UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

DISEÑO DE UNA RED DE DATOS CONVIVENCIA ENTRE REDES NOVELL, UNIX Y EQUIPO AS400

(DISEÑO DE LA RED CORPORATIVA DE CASA DE BOLSA BANCOMER)

T E S I S

Que para obtener el Título de

INGENIERO EN COMPUTACION

P r e s e n t a n:

LUIS PIÑA SANTANA
JESUS AYALA MARTINEZ
ALFONSO TRILLO VAZQUEZ
ALEJANDRO HERNANDEZ RODRIGUEZ
JORGE ROLANDO RODRIGUEZ ARIANO

DIRECTOR:

ING. ROCIO ROJAS MUÑOZ

México, D.F. 1995

A LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

A nuestra ALMA MATER; la máxima casa de estudios, la cual nos abrió la puerta de su recinto y nos distinguió con el título de UNIVERSITARIOS que orgullosamente ostentamos y defenderemos para el bienestar social.

A LA FACULTAD DE INGENIERIA

A nuestra querida FACULTAD, de la cual honorosamente nos consideramos sus hijos, donde nos formamos y de donde surgimos como profesionistas.

A LOS PROFESORES DE LA FACULTAD

Por brindar generosamente el don de sus conocimientos a todos sus alumnos.

A NUESTRA DIRECTORA DE TESIS LA ING. ROCIO ROJAS MUÑOZ

Por toda la ayuda y paciencia que nos brindó durante la relización de este trabajo. Gracias.

1. INTRODUCCION

I. INTRODUCCION

En nuestros días un factor clave para el éxito de las empresas, es contar con información oportuna, accesible al mayor número de personas, en todos los niveles de la organización. El amplio desarrollo de la tecnología en sistemas ha permitido que la información se encuentre mas cerca del usuario que la necesita, evolucionando de esquemas centralizados a esquemas de información distribuida.

La tendencia de los sistemas de información basados en computadoras, ha sido pasar de los antiguos y sofisticados sistemas de cómputo centralizados a una tecnología más flexible, donde el almacenamiento y procesamiento de la información pueden ser distribuidos en varios equipos. En gran medida esto ha sido posible gracias a las redes de computadoras, que permiten a usuarios ubicados en sitios diferentes compartir información y recursos.

En la actualidad la mayoría de empresas medianas y grandes poseen una o varias redes de área local (**LAN**) , y sistemas de cómputo centralizados, esto, ha creado la necesidad de *intercomunicar* a las redes de las diferentes oficinas o departamentos con los sistemas de cómputo de la empresa, para crear una red de computadoras mas amplia, donde los usuarios puedan accesar múltiples aplicaciones sin necesidad de cambiar de terminal o equipo.

Las redes de área local , permiten a un grupo de usuarios de computadoras comunicarse uno con el otro y compartir información y dispositivos periféricos. Los usuarios de una LAN en particular se encontrarán ubicados típicamente muy cerca entre sí, posiblemente en el mismo edificio, en el mismo piso, o en la misma oficina. Las LAN son usadas comúnmente para permitir a miembros del mismo grupo de trabajo o departamento trabajar en cooperación y permitirles compartir recursos, especialmente información.

Las LAN han probado ser muy efectivas en cuanto a permitir el intercambio de información dentro de un grupo de trabajo o departamento. Pero los grupos de trabajo también necesitan comunicarse y compartir información fuera de su propia área, como por ejemplo con otros grupos de trabajo, con otros departamentos dentro de su misma empresa, con otras empresas, o con otras fuentes de información pública. Utilizar redes o facilidades de comunicación que sean separadas (exclusivas), para cada una de estas necesidades es posible y, es el enfoque usado en muchos casos. Sin embargo, *interconectar* redes puede proporcionar una opción más rápida, menos cara y más fácil de usar para resolver este problema.

Los beneficios de este modelo se reflejan en mayor productividad de los usuarios, al contar con información oportuna en su escritorio, así como en una reducción en los costos de los equipos, debido a que la inversión en una red de computadoras es significativamente menor que la requerida por un sistema de cómputo centralizado.

Por la necesidad de contar con una infraestructura de cómputo de vanguardia tecnológica y para obtener los beneficios de comunicación e intercambio de información entre todos los

usuarios de sistemas nació el presente trabajo para ofrecer una solución unica y estándar para sus esquema de cómputo.
En el capítulo de Antecedentes se discutirán los aspectos más importantes de las redes de computadoras utilizadas actualmente, así como los elementos necesarios para su interconexión. Se revisará la estructura del modelo OSI. Como punto importante se revisará las características de los medios de transmisión, de las topologías de red y dispositivos de interconexión.
En el capítulo de Diseño Global de la Red Corporativa revisaremos y tomaremos las consideraciones y recomendaciones generales para el diseño de la red. Las recomendaciones que se darán serán para seleccionar las topologías de las redes y los elementos de hardware.
Dentro de este mismo capítulo en el apartado de Redes de Area Local (LAN) se explicará como fue estructurado el diseño de dichas redes. Se hablará de la integración de las redes y el sistema AS/400 y como se fué dando está en el transcurso del diseño.

En el apartado de Red de Area Amplia (WAN) se menciona como se realizó la conexión de las redes locales a través de una WAN utilizando enrutadores como dispositivos principales de comunicación.

En el capítulo de Administración de la Red, se trata el aspecto de la administración de las redes y su importancia debido a la complejidad que tiene administrar dispositivos separados en diferentes localidades. También se mencionan algunas herramientas a utilizar para la administración.

2. PROBLEMATICA

2.PROBLEMATICA

El proyecto "Diseño de la Red Corporativa de Casa de Bolsa Bancomer (CBB)" nació por la necesidad de contar con una plataforma tecnológica acorde a sus necesidades, que les permitiera obtener una posición sólida en el mercado financiero nacional. Al visualizar las tendencias tecnológicas se solicitó una propuesta que incluyera lo último en tecnología y que cuidara la inversión realizada en algunos equipos como el AS/400.

A continuación se citan los aspectos más relevantes que CBB presentaba antes del proyecto.

ISLAS DE INFORMACION (COMPUTADORAS PERSONALES AISLADAS).
En el edificio corporativo se tenían instaladas más de veinte computadoras personales en configuración "stand alone", con software de oficina de diferentes versiones, esta situación se repetía en los demás edificios de la institución, desaprovechando la posibilidad de compartir información y recursos.

SISTEMA AS/400.
Para accesar el equipo AS/400, los usuarios debían de tener además de su computadora personal, una terminal exclusivamente para realizar las consultas a las aplicaciones del sistema AS/400. Esto limitaba el espacio de trabajo de cada uno de los usuarios.

TIPO DE CABLEADO.
En el edificio corporativo se tenía un cableado, que no cumplía con los requerimientos para red local de Ethernet y Token-Ring para transmitir datos a las velocidades de 10 y 16 Mbps.

SEGURIDAD DE LA INFORMACION.
Considerando la importancia de la información se requiere tener medidas de seguridad confiables y eficientes. En CBB se compartía la información a través de discos flexibles (diskettes), los diskettes no son un medio suficientemente confiable, ya que estos tienen mayor probabilidad de falla que los discos duros. No existía seguridad para la información confidencial, y se corría el riesgo de que diskettes infectados con virus podían ser tranportados de computadora en computadora sin un control ni proceso de vacunación.

No se realizaban respaldos de la información en forma periódica, algunos de los usuarios realizaban respaldos parciales en diskettes. Con el inconveniente de que se podían presentar fallas al recuperar la información y duplicidad en los respaldos.

SOFTWARE.
El software instalado se tenía que actualizar con las nuevas versiones en cada una de las computadoras personales. Esto ocasiona pérdida de tiempo y posibles deficiencias en las configuraciones, sin considerar el costo por actualización o licencia.

ACCESO A LA INFORMACION DE LA BOLSA MEXICANA DE VALORES.
En algunas estaciones de trabajo se recibía el software INFOSEL, el cual es un software financiero que se recibe durante el día, con información de la Bolsa Mexicana de Valores y noticias económicas del mundo. También reciben por medio del mismo software información

de indicadores económicos de México y el comportamiento de las bolsas de valores en otros países. En lo que respecta a estas estaciones que recibían el Infosel, la señal era dividida para repartirla entre todas las estaciones, razón por la cual la señal se debilitaba y ocasionaba interrupciones eventuales en algunas de las estaciones. El cableado que se utilizaba para llevar la señal de Infosel a los usuarios era del tipo coaxial y presentaba mucha dificultad para relocalización y movimiento de servicios.

IMPRESION
Los usuarios que no tenían impresora conectada localmente, necesitaban llevar una copia del archivo en diskette e imprimir en otra máquina que tuviese impresora, esto representaba molestias a otros usuarios, además de que la información confidencial podía ser leída por otras personas.

Además de todos los servicios descritos anteriormente se tenía contemplado un proyecto de Análisis Bursátil el cual les permitiera tener información al detalle de las operaciones de la Bolsa y distribuirla a todos los usuarios que lo necesitarán para su trabajo.

Debido a las condiciones señaladas anteriormente, se propone como solución global el establecer un esquema de comunicación por medio de una red de dimensión corporativa, para poder compartir información y recursos, eliminando las islas de información al integrar todas las computadoras en "stand alone" permitiendo además tener en un mismo equipo las aplicaciones del AS/400, UNIX y los sistemas propios de una computadora personal, eliminando la duplicidad de equipo en los escritorios. La seguridad y confidencialidad de la información se garantiza a través de una adecuada administración de la red, con el uso de contraseñas para restringir el acceso de los usuarios. Al implementar una red corporativa se evita el traspaso de información vía diskettes, ya que desde cualquier punto de la red es posible transferir y compartir información. Al tener acceso a información y aplicaciones compartidas, se elimina la necesidad de instalar y actualizar las diferentes aplicaciones ubicadas en cada equipo.

En el presente trabajo de tesis se exponen las bases teóricas que soportan el diseño de las redes locales y la red de área amplia, mismo que se detalla posteriormente, conformando el esquema de la red corporativa de la Casa de Bolsa Bancomer.

3. ANTECEDENTES

3. ANTECEDENTES

En este capítulo se discutirán los aspectos más importantes de las redes de computadoras utilizadas actualmente, así como los elementos necesarios para su interconexión. Se revisará la estructura del modelo OSI, el cuál sirvió como base teórica en la división de la arquitectura de la red. Como punto importante se revisaron las características de los medios de transmisión como tipo de cables, el cuál sirve para elegir el cableado a utilizar en las redes. Se realizó una revisión de las topologías de red, para tomar una decisión sobre la mejor topología a seguir en la implementación de las redes. La revisión de los protocolos de red, brindó el parámetro de selección de los protocolos de comunicación, tomando en cuenta su posibe comunicación en redes amplias. En la parte de dispositivos de interconexión se revisan los diferentes tipos que existen para entender el porqué se utilizan algunos de estos y la parte en que van a ser utilizados en el diseño del presente trabajo de tesis.

3.1 MODELO OSI

La Organización de Estándares Internacionales (ISO, por sus siglas en inglés) inició en 1977 la definición de un modelo de referencia llamado el **Modelo de Interconexión de Sistemas Abiertos** (el modelo OSI), que divide la arquitectura de la red en siete capas, cada una con funciones específicas independientes de las demás.

En este modelo, la capa N en una computadora realiza sus funciones comunicándose con la capa del mismo nivel (llamada entidad par) en la otra computadora. La comunicación entre entidades pares se lleva a cabo a través de reglas bien definidas --los **protocolos**-- para una arquitectura de red particular. Las funciones de la capa "N" sirven para que ésta pueda ofrecer un **servicio** a la capa inmediatamente superior en la misma computadora. De esta manera se van agregando servicios conforme se asciende por las capas de la arquitectura hasta llegar a la capa de aplicación, de donde los procesos de nosotros, los usuarios de la red, obtienen sus servicios.

El modelo OSI no define protocolos ni servicios, éstos dependen de la implementación específica a cada arquitectura de red. Lo que el modelo define es la función que debe realizar cada capa.

Es con la capa de aplicación que interactúan los usuarios finales de la red. En ella residen los procesos que otorgan los **servicios de red**, tales como correo electrónico y transferencia de archivos. Para ofrecer estos servicios, los procesos de la capa de aplicación también se comunican entre sí siguiendo un **Protocolo de Aplicación**.

