAX/APC corre en TANDEM se instaló el protocolo y se configuró para que lo reconociera el GUARDIAN90 de TANDEM.
- Se configuró la base de datos para que SNAX/APC emulara la aplicación de TANDEM como si fuera un LU de la red SNA.
- Identificar los principales verbos de SANX/APC que se utilizarán para entablar conversación e intercambiar información entre aplicaciones.



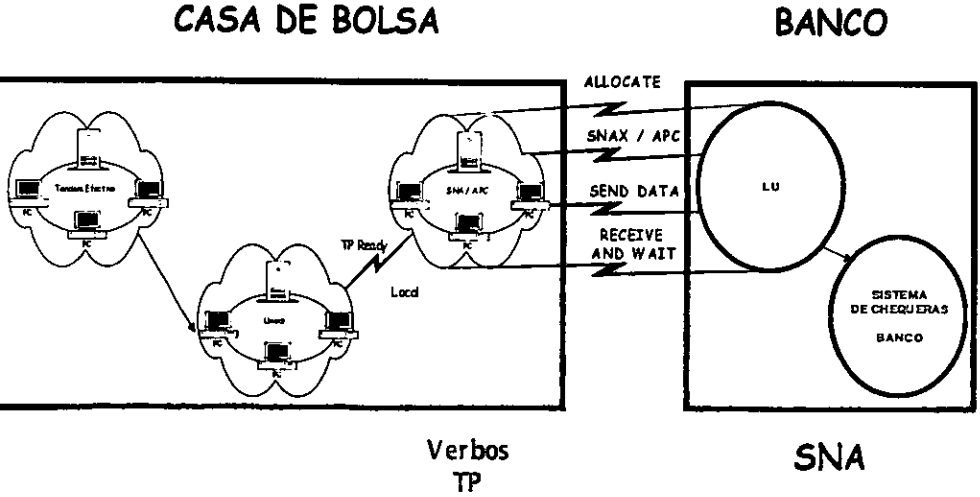
Los verbos a utilizar son:

a) **TP-READY**. Es un llamado de la aplicación local (TANDEM) hacia SNAX/APC, indicándole que está lista para entablar una conexión.
b) **ALLOCATE**. SNAX/APC trata de alojarse en el LU REMOTO (IBM), indicándole el destino remoto de la conversación (TP remoto)
c) **RECEIVE-AND-WAIT**. Una vez que la conexión LU-LU se logra, este verbo indica a cada TP el estado en que se encuentra la línea de comunicación, los estados son recibiendo información o listo a enviar información.
d) **SEND-DATA**. El TP que tenga estado listo a enviar información utiliza este verbo para enviar la información que tenga disponible.
e) **DEALLOCATE**. termina la sesión LU-LU.