Brevemente, OSI se divide en siete capas, las cuales tienen acceso a tres categorías:

- Física
- Comunicaciones
- Servicios

Las capas estan enlistadas en orden de complejidad, cada una de las capas subsecuentes estan construídas en su nivel inferior, las Capas 1 y 2 son las de abajo. También cada una de las capas solamente se puede comunicar con la capa que esta por debajo de ella.

Física:
Las dos primeras capas del modelo OSI forman el hardware y el nivel bajo del software de una red: el cable, los conectores y los "transceivers". los niveles de voltaje de corriente, el hardware que se comunica con cable (normalmente esta en una tarjeta de la computadora pero en algunos casos se encuentra en un grupo de chips) y el software que maneja las comunicaciones entre la computadora y el cable (frecuentemente almacenado en una tarjeta). La Capa 1 tiene las especificaciones del hardware y la Capa 2 contiene el software.

La clase de red que se esta empleando y como son mandados y recibidos los datos por el cable depende de la clase de tarjeta de la interface de la red que uno tenga en su sistema: Ethernet, o Token-Ring por ejemplo.

La tarjeta contiene la conexión física del cable a la computadora, frecuentemente también contiene el software que maneja, por lo general extendido a un bajo nivel de comunicaciones del cable a la computadora. Este software de bajo nivel esta diseñado para mantener una conexión confiable entre los nodos adyacentes.

Capa 7: *Aplicación*(Protocolo empleado por una aplicación)
Capa 6:*Presentación* (Código de aplicación programada, conversión de datos)
Capa 5: *Sesión* (Mantenimiento de la unión de datos entre nodos)
Capa 4: *Transporte* (Manejo de error/retransmisión de datos)
Capa 3: *Red* (La ruta de los datos)
Capa 2: *Unión de datos* (Hardware/software que dan acceso y manejan el cable)
Capa 1: *Física* (Cableado, señal intensa)

Capas del Modelo OSI.

Es usual en las redes de área local que el cable sea de cobre (trenzado o alambre coaxial), el cable de fibra óptica esta ganando popularidad conforme su precio ha disminuído.

Los dos primeros niveles son solamente capas de hardware en el modelo OSI, las otras cinco son software y una parte de la Capa 2 es software también.

Comunicaciones
Las Capas 3 y 4 especifícan como los datos son ruteados y como pueden ser corregidos los errores, estas dos capas se refieren a protocolos de comunicación y son controlados por drivers de software. El driver del protocolo de comunicaciones (software) de NetWare se denomina ***IPX***, estas letras aparecen en la pantalla cada vez que bootea el sistema. IPX es para el intercambio de paquetes con la red (intercambio de paquetes secuencial), el cual es una manera de identificar la red, la dirección de la estación y la aplicación.

La capa 3 controla el canal de datos entre dos huéspedes, si su red es pequeña, con solamente un servidor de archivos, esta capa relativamente no tiene importancia. La tiene cuando uno se enfrenta a una área ancha de redes, con protocolos diferentes. Un protocolo de comunicación que usualmente corre en una área ancha de red es el TCP/IP. El TCP/IP y el IPX pueden comunicarse con cualquier otro, lo cual no es fácil. NetWare maneja esta clase de intercambio de comunicaciones de redes a través de Puentes y Gateways, estos se describirán posteriormente.

Servicios:
Las últimas tres capas del modelo OSI proveen servicios a las aplicaciones, específicamente para el establecimiento y el fin de una sesión de comunicación (Capa 5), una forma de traducir el formato de los datos de tal modo que tanto el que envía como el que recibe pueden entender (Capa 6) y los protocolos para las aplicaciones finales del usuario incluyendo el mismo NetWare (Capa 7). Los protocolos afectados por la Capa 7 incluyen E-mail y un remoto acceso a la red, entre otros.

Las Capas 6 y 7 usualmente son implementadas por el MS-DOS (u OS/2) y por el NetWare, mientras que el BIOS de la red (NetBIOS) maneja el establecimiento y el fin de una sesión de comunicación. El NetWare a diferencia de otras redes (específicamente el Manejador LAN) no depende de NetBIOS, éste pasa los requisitos de establecimiento y fin a IPX.

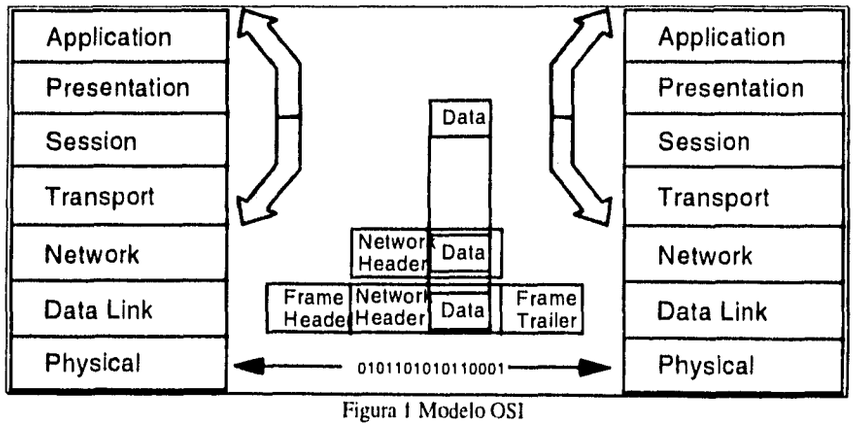

Figura 1 Modelo OSI

3.2 MEDIOS DE TRANSMISION

Para transmitir información binaria sobre una línea de transmisión, los dígitos binarios que conforman cada elemento a ser transmitido deben ser convertidos físicamente a señales eléctricas. Por ejemplo, un número binario 1 puede ser transmitido aplicando una señal de voltaje (o nivel) con amplitud de $+V$ volts en la terminal emisora de una línea de transmisión y un binario 0 puede transmitirse aplicando $-V$. En la recepción de tales señales, el

dispositivo receptor deberá interpretar un voltaje de +*V* como un dígito binario 1 y un voltaje de -*V* como un 0. En la práctica, sin embargo, las señales eléctricas transmitidas pueden llegar a atenuarse (disminuír en tamaño) y a distorsionarse (perder su forma original) debido a la naturaleza imperfecta del medio físico de transmisión. Esto tiene el efecto de que el receptor es incapaz de discriminar entre una señal de 1 o de 0. El grado de afectación sobre la señal se ve influenciado por factores tales como:

- el tipo de medio de transmisión
- la cantidad de bits que se están transmitiendo; y
- la distancia entre los dos dipositivos que se estén comunicando.

La transmisión de una señal eléctrica entre dos piezas de equipo requiere del uso de un medio de transmisión, el cual normalmente toma la forma de una línea de transmisión. En la mayoría de los casos, ésta consiste de un par de conductores o cables; sin embargo, la transmsión es algunas veces lograda al pasar un haz de luz a través de una pieza de fibra de vidrio o una onda electromagnética a través del espacio. El tipo de medio de transmisión usado es importante, dado que determina la cantidad de bits (razón), en términos de dígitos binarios (bits) por segundo o bps, de información que puede ser transmitida.

Líneas abiertas de dos cables

Una línea abierta de dos cables es el tipo más simple de medio de transmisión. Cada cable es aislado del otro y ambos se encuentran expuestos al exterior. Este tipo de línea es perfecta para conectar dos piezas de equipo que tienen una separación física muy corta (menos de 50m) y una razón de transmisión que sea modesta (menos de 19.2 kbps). La señal, que es un voltaje, el cual está relacionado típicamente a alguna referencia a tierra, es aplicado a un cable mientras la referencia es aplicada al otro.

Aunque una línea de dos cables puede ser utilizada para conectar dos dispositivos DTEs directamente, es usada principalmente para conectar un DTE a una pieza local de DCE, un modem por ejemplo. Como se sabe, las conexiones de este tipo necesitan más de un par de líneas; el arreglo más común utiliza un cable aislado para cada señal y un cable aparte para la señal de referencia de tierra que será común. El juego completo de cables puede estar contenido dentro de una protección a este conjunto se le llama cable multicore o puede encontrarse en la forma de cable plano.

Con este tipo de líneas, se necesita tener cuidado para evitar cortos entre líneas que se encuentren próximas en el mismo cable. Además de lo anterior existe algo conocido como crosstalk y es causado por el acoplamiento capacitivo entre dos cables. Además, la estructura abierta de este tipo de líneas las hace susceptibles de recoger señales de ruído de otras fuentes de señales eléctricas provocadas por radiación electromagnética. El principal problema con las señales de interferencia de este tipo es que sólo pueden ser recibidas en un cable, el cable de señal, por ejemplo, y no el cable de referencia. Como resultado, puede generarse una señal de diferencia adicional entre los dos cables y, como el receptor normalmente opera utilizando la diferencia de señales entre los dos cables, esto podría dar lugar a interpretaciones erróneas de la señal combinada (la señal original más el ruído) que

se recibió. Estos factores contribuyen al límite que estas líneas ofrecen en cuanto a longitud y razón de transmisión para ser usadas de una manera confiable.

Líneas de par trenzado

Se puede obtener una mejor inmunidad relativa a ruídos en las señales, conocida como inmunidad al ruído, si se emplean un par de alambres que están trenzados entre sí. Esto es conocido como línea de par trenzado. La proximidad cercana resultante entre la línea de referencia y la de señal significa que cualquier interferencia causada por una señal extraña será tomada por ambas líneas y de aquí que su efecto en una diferencia de señal sea disminuído. Además, si varios pares trenzados se encuentran dentro del mismo cable, el trenzado de cada par dentro del cable reduce los efectos de interferencia provocados por el crosstalk.

Los pares trenzados son adecuados, con un direccionador de línea y un circuito receptor que exploten las ventajas potenciales ganadas al usar tal esquema, para velocidades de transmisión en el orden de 1 Mbps sobre distancias cortas (menos de 100 m) y para velocidades más bajas en distancias mayores. En algunos cables de par trenzado, se usa una pantalla protectora adicional o blindaje para reducir más ampliamente los efectos de señales de interferencia. Este tipo de cable es conocido como par trenzado blindado (STP por sus siglas en inglés).

Cable coaxial

El factor limitante principal de una línea de par trenzado es causado por un fenómeno conocido como el efecto de piel: mientras la velocidad (razón) de la señal de transmisión se incrementa, la corriente que fluye en los cables tiende sólo a fluir en la superficie exterior del cable, con lo que utiliza una sección de transmisión menor. Esto tiene el efecto de incrementar la resistencia eléctrica de los cables para señales de mayor frecuencia, lo que provoca una atenuación más acentuada de la señal transmitida. Además, a frecuencias aún más altas, se pierde una cantidad creciente de potencia de la señal debido a efectos de radiación. Por lo tanto, para aplicaciones que demanden una velocidad mayor a 1 Mbps, es normal utilizar otro tipo de medio de transmisión. Un tipo de línea de transmisión que minimiza los dos efectos anteriores es el cable coaxial.

En un cable coaxial, los alambres de referencia y tierra toman la forma de un conductor de centro sólido corriendo concéntricamente (coaxialmente) dentro de un conductor circular exterior que puede ser sólido o tejido. El espacio entre los dos conductores debería ser idealmente relleno con aire, pero en la práctica se llena con un material dieléctrico aislante ya sea en con estructura sólida o de panal.

Debido a su geometría, el centro conductor es protegido de una manera efectiva de las señales de interferencia externas y también, sólo ocurren pérdidas mínimas por el efecto de piel o por radiación electromagnética. El cable coaxial puede ser utilizado con diferentes señales, pero típicamente con 10 o aún 20 Mbps sobre varios cientos de metros es perfectamente factible. También, el cable coaxial es aplicable a topologías punto-a-punto y multi-punto.

Fibra óptica

Aunque la geometría del cable coaxial reduce significativamente los diversos efectos limitantes, la frecuencia máxima de la señal, y por lo tanto la velocidad de transmisión, que puede ser alcanzada utilizando un conductor sólido (normalmente de cobre), aunque es muy alta, es limitada. El cable de fibra óptica difiere de estos tipos de medios de transmisión, en que transporta la información transmitida en forma de un rayo de luz fluctuante a través de una fibra de vidrio, en lugar de una señal eléctrica sobre una cable de conductor metálico. Las ondas luminosas tienen un ancho de banda mucho mayor que las ondas eléctricas y por lo tanto, los cables de fibra óptica pueden ser utilizados para transmitir velocidades muy altas, en el orden de cientos de megabits por segundo. Además, el uso de un haz de luz hace al cable de fibra óptica inmune a los efectos provocados por interferencia de señales electromagnéticas y de crosstalk. El cable de fibra óptica, por lo tanto, es también extremadamente útil para la transmisión de señales de baja velocidad a través de ambientes eléctricos extremadamente ruidosos. También se están usando crecientemente en ambientes que demandan un alto nivel de seguridad, dado que es difícil hacer una unión física a una fibra óptica (para una extensión, por ejemplo).

Un cable de fibra óptica consiste de una fibra de vidrio, para cada señal a ser transmitida, contenida dentro de una cubierta protectora, la cual también protege a la fibra de cualquier fuente externa de luz. La señal luminosa es generada por una unidad de transmisión óptica, la cual realiza la conversión de señales eléctricas normales como las usadas en un equipo DTE. Similarmente, en el otro extremo de la línea, un módulo receptor especial es utilizado para realizar la función contraria. Típicamente, el transmisor utiliza un LED (diodo emisor de luz) para realizar la operación de conversión y el receptor utiliza un foto-diodo o un foto-transistor. Ya que la fibra está cubierta con una película reflectora, la mayoría de la luz generada por el LED permanece dentro de la fibra y por lo tanto el efecto de atenuación es muy bajo. En general, los sistemas basados en cables de fibra óptica son más caros que los de cable coaxial y, dado su construcción, son mecánicamente más frágiles, lo que los hace más difíciles de instalar. Son también mucho más difíciles de unir (o dividir) debido a que pueden ocurrir grandes pérdidas por acoplamiento, y por lo tanto son considerados cuando se requiera ya sea de una gran velocidad de transmisión o de inmunidad al ruído.

Microondas

Todos los medios de transmisión mencionados han utilizado una línea física para transportar la información transmitida. Sin embargo, también pueden transmitirse datos usando ondas electromagnéticas (de radio) a través del espacio. Un ejemplo de tal medio son los satélites: un canal de microondas, sobre el cual la información es modulada, es transmitido al satélite desde tierra y éste es recibido y retransmitido a la dirección predeterminada. Un canal típico de satélite tiene un ancho de banda extremadamente ancho y puede proporcionar cientos de enlaces para transmisión de datos a alta velocidad por medio de una técnica conocida como multiplexaje. La capacidad total del canal es dividida en subcanales, cada uno puede soportar un enlace de de transmisión de datos a alta velocidad.

Los satélites usados con propósitos de comunicación son normalmente geoestacionarios, lo que quiere decir que el satélite orbita a la Tierra con sicronización de una vez cada 24 horas, lo que lo hace parecer estacionario con respecto a tierra. La órbita del satélite es seleccionada de tal manera que proporcione un camino de comunicación con línea-de-vista tanto a las estaciones transmisoras como a las receptoras. El grado de direccionamiento del rayo de microondas restransmitido por el satélite puede ser ya sea disperso, de tal manera que que la señal pueda ser recogida sobre una extensión geográfica amplia, o finamente enfocada, para que sólo pueda ser recogida sobre un área limitada. En nuestros días, la potencia de la señal es mayor y por lo tanto se pueden usar receptores de menor diámetro, tales como antenas o parabólicas. Los satélites están en gran uso como medio de transmisión de datos y sus aplicaciones van desde interconectar diferentes redes de computadoras dentro de un área, hasta proporcionar un camino de alta velocidad para enlace de redes ubicadas en diferentes partes del mismo país.

Los enlaces de microondas son también ampliamente usados para proporcionar canales de comunicación cuando es impráctico o demasiado caro instalar medios físicos de transmisión; por ejemplo, a través de un río o quizá una carretera o autopista muy transitada. Tales enlaces son conocidos como enlaces terrestres de microondas. Mientras el rayo de microondas direccionado viaja a través de la atmósfera terrestre con este tipo de aplicación, puede ser distorsionado por cosas tales como estructuras construídas por las manos del hombre o condiciones climáticas adversas. Con un enlace satelital, en el otro extremo, el rayo viaja la mayor parte de su camino a través del libre espacio y por lo tanto es menos afectado por tales elementos. Nunca, la comunicación por microondas con línea de vista puede ser utilizada confiablemente sobre distancias mayores a 50 km.

Transmisión Via Satélite

Un satelite de comunicaciones es una estación de relevo de micro-ondas. Es utilizado como medio de enlace entre dos o más estaciones de micro-ondas terrenas. El satelite recibe transmisiones una banda de frecuencia (uplink), amplifica o repite la señal, y la transmite en otra frecuencia (downlink). Un solo satelite en orbita puede operar sobre varias bandas de frecuencia, llamadas *canales transponders* o simplemente *transponders*.

Para la efectiva función de un satelite de comunicación, es generalmente requiere permanecer estacionario con respecto a su posición sobre la tierra. Por otra parte, no puede estar dentro de la línea de la señal de las estaciones terrestres todo el tiempo. Para permanecer estacionario, el satelite de tener periodos de rotación iguales al periodo de rotación de la tierra. Esto se logra a una altura de 35,784 km.

Dos satelites usando la misma banda de frecuencia, si estan lo suficientemente cerca, provocarán interferencia de uno a otro. Para evitar esto, el estándar actual requiere de 4° de espaciamiento (desplazamiento angular con respecto a la tierra) en la banda de 4/6 Ghz y 3° de espaciamiento a 12/14 Ghz. Por lo tanto, el número de satelites posible es limitado.

3.3 TOPOLOGIAS

La topología de una red es la forma en que están conectados y asociados físicamente o lógicamente los elementos de una red.

A continuación se analizaran las distintas formas en que podemos conectar los elementos que forman una red.
En redes locales, prácticamente existen tres tipos básicos de topologías, a saber:

- Estrella
- Bus
- Anillo

Se puden sumar a estos tres tipos básicos la topología de Arbol que es una conexión compuesta.
Para el estudio de las topologías se deben considerar dos tipos:

- Física
- Lógica

La topología Física es la determinada por la disposición de los elementos conectados a la RED.
La topología Lógica la determina el protocolo de comunicación operando en la RED, no importando la disposición física de los elementos, es decir, se puede implementar un anillo lógico en un bus físico.
El protocolo de comunicación en una RED, es el conjunto de reglas aplicadas a la comunicación entre los elementos de una RED.

3.3.1 Topología de Bus

Esta conexión se considera que es la más sencilla de todas, donde las microcomputadoras incluyendo al servidor, están enlazados por un solo cable (coaxial o par trenzado), donde la información viaja en ambos sentidos, por lo que se pueden producir colisiones. Todos los nodos comparten este cable, y éste necesita acopladores en ambos extremos. Las señales y los datos van y vienen por el cable asociados a una dirección de destino. Cada nodo verifica las direcciones de los paquetes que circulan por la red para ver si alguna coincide con la suya propia. El cable puede extenderse de cualquier forma a través de las paredes y techos de la instalación, y las estaciones de trabajo se conectan a él.

La topología de bus utiliza una cantidad de cable mínima, y el cable es muy fácil de instalar. La longitud total del cable será mucho menor que en una red de estrella.

Esta topología tiene sus desventajas, el cable central puede convertirse en un cuello de botella en entornos con un tráfico elevado, ya que todas las estaciones de trabajo comparten el mismo cable. Es difícil aislar los problemas del cableado de la red y determinar qué estación o segmento de cable los origina. Una rotura en el cable producira una caída del sistema En el caso de una colisión es necesaria la retrasmisión de la información.
Una colisión se produce cuando dos estaciones de trabajo de la RED tratan de accesar el bus de comunicación al mismo tiempo. Es muy importante en esta topología el prevenir las colisiones.

Por ello el protocolo adecuado para esta topología es CSMA/CD (Carrier Sense Multiple Access/Colision Detection).
En este protocolo el nodo transmite a la red y espera a que se le confirme que la información fue recibida correctamente, de otra forma, detecta la posible colisión, espera un tiempo a que el canal esté desocupado y la información se transmite nuevamente.

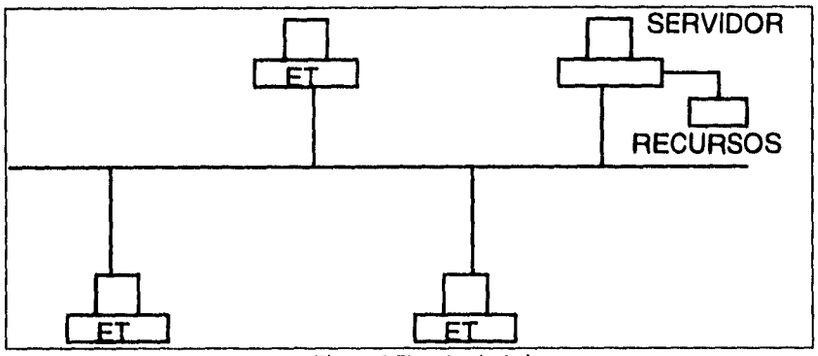

Figura 2 Topología de bus

3.3.2 Topología de Anillo

En esta conexión la información viaja ordenadamente en un solo sentido a través de un solo cable, describiendo un ángulo de 360 en cuyo anillo imaginario, están conectadas en serie las estaciones de trabajo y el servidor de la RED.

Una señal llamada TOKEN (receptáculo a modo de estafeta) va circulando por la red y pasando por cada estación, si la primera resulto ser solicitante, previa identificación entrega la información, de lo contrario la deposita en el token para que esta a su vez así la envíe a la siguiente, llevando consigna de entregarla hasta identificar a la solicitante.

Cada estación de paso, cunado más, colecta información adicional enviándola a la siguiente y así se la pasa la señal cerrando ciclos "circulares"; por ello el protocolo apropiado para este caso se conoce como TOKEN PASSING.

Con la topología en anillo, las redes pueden extenderse a menudo a largas distancias, y el costo total del cableado será menor que en una configuración de estrella y posiblemente igual al de un bus lineal. Sin embargo, el complicado cableado debe cerrarse sobre sí mismo. Una rotura en el cable hará caer el sistema.

Este tipo de topología tiene un buen costo y modularidad además de ofrecer gran flexibilidad para el incremento de estaciones de trabajo. Ahora bien, si el número de estaciones es elevado, el retardo total puede resultar excesivamente grande para determinadas aplicaciones en tiempo real, debido al retardo introducido por cada estación de trabajo.

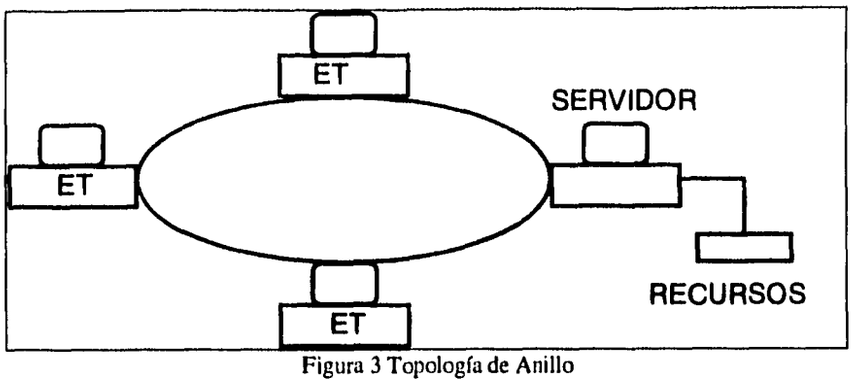

Figura 3 Topología de Anillo

3.3.3 Topología de Estrella

En este tipo de conexión, el elemento central es el servidor con sus periféricos. Se mantiene preguntando constantemente a cada estación de trabajo mediante una comunicación exclusiva y por turno, si se desea transmitir información; de ser afirmativo, la atiende y al terminar, prosigue con su interrogatoria permanente.
Todas las estaciones de trabajo están unidas mediante medios bidireccionales a un módulo o nodo central que efectua las funciones de comunicación. El nodo central asume además las labores de control y de gran parte de los recursos informáticos comunes.
Para este caso de pregunta-respuesta-pregunta a la siguiente etc; a la regla de comunicación se le conoce como protocolo POLLING (poleo), empleado en las minicomputadoras.
En el principio de las redes, esta topología fue la que se utilizó primero, pero resultaba una de las más caras.
Se utiliza un dispositivo como punto de conexión de todos los cables que parten de las estaciones de trabajo el dispositivo central puede ser un servidor o un dispositivo especial de conexión.
El diagnóstico de problemas de la red es fácil, debido a que las estaciones de trabajo se comunican a través del equipo central. Los fallos en los nodos son fáciles de detectar, y es fácil cambiar los cables. La colisión entre datos es imposible, ya que cada estación tiene su propio cable, y resulta fácil ampliar el sistema. Sin embargo, en grandes instalaciones, los cables de las estaciones de trabajo tiene a agruparse en la unidad central, creando una situación propensa a errores de gestión.
El nodo aisla a una estación de trabajo de otra, resultando una red fiable frente averías; es muy fácil de modificar en el número de estaciones de trabajo. No es adecuado para redes con gran dispersión geográfica.