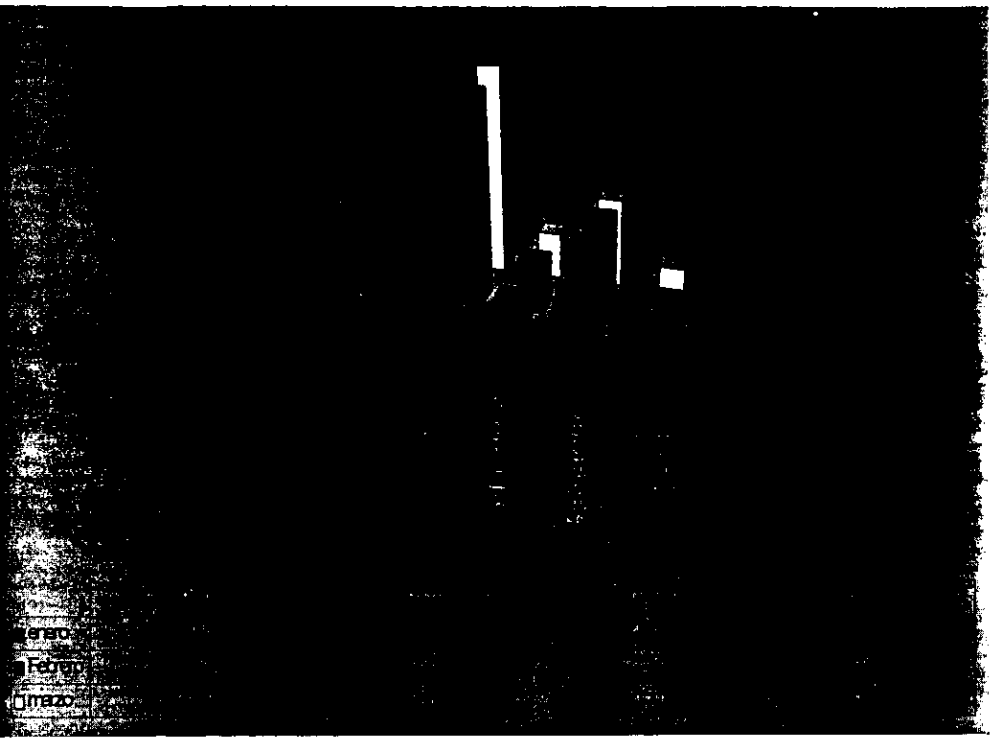
Una vez que se resolvió el problema de comunicación entre TANDEM e IBM se detectó otro problema, la seguridad y confiabilidad de la información que se intercambiaría. Esto es, como la información que viaja a través del protocolo es información que mueve dinero entre cuentas de cheques, se debe salvaguardar la integridad de cada una de las transacciones que se generen; para esto se pensó en desarrollar un sistema intermedio entre las aplicaciones de Efectivo y el protocolo de SNAX/APC, sin perder el concepto de un sistema totalmente automático. A este sistema se le llamó Sistema de Líneas Automáticas.

LINEAS AUTOMATICAS, es el sistema que se encargará de salvaguardar la integridad de operaciones, esto es se encargará de:

- Controlar los estados de operación de cada transacción enviada al sistema de cheques del banco.
- Salvaguardar la integridad de cada una de las operaciones, para esto se auxiliará del sistema de integridad de datos con el que cuenta el TANDEM.
- Retransmitir operaciones anómalas, es decir, transacciones que no hayan llegado a su término normal de operación.
- Interpretar errores que el protocolo SNAX/APC genere.
- Controlar operaciones que por su monto, horario de operación o naturaleza contable se le considere como riesgosa.



Una vez implementada la solución se procedió a realizar pruebas de comunicación y de intercambio de información entre aplicaciones, el resultado fue exitoso y se entrego el producto al área de Administración de Efectivo. Para realizar pruebas reales se tomó como clientes piloto a aquellos que tuvieran su contrato abierto directamente en el Banco del Grupo, ya que ellos por política deberían tener una cuenta de cheques en el del Banco del Grupo. Se les informó del nuevo servicio con el que contaba la Casa de Bolsa y se les invitó a que hicieran uso del mismo, el resultado fue el siguiente:



Movimientos de Retiro por Línea Electrónica

Una vez que se observó que el resultado de operaciones con los clientes piloto fue satisfactorio se procedió a liberar el producto a todos los clientes de la Casa de Bolsa. Para que funcionara la solución y fuera rentable se tenía que convencer a los clientes de tener por lo menos una chequera del banco del grupo para realizar sus operaciones financieras, el área de administración de efectivo se encargó de vender el nuevo producto a los clientes convenciéndolos de las ventajas que le ofrecería el usar el servicio en líneas.

CONCLUSIÓN

Para que una Casa de Bolsa sea rentable, necesita atraer clientes con capital y deseos de invertir en el sector financiero. También es importante que el flujo de operaciones sea constante y dinámico ya que la Casa de Bolsa obtiene ganancias sobre la base de diferenciales de tasa pactadas y por cobro de comisiones por operación.

Los productos que se ofrecen en el sector financiero son muy variados, pero en cualquier Casa de Bolsa se ofrecen los mismos productos con ganancias en general muy semejantes. Por esto, cada institución financiera se debe preocupar por ofrecer un extra en sus productos para hacerlos más atractivos a los clientes.

En estos tiempos de tanta competencia bursátil, los clientes además de buscar buenos rendimientos por el capital que invierten, buscan también que la empresa con la que hacen operaciones bursátiles les ofrezca servicios adicionales personalizados como son: Asesoría en sus inversiones, Información clara y oportuna sobre el mercado financiero y también rapidez en sus transacciones.

Por esto se hace importante la utilización de infraestructura de punta para ofrecer a los clientes ese servicio que buscan en las empresas financieras. El avance en las herramientas informáticas y las comunicaciones, permiten la interacción entre diferentes negocios, esto es, permite el eficiente intercambio de información, el poder lograr cerrar operaciones financieras electrónicamente, además de poder compartir clientes afines a cada uno de los negocios.

El gran avance que ha tenido la tecnología en herramientas informáticas y de comunicaciones ha dado a las empresas la facilidad de:

- Intercambiar información de interés mutuo
- Cerrar operaciones financieras electrónicamente
- Compartir clientes afines buscando siempre un servicio más completo.

Uno de los problemas con que se enfrentó la Casa de Bolsa, fue el querer intercambiar información con el Banco del Grupo para dar un servicio completo a sus clientes al liquidar operaciones bursátiles, pero la plataforma informática del Banco estaba montada sobre IBM, y como es bien sabido, IBM monopolizó sus productos y no los diseñó para que fueran compatibles con las otras tecnologías que estaban en el mercado. La tecnología Informática de Casa de Bolsa está montada sobre un Tandem y por lo tanto la comunicación TANDEM - IBM no se puede lograr utilizando los protocolos estándar del mercado.

Cuando IBM empezó a perder mercado por lo cerrado de sus productos, diseñó una herramienta con la cual sus productos pudieran convivir con otro tipo de tecnologías. Así nace SNAX/APC el cual fue diseñado para que cualquier aplicación no propia de IBM pudiera comunicarse con aplicaciones de IBM.

El lograr tener un medio para enlazar aplicaciones TANDEM - IBM benefició notablemente el servicio de liquidación de efectivo en Casa de Bolsa ya que el tiempo de respuesta para cerrar una transacción bursátil bajó de 2 hrs a 30 seg. aproximadamente. Con la implementación del sistema de Líneas Automáticas la Casa de bolsa redujo sus costos administrativos notablemente ya que anteriormente se necesitaban 4 personas para administrar el flujo de efectivo entre Casa de Bolsa y el Banco y ahora si la operación no tiene ninguna anomalía es totalmente automático el flujo.

Ejemplos como éste nos da la pauta para afirmar que la explotación de la tecnología informática y de comunicaciones en beneficio de las empresas es necesaria desde cualquier punto de vista, y que la no-utilización de esta tecnología podría ser la diferencia entre el éxito de una empresa o el fracaso. Tal vez en un principio el uso de la tecnología nos cueste un poco de trabajo ya que siempre esta la renuencia a la utilización de algo nuevo y novedoso, pero los beneficios que esto nos traerá justificarán la inversión de tiempo, dinero y esfuerzo que nos costó incorporar la nueva tecnología a nuestros negocios.

Las empresas de hoy entienden que los cambios tecnológicos representan el camino para crecer y mantenerse competitivos ante un mercado cambiante y demandante de más y mejores servicios.

Obstáculos de la Modernización

El atractivo comercial de las cosas tiene que ver no solamente con que sea la solución más eficiente, sino que esté al alcance de las personas o instituciones. Si el costo de la mejor solución es prohibitivo, muy pocos la van a obtener. Por lo tanto, el principal obstáculo de ese tipo de tecnología es el costo. No todas las instituciones se pueden actualizar, si acaso los bancos, las petroleras y algunos centros de investigación. Sin embargo, las universidades se están quedando atrás por la falta de fondos, y cuando se tenga acceso a ese tipo de tecnología, ya será obsoleta.