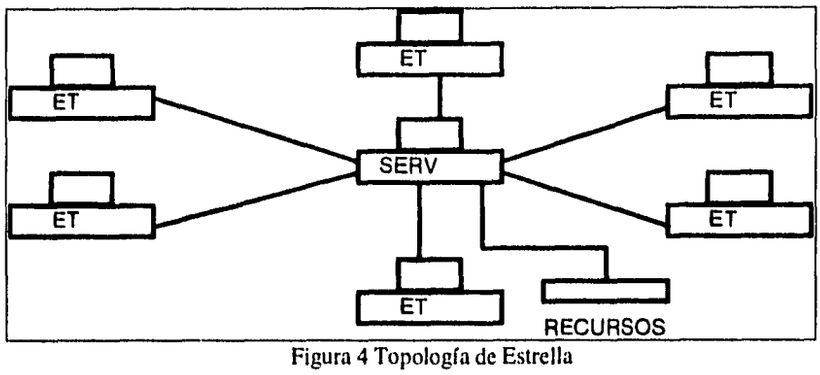

Figura 4 Topología de Estrella

3.3.4 Topología de Arbol

Esta conexión como se dijo anteriormente, es combinada y es una opción más para implementar redes, según las necesidades del usuario.
Este tipo de topología también es llamada de Estrella Distribuida, ya que es una extensión de la arquitectura de estrella por interconexión de varias de estas.
Este tipo de topología ofrece una gran flexibilidad para configurar la distribución de los cables.
Permite establecer una jerarquía clasificando a las estaciones en grupos y niveles según el nodo a que están conectadas, su distancia y jerárquica al nodo central.
La avería de una de las estaciones de trabajo no afecta el funcionamiento de la red. Permite incrementar y/o disminuir el número de estaciones de trabajo con relativa sencilles y están localizadas al nodo correspondiente. La detección de fallas en el cable es fácil, cuando todas las estaciones de trabajo tienen cable dedicado y los nodos compartan un nodo lineal.
Algunas desventajas de esta topología es que contiene características más propias de una red pública de datos que de una red privada local, además de que el costo en instalación es elevado.

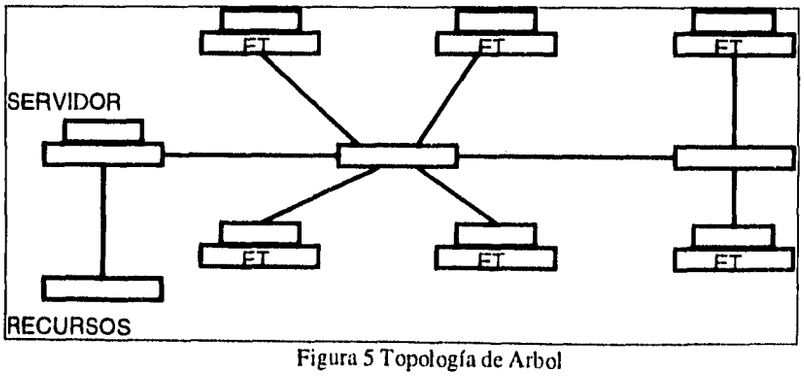

Figura 5 Topología de Arbol

3.4 ESTANDARES Y PROTOCOLOS

3.4.1 Estándares de red de área local

Logical Link Control (IEEE 802.2)
El estándar Logical Link Control (LLC) especifica el mecanismo para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios. La operación y formato de este estándar esta basada en HDLC (High-Level Data Link Control). Tres servicios son previstos como alternativas para conectar dispositivos usando LLC:

- *Servicio sin-conexión sin reconocimiento:* Este servicio es definido estilo datagrama. Es un servicio muy simple que no involucra ninguno de los mecanismos de flujo y control de error. Por tanto, la entrega de datos no esta garantizada. No obstante, en la mayoría de los dispositivos existe algún nivel superior de software que maneja confiablemente los datos.
- *Servicio modo-conexión:* Este servicio es similar al que ofrece HLDC. Una conexión lógica es establecida entre dos usuarios intercambiando información, el control de flujo y control de errores están disponibles en este servicio.
- *Servicio sin-conexión con reconocimiento:* Este servicio es una combinación de los dos servicios anteriores. Este provee aquellos datagramas que serán reconocidos, sin que exista una conexión lógica previa establecida.

CSMA/CD (IEEE 802.3)

Medio de transmisión
La tabla 1 sumariza las opciones definidas por el IEEE 802.3 estándar. El estándar original (10BASE5) especifica una red de área local de cable coaxial base banda a 10 Mbps. La longitud máxima del segmento de cable es 500 metros, con un máximo de 100 terminaciones por segmento permitido. La longitud de la red puede ser extendida usando repetidores. El estándar permite un máximo de cuatro repetidores en la ruta entre dos estaciones cualquiera extendiendo la longitud efectiva de la red a 2.5 km.
La versión original, lanzada en 1925, fue seguida de una opción algunas veces llamada como Cheapernet (10BASE2). Este estándar especifica el uso de cable coaxial más delgado a la misma velocidad de transmisión. El cable delgado resulta en componentes electrónicos significativamente más baratos, con la desventaja de tener menos estaciones y menor longitud de segmento. La longitud del segmento es reducida a 185 metros con un máximo de 30 terminaciones por segmento. Esto está dirigido a dispositivos de bajo costo, como estaciones de trabajo UNIX y computadoras personales.
Otra opción, conocida como Starlan (1BASE5), especifica una versión de par trenzado no blindado que opera a 1 Mbps usando una topología de estrella pasiva. Esta opción es substancialmente menor en costo que cualquiera de las opciones de cable coaxial y dirigida específicamente a instalaciones de computadoras personales que no requieren gran capacidad.
La opción 10BASE-T es también una versión de par trenzado no blindado que opera a 10 Mbps. Finalmente, la opción banda amplia (broadband 10BROAD36) a 10 Mbps ha sido

incorporada. Esto provee soporte a mas estaciones sobre distancias mas grandes que las versiones de banda base, a un costo mayor.

IEEE 802.3 (CSMA/CD)

Tipo	Medio de Transmisión	Técnica de señales	Velocidad de transmisión (Mbps)	Máxima longitud en el segmento (m)
10Base5 (Original)	Cable coaxial	Baseband (Manchester)	10	500
10Base2 (Cheapernet)	Cable coaxial	Baseband (Manchester)	10	185
10Base5 (StarLAN)	UTP (Unshielded twisted pair	Baseband (Manchester)	1	250
10Base T	UTP (unshielded twisted pair)	Baseband (Manchester)	10	100
10BROAD36 (Broadband)	Cable coaxial	Broadband	10	2600

Ethernet

El estándar original IEEE 802.3 a 10 Mbps fue basado y es muy similar a Ethernet. Ethernet es el tipo de LAN mas ampliamente utilizado. Fue desarrollado a mediados de 1970 por Xerox. El propósito de Xerox fue desarrollar un estándar de facto para la industria de las LAN's y ofrecer la licencia de la tecnología a otros proveedores.

Ethernet usa el mismo algoritmo de control de acceso al medio CSMA/CD y la misma especificación de cable coaxial banda base IEEE 802.3 . Desafortunadamente , Ethernet difiere en algunos detalles de la especificación IEEE. El formato del paquete es ligeramente diferente. En adición, Ethernet incluye la lógica tanto del control de acceso al medio (MAC) como el control lógico de enlace (LLC).

Token Bus (IEEE 802.4)

El estándar token bus especifica tres opciones para el nivel físico. El primero es un sistema de broadband, el cual soporta canales de datos a 1,5, y 10 Mbps con anchos de banda de 1,5,6 y 12 Mhz, respectivamente. El estándar recomienda el uso de un sistema de cable sencillo dividido con un traductor de frecuencias. La configuración de cable dual también esta permitida.

El segundo es un esquema conocido como banda portadora (carrierband), o canal sencillo de banda ancha. La señalización en banda portadora significa que el espectro entero del cable es dedicado a una sola ruta de transmisión para señales analógicas. Debido a que carrierband es dedicado a un solo canal de datos no es necesario tener cuidado que la salida del módem sea confinada a un ancho de banda pequeño. La velocidades de transmisión especificadas son 1,5, y 10 Mbps. La adición mas reciente incluye fibra óptica a velocidades de 5,10, y 20 Mbps. Cualquiera de las topologías de estrella; activa o pasiva pueden ser usadas.

IEEE 802.4 (Token Bus)

Tipo	Medio de Transmisión	Técnica de señales	Velocidad de transmisión (Mbps)	Máxima longitud en el segmento (m)

Broadband	Cable coaxial	Broadband	1, 5, 10	No especificado
Carrierband	Cable coaxial	Broadband	1, 5, 10	7600
Fibra óptica	Fibra óptica	ASK-Manchester	5, 10, 20	No especificado

Token Ring (IEEE 802.5)

El estándar IEEE 802.5 especifica par trenzado blindado a 4 y 16 Mbps y par trenzado no-blindado a 4 Mbps. El estándar token ring en par trenzado no es un competidor de token bus para cubrir grandes áreas o para aplicaciones en fabricas. De todos modos, puede ser considerado como una alternativa para el bus banda base CSMA/CD para muchas aplicaciones de oficina.
Token ring tiene varias ventajas sobre CSMA/CD. Primero, como con token bus, el algoritmo de control de acceso al medio exhibe superior desempeño que CSMA/CD. Una configuración de token ring puede proveer la misma salida efectiva que un bus CSMA/CD a 10 Mbps. Segundo, el cable par trenzado es más sencillo para trabajar que el cable coaxial.

IEEE 802.5 (Token Ring)

Medio de transmisión	Técnica de señales	Velocidad de transmisión (Mbps)	Máximo número de repetidores	Máxima distancia entre repetidores (m)
STP (Shielded twisted pair)	Differential Manchester	4, 16	250	No especificado
UTP (Unshielded twisted pair)	Differential Manchester	4	250	No especificado

Fiber-Distributed Data Interface (FDDI)

El estándar mas nuevo para red local es el Fiber-Distributed Data Interface (FDDI). La topología de FDDI es anillo. La técnica para el control de acceso al medio usada es token ring, con algunas diferencias menores de la especificación token ring de IEEE. El medio especificado es fibra óptica a 100 Mbps. La especificación del medio incorpora mediciones específicas diseñadas para asegurar alta disponibilidad.
El estándar FDDI abarca tres áreas generales de aplicación: redes locales backend, redes locales de alta velocidad para oficinas y redes locales backbone. Las redes locales backend son utilizadas en ambientes de computadoras delimitados a una pequeña área para interconectar mainframes y dispositivos de almacenamiento masivo. Las redes locales de alta velocidad para oficinas cumple con los requerimientos de alta velocidad de las aplicaciones actuales para oficina, que incluyen base de datos distribuidas, facsímile, terminales de texto y facsímile, aplicaciones gráficas y multimedia. Finalmente, las redes locales backbone son aquellas que interconectan otras redes locales y equipos independientes en áreas grandes.

Fiber-Distributed Data Interface (FDDI) Token Ring

Medio de transmisión	Técnica de señales	Velocidad de transmisión (Mbps)	Máximo número de repetidores	Máxima distancia entre repetidores (m)

Fibra óptica	ASK-NRZI	100	1000	2000

3.4.2 TCP/IP Suite

Dos tendencias relativas a las comunicaciones entre computadoras dentro del Departamento de Defensa (DOD) de los Estados Unidos motivaron la necesidad de un estándar militar para protocolos de comunicación, así como de una arquitectura de comunicación:

- La rápida proliferación de computadoras y otros elementos para procesar señales, dentro de la industria militar y la necesidad de utilizar equipos de múltiples proveedores.
- La rápida proliferación de redes de comunicación dentro de la industria militar y la necesidad de diversas tecnologías de red.

El costo decreciente y el incremento de la capacidad del hardware de las computadoras provocó un aumento en el uso de las minicomputadoras y microcomputadoras para manejar una amplia variedad de tareas. Reforzando esta tendencia podemos mencionar la superioridad de un ambiente de procesamiento de datos distribuido sobre la tradicional instalación de procesamiento de datos centralizada basada en una mainframe. Las ventajas del modelo distribuido incluyen un mejor rendimiento y mayor disponibilidad de aplicaciones.
De esta manera, tenemos una situación en donde existen un gran número de diferentes computadoras, localizadas en diferentes redes, con la necesidad de comunicarse entre sí. En términos generales, dos requerimientos técnicos se presentan:

1. Sistemas finales (computadoras, terminales) deben compartir un conjunto común de protocolos de comunicación para poder interoperar.

2. El conjunto de protocolos usado para este propósito debe soportar la capacidad de intercomunicarse con otras redes, en un ambiente de redes múltiples.

Basado en estos requerimientos, el DOD, a través de la Agencia de Comunicaciones de la Defensa (ACD), estableció un conjunto de protocolos estándar [STAL86], listados en la siguiente tabla.

Protocolos militares estándar del DOD

MIL-STD-1777 Internet Protocol (IP)

Provee servicio sin conexión en sistemas finales para comunicarse a través de una o mas redes.
MIL-STD-1778 Transmission Control Protocol (TCP)
Servicio confiable para la transferencia de datos punto a punto. Equivalente al protocolo de transporte ISO Capa 4
MIL-STD-1780 File Transfer Protocol (FTP)
Aplicación para la transferencia de archivos ASCII, EBCDIC, y archivos binarios.
MIL-STD-1781 Simple Mail Transfer Protocol (SMTP)
Utilería sencilla de correo electrónico
MIL-STD-1782 TELNET Protocol
Provee la capacidad de una terminal en modo scroll

Existen varias ventajas que convierten a estos estándares en los mayormente utilizados para sistemas abiertos:

- *Interoperabilidad*: Si el mismo conjunto de protocolos es implementado sobre diferentes equipos, estos podrán comunicarse independientemente de la plataforma.
- *Productividad y eficiencia del proveedor:* Los proveedores se concentran en desarrollar los protocolos estándar y no en dedicar recursos en protocolos de conversión para interoperar con sus esquemas propietarios.
- *Competitividad:* Diferentes proveedores pueden ofrecer equipos y servicios, eliminando la dependencia con un solo proveedor.
- *Simplificación en la adquisición:* Las decisiones sobre la adquisición de equipo, pueden ser basadas en el costo relativo y rendimiento del equipo de diferentes proveedores, si tener que considerar costos por conversión de protocolos, y consecuentes retrasos en la instalación.

Uso no militar del protocolo TCP/IP

Una interesante y amplia propagación ha tenido la utilización del protocolo TCP/IP en aplicaciones no militares. Desde la introducción del estándar SNA (System Network Architecture) de IBM, seguida de la aparición de arquitecturas de comunicaciones propuestas por proveedores competidores, la mayoría de usuarios de computadoras eligieron los sistemas propietarios de IBM. Actualmente, tanto los fabricantes como los usuarios están evolucionando hacia el uso de estándares internacionales basados en la arquitectura OSI (Open Systems Interconnection). Sin embargo, para sorpresa de muchos observadores, muchos usuarios han decidido hacer un paso intermedio hacia el protocolo TCP/IP.

Esta tendencia ha sido confirmada por diversos estudios, como se ilustra en la figura 6

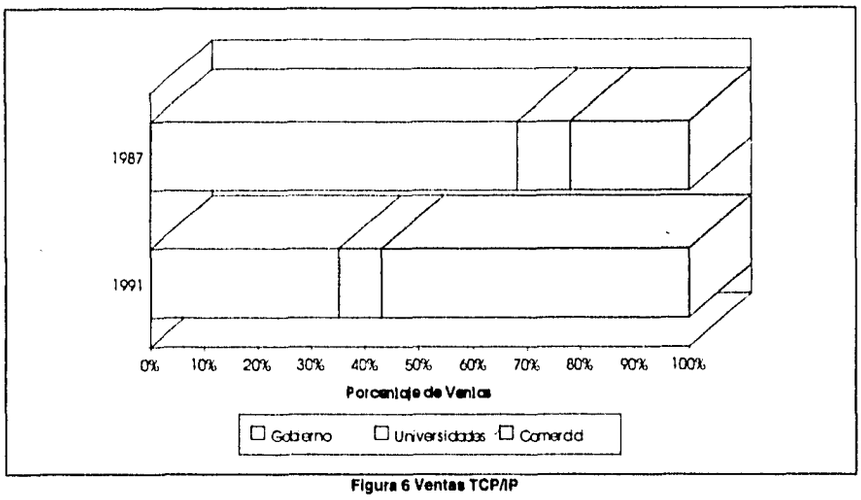

Figura 6 Ventas TCP/IP

Arquitectura del protocolo TCP/IP

Estructura

Cualquier aplicación distribuida, como puede ser la transferencia de archivos o el correo electrónico requiere un conjunto de funciones complejas de comunicación para su adecuada operación. Muchas de estas funciones, así como mecanismos dependientes, son comunes en muchas ó quizá todas las aplicaciones. De este modo, las tareas de comunicación son vistas como una arquitectura modular, en la cual los varios elementos de la arquitectura desarrollan las diversas funciones requeridas.
La arquitectura TCP/IP esta basada en una visión de que la comunicación de datos involucra tres agentes: procesos, computadoras y redes. Los procesos son la entidad fundamental a comunicar. Un ejemplo es la operación de transferencia de archivos (File Transfer). Los procesos se ejecutan en la computadora (host), la cual frecuentemente puede soportar múltiples procesos simultáneos. Las computadoras son conectadas por redes, y los datos para ser intercambiados son transmitidos por la red desde una computadora a otra.
La organización de las tareas de comunicación se organiza en cuatro niveles relativamente independientes:

- Nivel de acceso a red
- Nivel internet
- Nivel host-to-host
- Nivel de procesos

El *nivel de acceso a red* se refiere al intercambio de datos entre el host y la red a la cual esta conectada. En aquellos casos en que dos hosts estén conectadas a diferentes redes, son

necesarios procedimientos para permitir el transito de datos a través de diferentes redes. Esta es función del *nivel internet*. El protocolo internet es utilizado para proveer la función de enrutamiento a través de diferentes redes. Independientemente de la naturaleza de los procesos que intercambian datos, existe la necesidad de que el intercambio sea confiable. Los mecanismos para proveer seguridad en la transmisión son en esencia independientes de la naturaleza del proceso. Por lo tanto, tiene sentido agrupar estos mecanismos en un nivel común compartido por todos los procesos, este es el *nivel host-to-host*.
Finalmente, el *nivel de procesos* contiene protocolos necesarios para soportar las diversas aplicaciones. Para cada tipo de aplicación , como por ejemplo el file tranfer, se requiere un protocolo particular para esa aplicación.
La siguiente figura ilustra la arquitectura y los protocolos que integran cada nivel.

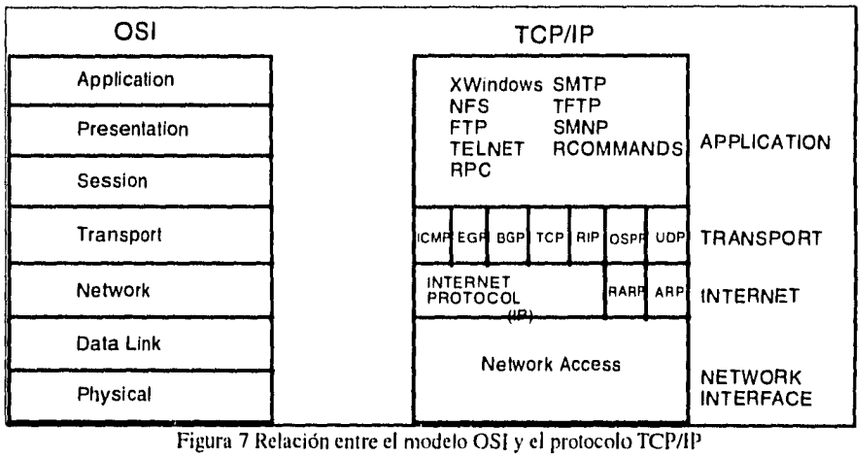

Figura 7 Relación entre el modelo OSI y el protocolo TCP/IP

Operación

Cada computadora contiene software en los niveles de acceso a red, internet y host-to-host y software en el nivel de procesos para uno o mas procesos. Los gateways entre redes requieren del nivel de acceso a red como interface para conectarse con otras redes, y el nivel internet esta habilitado para realizar el ruteo y las funciones de relevo. Para una comunicación exitosa, cada entidad dentro de todo el sistema deberá tener una dirección única.
Actualmente, dos niveles de direccionamiento se necesitan. Cada computadora dentro de la red debe tener una dirección global de red única; esto permite que los datos sean enviados a la computadora correcta. Cada proceso dentro de la computadora debe tener una dirección única asociada a la computadora; esto permite al protocolo host-to-host (TCP) enviar los datos al proceso deseado. Esta última dirección es conocida como puerto.

Para controlar esta operación, la información de control como los datos deben ser transmitidos (como se sugiere en el siguiente diagrama). El proceso emisor genera un bloque de datos y los pasa al protocolo del nivel host-to-host (TCP). TCP puede romper estos bloques en dos partes para hacerlos mas manejables. Para cada una de estas partes TCP agrega un encabezado. La combinación de los datos del nivel del proceso y la información de control de TCP es conocida como *segmento TCP*. El encabezado de cada segmento contiene información de control para ser usada por el protocolo TCP homólogo en la computadora destino.
El siguiente paso para TCP es el manejo de cada segmento sobre el nivel internet, con las instrucciones para transmitir el segmento a la computadora destino. Estos segmentos deben ser transmitidos a través de una o más redes y entregada a gateways intermedios. Como antes, esta operación requiere del uso de información de control. En este caso el protocolo Internet (IP) agrega un encabezado IP a cada segmento que recibe de TCP; el resultado es llamado *datagrama IP*. Finalmente, cada datagrama IP es presentado al nivel de acceso a red para la transmisión a través de la primera red de la ruta para llegar al destino. El nivel de acceso a red agrega su propio encabezado, creando un *paquete*. El paquete es transmitido del host a la red; el encabezado del paquete contiene información que la red necesita para transmitir los datos a través de la red.

Cuando los datos son recibidos en la otra computadora, el proceso se repite en sentido contrario. En cada nivel, el encabezado correspondiente es removido, y el resto es pasado al siguiente nivel hacia arriba, hasta que los datos del proceso original son entregados al proceso destino.

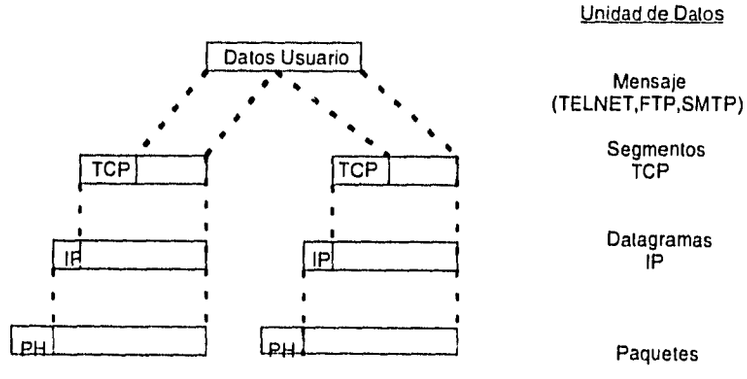

Figura 8 Datos de usuario y protocolo de control de información

Mecanismos del protocolo TCP/IP
Segmentación y reensamblado

El objetivo de un protocolo de comunicaciones es el intercambio de flujo de datos entre dos entidades. Usualmente, la transferencia puede ser caracterizada como una secuencia de bloques de datos de tamaño limitado. En el nivel de procesos, podemos referirnos a una unidad lógico de transferencia de datos como un mensaje. Ahora, ya sea que la aplicación (por ejemplo TELNET,FTP,SMTP) envíe los datos vía mensajes o en un flujo continuo, los protocolos de nivel inferiores requieren romper los datos en bloques de menor tamaño. Esta función es llamada segmentación. Por conveniencia, nos referiremos a un bloque de datos intercambiados por dos entidades vía un protocolo como PDU (Protocol Data Unit).
La contraparte de la segmentación es el reensamblado. Eventualmente, los datos segmentados deben ser reensamblados en mensajes apropiados a la aplicación. Si los PDU's llegan fuera de orden, la tarea se complica.