Muchos manejan estos conceptos de manera teórica, y quizás han tenido experiencia práctica en otros países, pero aquí el problema es el costo.

La mayoría de las empresas están reacias a invertir en este tipo de tecnología y son muy cuidadosas, ya que se trata de grandes inversiones y quizás no ameriten un cambio tan drástico en las prestaciones porque hasta ahora han sido eficientes. Pero en el futuro, cuando crezca la demanda de Internet llegará el tiempo en que

se tenga que actualizar. Si requerimos desarrollarnos como país y estar al día necesitamos invertir.

Hasta la fecha las llamadas redes Gigabits son una especificación. En computación se trabajó mucho sobre especificaciones y modelos, no es que el fabricante de productos lo tengáse que hacer así, es simplemente el medio de referencia. Por ejemplo, ATM fue una especificación pero ahora es algo tangible, las empresas están fabricando productos que cumplen y se ajustan a esa especificación.

Dentro de esta tendencia para mejorar el flujo e intercambio de información, la arquitectura de las computadoras no se puede escapar. Ahora están tratando de elevar las velocidades de los procesadores, mejorar el bus de sistema de 66 MHz a 100 MHz.

Si el procesador de una PC, por ejemplo, va a 400 MHz y el bus a 66 MHz se crea un cuello de botella que debilita el rendimiento que pudiera tener el equipo. Antes se tenía un bus común para todos los componentes. Hoy en día existen buses locales como la especificación PCI de Intel, que tiene uno dedicado a la tarjeta y a la memoria de video y otro para los demás componentes. Cuando la tarjeta de video necesita transferir memoria al monitor entonces accede de manera directa sin tener que pasar por el bus.

Se esta estudiando la posibilidad de hacer memorias RAM más rápidas. Por ahora se encuentran en el orden de los 70 y 60 ns, y lo ideal seria 10 ns. Que es la velocidad que tiene la memoria caché.

Tendencias a Corto Plazo

Redes públicas, mayor fluidez, aplicaciones corriendo en Web, cableado estructural, fibra óptica y switches de capa 3 son algunas de las tendencias que vislumbran a futuro en el terreno de la conectividad.

La TI (termino para la tecnología de información, el amplio tema referido a todos los aspectos de la información de manejo y de proceso, especialmente dentro de una organización o de una compañía grande) ha respondido últimamente a la estructura y necesidades de los negocios pero el nuevo motor es ahora la Red Pública Internet, ya que replantea la manera de hacer negocios, desarrollar aplicaciones y construir redes, además de marcar nuevos estándares.

El protocolo de Internet (IP) se ha convertido en el protocolo por excelencia en el ambiente LAN y WAN, limitando a otros productos a soportar aplicaciones heredadas o muy especializadas.

De ahí se desprenden las tendencias que regirán el mundo de las redes y la conectividad en los próximos años.

Tendencias:

Características que definirán el papel de las nuevas tecnologías.

- Las corporaciones migrarán a arquitecturas Intranet/ Extranet.
- El patrón de tráfico actualmente dividido en 80 por ciento para LAN y 20 por ciento para WAN, se modificará hasta que dichos porcentajes estén 20-80
- En cuanto a los servicios telefónicos, se migrarán de Conmutadores de circuitos a Conmutadores de Paquetes en Redes Públicas
- El ancho de banda en última milla será cada vez más crítico y habrá nuevas tecnologías
- Aumentará la demanda por acceso remoto sobre redes públicas, así como la necesidad de seguridad, compatibilidad y desempeño
- Se solicitarán servicios de voz, fax, datos y video
- Incrementará la demanda por el manejo de características de seguridad como autentificaciones, firewalls y encriptaciones.

Lo que Permanecerá

El cableado estructurado (UTP) y la fibra óptica seguirá siendo los medios físicos de transporte en las redes corporativas del 2000. Las redes LAN se manejarán con Ethernet y Fast Ethernet, y las redes WAN con Gigabit Ethernet.