Encapsulado

Cada PDU contiene no sólo datos también contienen información de control. En algunos casos, los PDU's consisten solo de información de control.
La adición de la información de control a los datos es referida como encapsulado. La información es recibida o generada por una entidad y encapsulada en un PDU conteniendo datos mas información de control.

Control de conexión

Una entidad puede transmitir datos a otra entidad de una manera no planeada, sin coordinación previa. Esto se conoce como transmisión de datos sin-conexión (connectionless data transfer). Aunque este modo puede ser útil, es menos común que la transferencia de datos orientada-a-conexión (connection-oriented data transfer)
La transferencia de datos orientada es preferida (hasta requerida) si la estación anticipa la longitud del intercambio de datos y/o ciertos detalles del protocolo deben ser enviados fuera dinámicamente. Tres fases ocurren:

- Establecimiento de la conexión
- Transferencia de datos
- Terminación de la conexión

El protocolo internet es del tipo sin-conexión; esto es deseable para proveer la capacidad de interconexión de redes. TCP es orientado-a-conexión para soportar confiablemente la transferencia de datos. Como FTP,SMTP y TELNET hacen uso de TCP también presentan la característica de orientados-a-conexión.

Direccionamiento

La arquitectura de comunicaciones TCP/IP intenta soportar un ambiente en el cual existan múltiples redes, múltiples nodos en cada red, y múltiples procesos en cada nodo. Esto requiere un esquema de direccionamiento complejo.

Las direcciones de los nodos TCP/IP consisten de 32 bits, tradicionalmente divididos en cuatro partes de 8 bits donde cada uno representa un número entre el 1 y el 255, separados por un punto. Existen tres clases de direccionamiento:

Clase A - Considera siete bits del primer byte para definir la dirección de la red con un rango que va del 1.0.0.0 al 127.0.0.0, los tres bytes restantes son utilizados para definir la dirección de los nodos con un rango que va del 1 al 255. Esta clase es utilizada en empresas con pocas redes, pero con muchos nodos en cada sus redes. Con la clase A se pueden tener 128 redes con hasta 16,777,216 nodos cada una.

Clase B - Considera seis bits del primer byte y ocho bits del segundo para definir la dirección de la red con un rango que va del 128.1.0.0 al 191.254.0.0, los dos bytes restantes son utilizados para definir la dirección de los nodos. Esta clase es utilizada por la mayoría de las empresas debido a que es capaz de soportar una gran cantidad de redes y nodos. Con la clase B se pueden tener hasta 16,384 redes con 65,536 nodos cada una.

Clase C - Considera cinco bits del primer byte y 16 bits del segundo y tercer byte para definir la dirección de la red con un rango que va del 192.1.10.0 al 254.254.254.0, el último byte es utilizado para la dirección de los nodos. Esta clase es utilizada en empresas que requieren de una gran cantidad de redes pequeña hasta 2,097,152 con hasta 256 nodos en cada una.

La siguiente tabla muestra el esquema de direccionamiento TCP/IP

Clase	Modo de Direccionamiento	Número de redes en la clase	Nodos Direccionados
A	0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh	128	16,777,216
B	10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh	16,384	65,536
C	110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh	2,097,152	256

n: bit de dirección de red 0: fijo
h: bit de dirección ID del nodo 1: fijo

Los nombres y direcciones de los elementos o nodos de una red son muy importantes en un ambiente de cómputo cooperativo y distribuido que soporta la arquitectura Cliente/Servidor. Las direcciones de los nodos deben ser globalmente únicas en toda la red.

La clase es seleccionada en el diseño de la red y no puede ser cambiada arbitrariamente.

La definición de la dirección de la red se vuelve importante cuando la red que se diseña va a integrarse con otras redes que estén inscritas en Internet. En ese caso se deberá solicitar la dirección de la red a Network Information Center (NIC)

3.4.3 IPX

IPX es otro de los protocolos que ha tenido mucho éxito en los ambientes de redes locales en oficinas. Este protocolo fue desarrollado por Novell, tomando como base el protocolo XNS desarrollado por Xerox.

La siguiente figura muestra la relación que existe entre los niveles que conforman el protocolo IPX y el modelo OSI. Entre las características más importantes del IPX se encuentran:

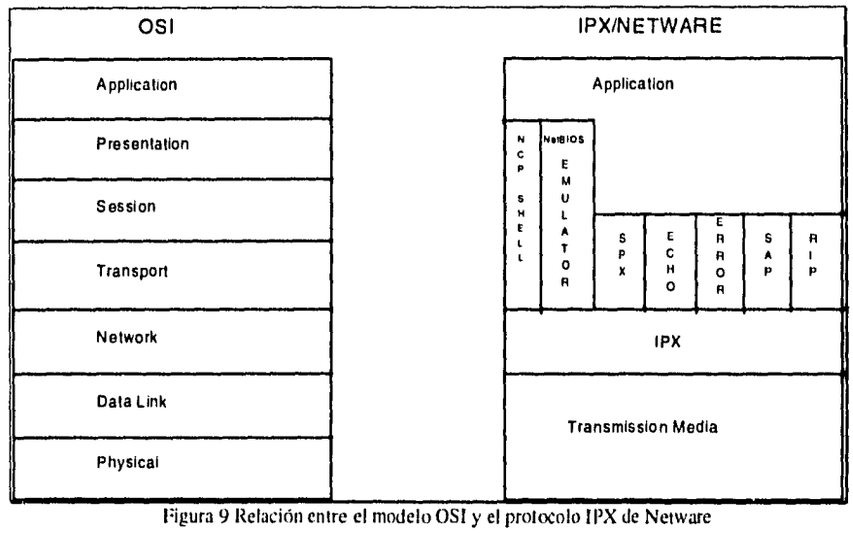

Figura 9 Relación entre el modelo OSI y el protocolo IPX de Netware

- Es "connectionless", mejor servicio en la entrega de paquetes.
- No realiza "checksum" como lo hace el XNS, la detección de errores de transmisión se lleva a cabo en la capa "data-link".
- Este protocolo es soportado por una amplia variedad de topologías de LAN y "media".

La estructura del "stack" del Sistema Operativo de red Netware de Novell es descrita en los siguientes puntos:

- El Protocolo de Novell, Netware Shell/NetWare File Server Protocol (NFSP) implementa el protocolo NetWare Core Protocol (NCP) tanto en la workstation como en el server. Lo utilizan las workstations para comunicarse con el servidor.

- El emulador de la interface NetBIOS permite que dos aplicaciones escritas en este protocolo que estén en diferentes máquinas se comuniquen entre ellas.

- El protocolo de transporte SPX, proporciona es servicio de transferencia de datos, confiable y "connection oriented".

- El protocolo ECHO proporciona la validación de la existencia de hosts y verifica que exista enrutamiento a esos hosts.

- El protocolo de publicación de servicio (SAP) proporciona el servicio de broadcast para los servidores de Novell, identificando su existencia y tipo de servicios en la red.

- El protocolo de enrutamiento RIP proporciona la información para el enrutamiento de la información entre hosts "internet" o "full function" y estaciones finales, balanceando las rutas basándose en retardos, ancho de banda, "metric", etc.

- El protocolo IPX proporciona el servicio de entrega de los paquetes de información basado en enrutamiento "connectionless" y menos confiable. Utilizando los servicios de los protocolos descritos anteriormente:

  - IPX es utilizado a través de las redes.
  - SAP, ERROR y ECHO son utilizados para enrutar a las estaciones finales.
  - RIP es utilizado para enrutamiento entre dominios o inter-redes.

- La administración de la red es proporcionada por el agente SNMP, el cual pasará la información de las variables (MIB), basado en la tabla de enrutamiento.

3.4.4 NFS (Network File Services)

NFS (Network File Services, por sus siglas en inglés, Servicios de Archivo en Red) es un filesystem distribuido que permite el acceso transparente a discos remotos. NFS permite centralizar la administración de los discos. En lugar de duplicar directorios comunes como

/usr/local en cada sistema de la red, NFS otorga una copia del directorio que se está compartiendo por todos los sistemas de la red.

Para un host local corriendo NFS, los filesystems remotos no parecen distintos a los locales. Para el usuario final NFS significa, el no tener que accesar mediante un "login" a otros sistemas, para poder accesar los archivos. En un sistema Unix no es necesario utilizar rcp o cintas para mover archivos de un sistema a otro.

Una vez que los servicios de NFS han sido configurados correctamente pueden realizar todo su trabajo en sus sistemas locales; archivos remotos (datos y ejecutables) aparecerán como locales a su propio sistema. NFS y NIS (Network Information Service) son usados frecuentemente juntos; NIS se asegura que la información de la configuración se propaga a todos los hosts, y NFS se asegura que los archivos que el usuario necesita sean accesibles desde estos hosts.

NFS está construído en el protocolo RPC (protocolo de sesión) e impone una relación cliente-servidor en los hosts que lo utilizan. Un servidor NFS es un host que posee uno o más filesystems y pone estos a disposición en la red; los clientes de NFS montan estos filesystems de uno o varios servidores. Esto sigue el modelo Cliente/Servidor donde el servidor es dueño de recursos que son utilizados por el cliente. En el caso de NFS, el recurso es un drive de un disco físico que se comparte con todos los clientes de el servidor.

3.4.5 X.25

En la actualidad X.25 es la norma de interfaz orientada al usuario de mayor difusión en las redes de paquetes de gran cobertura.

Las redes de paquetes y las estaciones de usuario han de disponer de mecanismos de control que les permitan interconectarse. Quiza el más importante de estos mecanismos, al menos desde el punto de vista de la red, sea el control de flujo, que sirve para limitar la afluencia de tráfico procedente de los usuarios, evitando así la congestión de la red. También el ETD (equipos terminales de datos) ha de controlar el flujo que le llega de la red. Además de ello, tanto los ETD como la propia red han de poseer procedimientos de control de errores que garanticen la recepción correcta de todo el tráfico. El X.25 proporciona estas funciones de control de flujo de errores.

En X.25 se definen los procedimientos que realizan el intercambio de datos entre los dispositivos de usuarios (ETD) y un nodo de la red encargado de manejar los paquetes (un ETCD equipo de terminación del circuito de datos). Su título formal es "Interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos públicas".

Las redes utilizan la norma X.25 para establecer los procedimientos mediante los cuales dos ETD que trabajan en modo paquete se comuniquen a traves de la red. En efecto, en X.25 se definen las dos sesiones de los ETD con sus respectivos ETCD. La idea que subyace en este estándar consiste en proporcionar procedimientos comunes de establecimiento de sesión e intercambio de datos entre un ETD y una red de paquetes (ETCD). Entre estos procedimientos se encuentran funciones como las siguientes: identificación de paquetes procedentes de ordenadores y terminales concretos (mediante números de canal lógico (LCN)), asentimiento de paquetes, rechazo de paquetes, recuperación de errores y control de flujo. Además, X.25 proporciona algunas facilidades muy útiles, como por ejemplo la facturación a estaciones ETD distintas de la que genera el tráfico.

Curiosamente, el estándar X.25 no incluye algoritmos de encaminamiento, estos se dejan a criterio de cada fabricante, y son especificos de sus productos. Conviene resaltar también que, aunque las interfaces ETD/ETCD de ambos extremos de la red son independientes uno del otro, X.25 interviene desde un extremo hasta el otro, ya que el tráfico seleccionado se encamina desde principio hasta el final.

La ausencia de algoritmos de encaminamiento en X.25 es a veces motivo de confusión. La figura muestra la relación existente entre el nivel de red en X.25 (3) y los sistemas de encaminamiento o retransmisión. El tráfico pasa del ETD del usuario A a un nodo intermedio, que podría ser el nodo de entrada del usuario a la red (en X.25), el ETCD). En este nodo, para atender al usuario A se invoca al nivel físico (1), al nivel de enlace (2, LAPB) y al nivel de red (3,X.25). En esta ilustración, el usuario A se identifica de cara a la red mediante el número de canal lógico (LCN) 11.

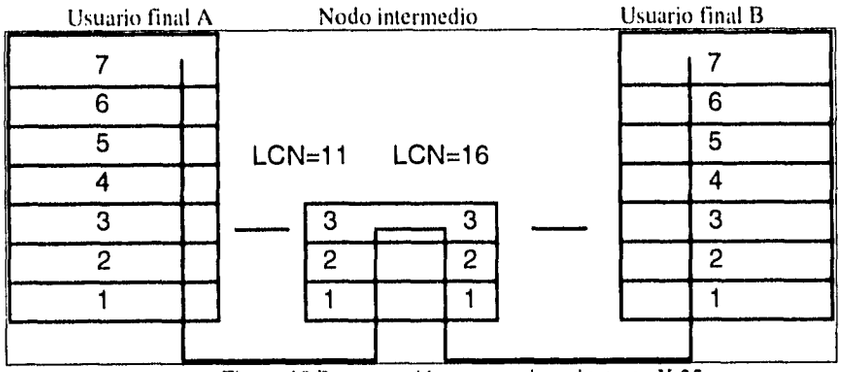

Figura 10 Regeneración y encaminamiento en X.25

A continuación , los datos se entregan a un determinado programa, el cual lleva a cabo las funciones de encaminamiento (estas funciones no forman parte del X.25). Los datos regresan a X.25 (y a los niveles inferiores) y se transmiten desde el nodo intermedio (que podría ser el nodo de la red (ETCD) correspondiente al usuario B) hacia el ETD del usuario B.

Son varias las razones por las cuales se aconseja utilizar una norma como X.25. En primer lugar, la adopción de un estándar común a distintos fabricantes nos permite conectar facilmente equipos de distintas marcas. En segundo lugar, la norma X.25 ha experimentado numerosas revisiones, y hoy por hoy puede considerarse relativamente madura. En tercer lugar, el empleo de una norma tan extendida como X.25 puede reducir sustancialmente los costos de la red, ya que su gran difusión favorece la salida al mercado de equipos y programas orientados a tan amplio sector de usuarios. Por último, es mucho más sencillo solicitar a un fabricante una red adaptada a la norma X.25 que entregarle 180 páginas de especificaciones de otro fabricante.

3.4.6 SNA

El modelo de arquitectura para sistemas en red (Systems Network Arquitecture) es un modelo de siete capas que es similar, aunque no idéntico, al Modelo de Referencia OSI. Una de las razones para esa diferencia es que el SNA fue anunciado primeramente en 1974 y precedió al Modelo de Referencia OSI por varios años. Aunque el trabajo sobre el Modelo de Referencia OSI comenzó en los últimos años de la década de los 70's, no fue publicado sino hasta 1984. Una segunda razón fue que IBM desarrolló el SNA como parte de su arquitectura de red propietaria; la Organización Internacional sobre Estándares designó al Modelo de Referencia OSI como un estándar abierto para interconectar redes de diferentes fabricantes. Dado que los dos modelos provienen de diferentes perspectivas, no es sorprendente que tengan algunas divergencias.

La arquitectura SNA divide sus niveles funcionales como a continuación se describe. Los tres niveles más bajos (Físico, Control de Enlace de Datos, y Control de Rutas) habilitan los procesos de los usuarios terminales para transmitir y recibir datos. Por esta razón, estos niveles son llamados Servicios de Red de Control de Ruta. Los cuatro niveles superiores (Control de Transmisión, Control de Flujo de Datos, Servicios de Presentación, y Servicios de Transacción) definen las funciones que las Unidades Direccionables de Red (NAUs) realizan dentro de un nodo específico. (Hay tres tipos de NAUs. El Punto de Control de Servicio del Sistema (SSCP) reside dentro del host y administra la red. Una Unidad Física (PU) representa un dispositivo de hardware o software en la red. Una Unidad Lógica (LU) es una adición lógica a través de la cual los usuarios finales pueden intercambiar datos.)
Para una vista con un poco de más profundidad, consideremos brevemente cada uno de los niveles separadamente.

Nivel de Control Físico

El Nivel de Control Físico maneja la transmisión de bits sobre un circuito físico. Aunque el nivel de control físico es direccionado en la arquitectura, el modelo SNA no define protocolos específicos en este nivel. En cambio, la arquitectura SNA asume el uso de diversos estándares internacionales existentes en este nivel.

Nivel de Control de Enlaces de Datos

El Nivel de Control de Enlace de Datos es el responsable de la transmisión de información entre dos nodos sobre un enlace físico en particular. Una función primaria de este nivel es el detectar y recuperar errores de transmisión.

Nivel de Control de Ruta

El Nivel de Control de Ruta concierne al ruteo de información desde un nodo hacia el siguiente en la ruta que el mensaje toma a través de la red. Esta ruta frecuentemente cruza diferentes nodos mientras un mensaje se mueve desde un nodo fuente hacia un nodo destino.

Nivel de Control de Transmisión

El Nivel de Control de Transmisión mantiene la pista del estado de los enlaces, o sesiones, entre los usuarios de la red, controla el ritmo del flujo de datos en una sesión, y observa que las unidades de datos que conforman un mensaje sean enviadas y recibidas en la secuencia apropiada. Este nivel también proporciona facilidades opcionales para encriptar y desencriptar datos.

Nivel de Control de Flujo de Datos

El Nivel de Control de Flujo de Datos se refiere a la integridad general del flujo de datos durante una sesión entre dos usuarios de red. Esto puede involucrar la determinación del modo de enviar y recibir datos, manejar grupos de mensajes relacionados, o determinar el tipo de modo de respuesta a ser usado.

Nivel de Servicios de Presentación

El nivel de Servicios de Presentación es el responsable de dar formato a la información para los diferentes medios de presentación usados en una sesión. Esto involucra la conversión de mensajes desde un código de caracteres a otro y el formateo de la información para ser desplegada en diferentes tipos de dispositivos.

Nivel de Servicios de Transacción

Este nivel proporciona servicios de aplicación a usuarios finales de la red, éstos incluyen: el control del operador sobre las sesiones, la distribución e intercambio de documentos, y el acceso a la información distribuída.
Ninguna red de área local se apega completamente a la arquitectura SNA. Sin embargo, el modelo SNA es importante a la tecnología de LANs porque en muchas situaciones, una red de área local debe conectarse, y ser convertida, en una parte lógica de una red con un mainframe SNA.

3.5 DISPOSITIVOS DE INTERCONEXION

Son dispositivos que sirven para comunicar redes de diferentes configuraciones y topologías, permitiendo su comunicación y entendimiento sin importar restricciones técnicas.

Tal como las plantas manufactureras tienen cuartos de correo y puertos de embarque las redes de área local tiene lugares específicos llamados dispositivos de interconexión (repetidores, puentes, gateways y enrutadores); estos prolongan y segmentan el cable de alta velocidad de las redes de área local y cada dispositivo ofrece un diferente grado de discriminación y capacidad de manejo de datos.

Si dos redes utilizan la misma señal en la red y el mismo protocolo de control de acceso, como Ethernet, las redes pueden ser enlazadas con un puente existente en cada LAN. Pero si las redes son diferentes, por ejemplo, si una está basada en Ethernet y otra utiliza Token Ring, los enrutadores serían la mejor alternativa dado que estos transforman los paquetes formateados para IPX o IP de los frames de bajo nivel a través de los enlaces de inter-LAN's. Los enrutadores alguna vez fueron muy complejos y caros a comparación de los puentes, pero las diferencias entre las capacidades de los productos se han reducido, de tal forma que hoy los enrutadores son preferidos ya que ellos colocan menos datos sobre los costosos circuitos de comunicación. En las siguientes secciones se presentará una breve descripción de los dispositivos antes mencionados.

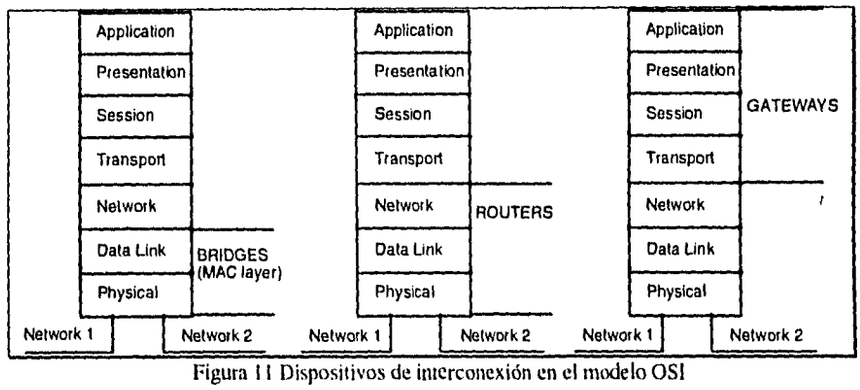

Figura 11 Dispositivos de interconexión en el modelo OSI

3.5.1 Repetidores

El dispositivo más simple utilizado para extender el segmento de las redes es el *repetidor*. Los repetidores no son utilizados para interconectar redes que no sean similares, sino para conectar segmentos individuales de red que formen una red extendida más grande. La figura 12 ilustra el uso de un repetidor. La función de un repetidor es recibir un mensaje y retransmitirlo, regenerando la señal a su potencia original.

Repetidor

Fig. 12

Una LAN usualmente tendrá un límite en el tamaño físico de cualquiera de sus segmentos de red. Este límite está basado en el medio físico y la técnica de transmisión utilizada. Los repetidores ayudan a una red a estar construída de tal manera que pueda exceder el tamaño físico de un segmento de la red, permitiéndole conectar segmentos de cable adicionales para formar una red extendida. El número de repetidores que pueden ser usados en cascada es también generalmente limitado por la arquitectura de la red.

Los repetidores son comunmente utilizados con LANs que usan una topología de bus. Para aquellas con una topología de anillo, cada estación actúa típicamente como un repetidor, recibiendo un mensaje y retransmitiéndolo con la señal restaurada a su potencia total.

Para que un repetidor pueda ser usado, ambos segmentos de red deben ser del mismo tipo. Los dos segmentos deben usar los mismos protocolos de red para todos los niveles (capas), incluyendo el uso del mismo método de control de acceso al medio y la misma técnica de transmisión física. De tal manera, por ejemplo, un repetidor puede ser usado para interconectar dos segmentos de red que utilizan el CSMA/CD con una transmisión de banda ancha. A las estaciones en diferentes segmentos de red no se les permite tener la misma dirección de red, todas las direcciones individuales en la red extendida, deben ser únicas.

3.5.2 Puentes

Un segundo elemento que puede ser usado para conectar segmentos de red es llamado *puente*. Un puente es capaz de interconectar redes distintas físicamente. Un puente puede ser un dispositivo separado pero es típicamente una estación que pertenece a dos o más redes simultaneamente. El puente recibe todos los mensajes en cada red de la que forme parte. Checa las direcciones de destino, y cuando reconoce que el mensaje es dirigido a una estación en una red diferente, transmite el mensaje en esa red. Así, por ejemplo, una estación

B envía un mensaje a la estación N, la estación C recibe el mensaje como parte de la red 1 y lo retransmite en la red 2, como se ilustra en la figura 2. Este tipo de conexión implementa una función de *almacena-y-envía*, dado que los mensajes son almacenados temporalmente en el puente y después enviados a otra red.