En el caso de WAN, consideramos que la fibra óptica y el cobre seguirán dominando. Creemos que en México las nuevas Tecnologías para enlace terrestre como el xDSI o el modem todavía tardarán años en convertirse en una alternativa viable.

Sin embargo, no descartamos la posibilidad de que surjan alternativas inalámbricas accesibles y variables.

Retos

El proceso de transición de las redes actuales a las redes optimizadas IP del futuro tiene que darse cubriendo las expectativas del usuario, el técnico y el directivo.

El usuario espera que dicha transición sea invisible y no interrumpa sus operaciones; el técnico, por su parte, espera una solución segura, fácil y administrable. Por último, el directivo desea obtener ventajas estratégicas en sus aplicaciones de misión crítica.

Construir una nueva red sin interrumpir las operaciones actuales y sin perder la inversión implica muchos retos, entre los que se encuentra la necesidad de dar al IP mayor fluidez y los recursos que demanda, ofreciendo servicios de calidad a los protocolos heredados.

Lo anterior se puede lograr mediante soluciones disponibles como los Switches de Capa 3 y en un tiempo no muy lejano Internet2 (concepto que se definirá más adelante). Donde se podrán ampliar los servicios con: integración de voz, fax, datos y vídeo sobre IP, y switches Extranet que integran el acceso simultáneo de hasta 2000 enlaces a una Intranet.

Un profesional es alguien que tiene responsabilidad por su trabajo. En la empresa tradicional, si usted es mi gerente, aunque yo haga el trabajo usted es el responsable. Un profesional es alguien que entiende el negocio, sabe lo que hace la demás gente, tiene responsabilidad por los resultados y se preocupa por el cliente. Un trabajador es alguien que sigue órdenes.

Las organizaciones tradicionales tienen gerentes que piensan y trabajadores que trabajan. No podemos sostener eso por más tiempo. Ahora necesitamos profesionales que piensen y trabajen. Y eso se aplica lo mismo en la fábrica que en la oficina de ventas o en la de servicio al cliente; en todas partes. Estamos viendo cómo sucede esto en muchas industrias.

La única manera de crear valor para el accionista es primero creando valor para el cliente. El cliente tiene que ser la primera preocupación.

En la actualidad se considera a la herramienta en sí misma, como transportadora o vehículo del conocimiento.

1. Aplicar el conocimiento como inteligencia. Usar el conocimiento del mercado, o información, para tomar ventaja de las oportunidades de negocios. Como las cotizaciones matutinas de las acciones, estas especulaciones competitivas tienen una vida muy corta de altibajos. Actúe rápidamente sobre el mercado para golpear a la competencia.
2. Usar el conocimiento para persuadir. Publicar poderosas piezas de información para crear demanda.
3. Controlar la plataforma del conocimiento. Hacer del conocimiento los bienes y raíces que todo el mundo debe utilizar.
4. Vender el conocimiento como un producto. No obstante que los productos de conocimiento han existido por siglos, en forma de enciclopedias y otras fuentes de referencia, en el siglo XX los revendedores de conocimiento pueden crear productos de tecnología que estandarizan cuerpos completos de conocimiento. Estos regatones del conocimiento que ofrecen sus productos en el Web pueden enganchar de manera instantánea grandes poblaciones de clientes.

Los sucesores de Internet

Internet 2 (I2) y next Generation Internet (NGI) son ya una realidad y, contrario a lo que parecería no ha requerido de grandes inversiones ni su desarrollo ha durado décadas. En ambos casos los presupuestos no exceden los 500 millones de dólares.

El vínculo entre ambos proyectos es el trabajo y las investigaciones de más de un centenar de universidades, algunas tan importantes como Stanford o la UCLA. Sin embargo, también participan empresas de alta tecnología.

Para muchos analistas NGI es el "Internet Particular" del gobierno estadounidense, empezando por el financiamiento, el cual proviene de entidades como el Departamento de Energía, la NASA o el Departamento de Defensa.

La participación del Pentágono no resulta extraña (aunque se guarde discreción sobre ella). El Ejército fue el principal promotor de Internet "tradicional" aunque luego cediera su control a las universidades y al público en general.

Con un enfoque muy pragmático las universidades se han acercado a las grandes firmas de computación y telecomunicaciones para que apoyen los proyectos. A corto plazo no será raro que ambas redes se encuentren disputando los mismos patrocinios y sean respaldadas por las áreas de investigación corporativas.

Los estadounidenses parecen haber tomado conciencia de que si no asume la delantera en telecomunicaciones, su liderazgo mundial podría tambalearse, en especial frente a una Europa que va despertando de su letargo en tecnología.

Respecto a lo anterior. Basta considerar empresas como la holandesa Philips, que va de los electrodomésticos a los radiolocalizadores; la finlandesa Nokia, que conquista posiciones cada vez más importantes en telefonía celular o SAP AG, firma de software de ERP (Enterprise Resource Plannig; Planeación de los recursos empresariales).

Mexicanos en la nueva red

En tecnología, los proyectos para públicos muy limitados están condenados al fracaso si no terminan por masificarse, pues a mediano plazo el dinero resulta insuficiente para mantenerlos. Ya se ha observado que tecnologías atractivas e interesantes no resultan exitosas si no logran ventas masivas. Dos ejemplos de ello son el disco láser (creado por Philips) y el mini disc (de Sony). Ninguno ha recuperado lo que se invirtió en ellos.

De esa manera, los promotores de NGI e I2 han considerado abrirlos en dos o tres al comercio electrónico y que éste los haga autofinanciables. Estos ingresos permitirán a las instituciones educativas disponer de recursos para desarrollar contenidos con video tridimensional y sonido estereofónico, laboratorios virtuales teleducación, entre otras.

Aunque I2 es un proyecto estadounidense, un número reducido de universidades de otras nacionalidades, entre ellas mexicanas, tendrán acceso al proyecto, lo cual se espera que ocurra en este año.

Entre las instituciones nacionales participantes se encuentran algunas públicas y privadas como Universidad Nacional Autónoma de México (UNAM), Universidad de Guadalajara ((UdeG), Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) y la Universidad de las Américas.

La selectividad del grupo no se debe sólo al costo de instalar en México un Gigapop (Gigabit Point of Presence; switch que facilita la interconexión local), sino a que las universidades deben presentar programas de investigación que se verían beneficiados con el acceso a I2.

Los Gigapop representan una de las principales ventajas de I2 sobre la actual Internet, pues la información puede moverse 100 veces más rápido . Pero eso no es todo: será posible identificar y clasificar los servicios según sus requerimientos de calidad, lo que permitirá diferenciar las tarifas que se cobrarán a los usuarios, una vez que estén abiertos para uso empresarial.

En cuanto a NGI, la tecnología empleada son redes ópticas, así como switch y ruteadores de gran velocidad y tecnología multicast.

Todo indica que la libertad que hasta ahora ha gozado Internet se reflejará en ambos proyectos, pues se busca que los protocolos sean abiertos.

Un último detalle: no hay que despedirse de Internet "tradicional" pues ni NGI ni I2 buscan sustituirlo, sino complementarlo. Habrá que ver los primeros resultados en 1999.

BIBLIOGRAFÍA

Santos, Ángeles Olalla, Curso de ATM, Redes ATM, http://a01-unix.gsyc.inf.uc3m.es/~bluff/mi_practica.html

Commer, Douglas E., Redes globales de información con internet y tcp/ip, Prentice-Hall, 1996

Coran, Carlos Marlon, Estudio del impacto de la seguridad en el desempeño de internet, Universidad de los Andes, 1997

Coran, Marlon y León, Diego Mauricio, Seguridad para aplicaciones distribuidas, Universidad de los Andes, 1995

Estopier, David B., Curso de señalización y la RDSI, UNAM

Ferrera, William y Marinho, José Fabio, Redes locales de computadoras, McGraw-Hill

Guirao, P., Diccionario de informática, Ediciones prisma

Madron, Thomas W., Redes de área local, siguiente generación, Megabyte Grupo Noriega Editores

Meneses, J.C. y C., Reichert, Redes de conmutación rápida de paquetes, Universidad de los Andes, 1995

Stallings, William, Bussines data comunication, Macmillian Publising Conpany, 1990

Sustaita, Fernando, Aprenda.mos redes lan, Microasist, 1993

HEMEROGRAFÍA

Canales TI, Internet 2 en busca de mejores servicios, Leticia Zamora, año 2, marzo 1 de 1999, no. 71, pp 26-27

Canales TI, Oportunidad comercial en internet 2, Marlene Nava, año 2, marzo 15 de 1999, no. 73, pp 22-24

Computerworld, Innovación en redes: un problema de costo, César Laya Montes, año 19 Núm. 600, Enero 25-29 de 1999, pp B10-B11

Computerworld, Tendencias a corto plazo en conectividad, Lizzette Pérez Arbesú, año 19 Núm. 600, Enero 25-29 de 1999, p A7

Computerworld, Cómo convertir el conocimiento en lucro, Leonard M. Fuld, año 19 Núm. 602, Febrero 8-12 de 1999, p D16

Expansión, Ahora necesitamos profesionales que piensen y trabajen, Ernesto Flores Vega, Grupo Medcom, México, 1998, edición especial, pp 4-9

Red, revista de redes de computadoras, Breve historia de las redes locales, Ing. Luis Rueda Toledo, año 94, El ABC de las redes locales, pp 1-2

Red, revista de redes de computadoras, Visión comparativa de diversos tipos de redes locales, Ing. Marcelino Gómez Velasco, año 94, El ABC de las redes locales, pp 4-8

Red, revista de redes de computadoras, Proceso distribuido, Ing. Rafael Fernández Corro, año 94, El ABC de las redes locales, pp 13-18

Red, revista de redes de computadoras, Protocolos y estándares de las redes locales, Ing. Rafael Gálvez, año 94, El ABC de las redes locales, pp 27-28

Red, revista de redes de computadoras, Cables para redes locales, Ing. Alejandro Ramírez, año 94, El ABC de las redes locales, pp 32-34

Telesoluciones, México en la era de las comunicaciones Personales y multipartitas (Multicast), Felipe R. Manchaca G., sep. 1998, Xview, S.A. de C. V., pp 22-24

3TECH, The big three contenders: FDDI, ATM and Fast Ethernet, George Prodam, Sept 1993, Vol. 4, No 3, pp 11-17

MANUALES

Facultad de ingeniería, UNAM, Introducción a las redes lan de micros, 1995

Facultad de ingeniería, UNAM, Redes lan de microcomputadoras, 1995

IBM corporation, Education and training, Client Access/400 dos implementation with additional topics, 1995

IBM corporation, Education and training, Comunicaciones TCP/IP entre AS/400, 1994

IBM corporation, Education and training, AS/400 comunication introduction, 1995

IBM corporation, Education and training, IBM en internet, 1997

IBM corporation, Education and training, IBM lan system, 1992

INEGI, red, Curso básico de comunicaciones, 1994

Microsoft Corporation, Enciclopedia encarta, 1998

Microsoft Corporation, SNA Server R. Conectivity for IBM, 1995

Microsoft Corporation, Microsoft SNA server 2.11 reviewer's guide, 1995

Publicaciones IBM, SNA technical overview, 1997

Publicaciones IBM, Lan basics cours, 1997

Tandem Computer Incorporated, SNAX/APC Management Programming Manual, 1992

Tandem Computer Incorporated, SNAX/APC Application Programming Manual, 1992

Tandem Computer Incorporated, SNA Networking and data Comunicaions, 1995

Tandem Computer Incorporated, Introduction to SNA capabilities of tandem System, 1992

Tandem Computer Incorporated, SNAX Connection Manager Manual, 1995

Tandem Computer Incorporated, Tandem system review, 1990