La figura 13 muestra que un puente opera en el nivel de enlace de datos. Una interconexión con

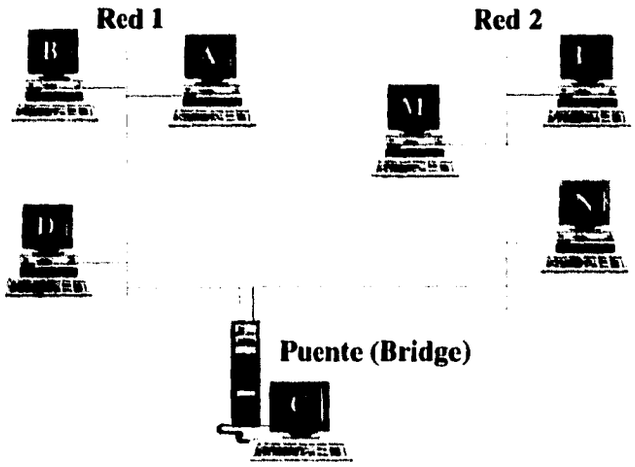

Fig. 13

puentes puede ser utilizada para redes que usen diferentes protocolos en el nivel físico, mientras utilicen un protocolo común en el nivel de enlace de datos. Por ejemplo, una red utilizando CSMA/CD con una transmisión de banda ancha sobre cable coaxial podría utilizar un puente para conectarse con una red CSMA/CD usando transmisión de banda base sobre cable de par trenzado. Es también posible para un puente implementar una interconexión entre LANs utilizando diferentes MACs (controles de acceso al medio), por ejemplo una red CSMA/CD con una red Token Ring. Aquí ambas redes deben tener implementaciones compatibles del subnivel de control de enlace lógico (LLC), y la estación puente debe ser capaz de direccionar mensajes en el nivel LLC. El puente debe ser también capaz de resolver diferencias de formato de frame o algunas otras entre los dos métodos de MAC.

Nuevamente, todas las direcciones en las redes interconectadas deben ser únicas y deben usar el mismo formato (16-bits o 48-bits). Las redes deben también usar formatos y tamaños de marco que sean lo suficientemente similares de tal manera que cualquier diferencia pueda ser manejada en el nivel de enlace de datos.

Para pasar mensajes apropiadamente, una estación que opere como puente debe saber cuáles estaciones pertenecen a las diferentes redes a las que está interconectando. Para lograr esto se le puede proporcionar al puente la información desde un medio externo, tal como un administrador de red. La estación que actúe como puente puede también ser programado para "aprender" esta información, por ejemplo, enviando un mensaje de difusión en una de las redes y solicitando respuesta de todas las estaciones en esa red. Un puente puede también aprender la ubicación de una estación al observar sus transmisiones. Cuando la estación C detecta una transmisión en la red 1 con A como la dirección fuente, graba a la estación A como perteneciente a la red 1. Cuando observe una transmisión en la red 2 teniendo como origen a la estación N, almacenará que la estación N pertenece a la red 2. El puente puede entonces usar esta información almacenada para determinar cuando reenviar un mensaje.

3.5.3 Enrutadores

Una forma con más capacidades para interconexión de redes utiliza un dispositivo llamado en*enrutador* o *sistema intermediador (o mediador).* El uso de un enrutador está basado en un concepto que no ordinariamente se aplica dentro de una sola red de área local, este concepto es el ruteo de un mensaje a través de nodos intermedios. Dentro de una LAN, cuando un mensaje es transmitido es enviado a todos los nodos en esa red. Un nodo receptor determina según la dirección de destino, si debe recibir ese mensaje y procesarlo. Sin embargo, cuando una LAN se interconecta con otras redes, ya sea una WAN (red de área amplia) o con otras LANs, el ruteo se convierte en un elemento crítico.

Con otros tipos de redes, particularmente WANs, un mensaje es ordinariamente enviado de un nodo a otro nodo específico en la red, y el mensaje puede pasar a través de una serie de nodos intermedios antes de que alcance el nodo destino. Puede haber más de una secuencia de nodos (más de una *ruta*) que un mensaje pueda tomar para llegar del nodo emisor al nodo destino.

Cuando un mensaje es ruteado a través de nodos intermedios, deben acompañarlo dos direcciones. La primera es la dirección del nodo de destino final del mensaje; esta dirección permanece constante mientras el mensaje atraviesa la red. La segunda es la dirección del siguiente nodo a lo largo de la ruta; esta dirección cambia mientras el mensaje se mueve de nodo a nodo a través de la ruta que tome en la red.

Para que un enrutador pueda ser usado, las redes que están siendo interconectadas deben compartir los mismos protocolos de red y deben ser compatibles en niveles más altos. Las redes pueden diferir, sin embargo, en los niveles físico y de enlace de datos. Así, por ejemplo, un enrutador puede ser usado para interconectar una LAN que utiliza el estándar IEEE *token bus* y el control de enlace lógico de IEEE con una WAN que utiliza técnicas de conmutación de paquetes y el protocolo X.25 en el nivel de enlace de datos, mientras ambos han implementado protocolos compatibles en el nivel de red y superiores.

Se pueden utilizar múltiples enrutadores, y pueden ser conectados de manera que permitan diferentes caminos (rutas) entre cualquier par de redes, como se muestra en la figura 14 .Si

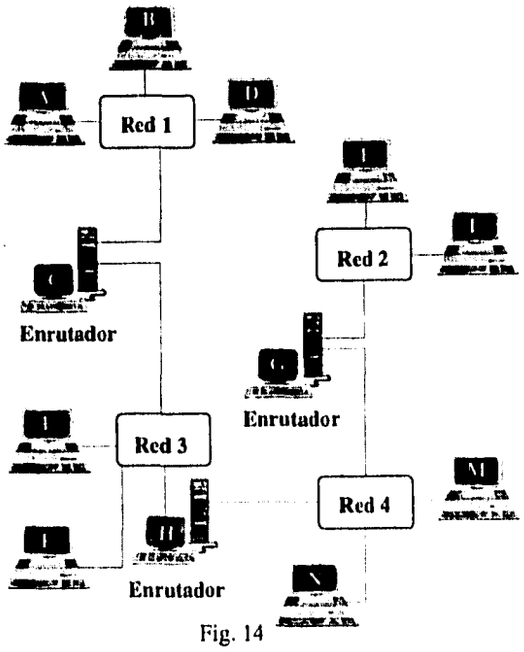

Fig. 14

un mensaje se está enviando del nodo B al nodo M, es primero dirigido al nodo enrutador C, el cual lo envía ya sea al nodo G o al H. Dado que los mensajes son enviados a un nodo enrutador, la presencia de múltiples caminos no causará que un mensaje sea multiplicado. La posibilidad puede existir, sin embargo, de que diferentes unidades relativas (pertenecientes) a un mensaje tomen diferentes caminos y puedan arrivar fuera de secuencia. Si esto es posible, las capas más altas de red deben estar preparadas para re-secuenciar esas unidades pertenecientes al mensaje.

Una tarea clave de un enrutador es el determinar el siguiente nodo hacia el cual el se dirigirá el mensaje; se pueden utilizar diferentes métodos para lograr esto. El ruteo de información puede ser predefinido como parte del diseño de la red y como función de la administración, y puede ser almacenado en forma de tablas de ruteo. Los enrutadores pueden desarrollar un mapa de la topología de la red intercambiando información acerca de los nodos activos y sus enlaces (uniones), y en ese momento seleccionar una ruta basada en el mapa actual de la red. Cuando se utiliza algo llamado *ruteo fuente*, el enrutador fuente (o inicial), o la estación emisora especifican la ruta total que será utilizada. Esto puede estar basado en información predefinida o en información recibida como resultado de un mensaje de difusión. No han surgido aún estándares para un ruteo equivalente a los estándares de IEEE.802 para los niveles de red más bajos. Esta carencia de estándares definidos ha dado como resultado la

diversidad en los algorítmos de ruteo utilizados (EGP, RIP, STA, ver apéndice D) y en las diferentes implementaciones de red. Los enrutadores son más comunmente usados cuando se interconectan redes de un mismo proveedor o en redes basadas en la misma arquitectura.

La figura anterior ilustra también, que las direcciones de los nodos no tienen que ser únicas a través de las redes interconectadas. La estructura de direccionamiento usada por la capa de red y superiores a menudo permiten una dirección que consta de varias partes (dirección multipartita), la cual consiste de un identificador de red y de una dirección de nodo dentro de una red. En este caso, la dirección de nodo debe ser única en esa red a la que pertenece pero no necesariamente en el entorno del conjunto de redes que se están interconectando.

3.5.4 Gateways

El último y más complejo método de interconexión de redes es un *gateway*. Un gateway es utilizado para interconectar redes que pueden tener arquitecturas totalmente diferentes. Un gateway, por ejemplo, puede ser usado para interconectar una red SNA con una red de conmutación de paquetes que se apega al modelo OSI.

Como resultado de que se usan diferentes arquitecturas, pueden entonces, ser usados diferentes protocolos en cualquiera o en todos las capas de la red. El gateway maneja cualquier conversión que es necesaria para ir de un conjunto de protocolos hacia otro, incluyendo estas:

- Conversión de Formato del Mensaje
Las redes pueden emplear diferentes formatos de mensaje, tamaños máximos de mensaje, y códigos de caracteres. El gateway debe ser capaz de convertir mensajes a un formato, tamaño, y código apropiado para la red a la que está entrando el mensaje.

- Traducción de direcciones
Las redes pueden usar diferentes estructuras de direccionamiento. El gateway debe ser capaz de traducir todas las direcciones asociadas a un mensaje de acuerdo a la estructura de direcciones requerida por la red de destino.

- Conversión de Protocolos
Cuando un mensaje es preparado para su transmisión a través de una red, cada capa de red le agrega información de control que es usada por la capa correspondiente en el nodo receptor para determinar qué protocolos se están usando y cómo debe ser procesado el mensaje. Un gateway debe ser capaz de reemplazar la información de control de una red con la información de control que es requerida para realizar funciones comparables en la otra red. Esta conversión debe permitirle a los servicios tales como el de segmentación y reensamble de mensajes, el de control del flujo de información, y los de detección y recuperación de errores ser ejecutados de una manera consistente mientras el mensaje atraviesa las redes.

Los gateways ofrecen la flexibilidad más grande en la interconexión de redes, dado que dos redes completamente diferentes pueden ser enlazadas. Sin embargo, los gateways son más complejos y más caros en su implementación. Estos son típicamente construídos para interconectar redes que se adecúan a dos tipos de arquitectura de red específicos. Dado que se debe proporcionar la conversión para protocolos en cada nivel, el diseñar un gateway generalizado se llega a convertir en algo realmente complejo.

3.5.5 Modems

El sistema telefónico analógico no puede soportar los cambios de tensión continua requeridos para la transmisión digital de datos. Los teléfonos estan construídos para transportar la información de voz. Por ello, los datos digitales tienen que ser convertidos primero a señales de audio que puedan ser transmitidas por las líneas telefónicas. Esta conversión de 1's(unos) y 0's(ceros) digitales a señales de audio se denomina *modulación*. La reconversión de estas señales de audio a niveles digitales al otro extremo de la línea de comunicaciones se denomina *demodulación*. El dispositivo capaz de realizar estas conversiones se denomina modulador/demodulador, y su abreviatura es *modem*.

Los primeros modems, eran mucho más lentos que los que manejan estándares actuales, capaces de transmitir exclusivamente a 110, 150 ó 300 bps. Los siguientes modems funcionaban a la velocidad mucho más respetable de 1200 bps. No mucho después, aparecieron los modems de 2400 bps; actualmente, los modems de 1200 y 2400 bps. constituyen el extremo inferior de la gama de modems actuales instalados. La compatibilidad entre modems de 300, 1200 y 2400 bps de distintos fabricantes rara vez resulta problemática, ya que (si no todos) la mayoría de los modems utilizan las mismas técnicas de modulación.

Luego aparecen los modems de alta velocidad. El estándar actual mínimo es de 9600 bps. Utilizando nuevos protocolos y técnicas de compresión de datos, muchos de estos modems alcanzan una velocidad efectiva mucho mayor de 9600 bps; llegando en algunos casos a 19200 bps.

Los dos estándares de modulación que están acaparando la mayoría de la atención son V.29 y V.32 que son recomendaciones publicadas por la CCITT

Técnicas de modulación: V.29 y V.32

Existen dos tipos de modems: full-duplex y semiduplex. Los modems full-duplex pueden enviar y recibir datos simultáneamente; los modems semiduplex transmiten en un sentido cada vez, teniendo que "darle la vuelta a la línea" para invertir el flujo de datos.

Las normas V.29 y V.32 de la CCITT son los dos estándares principales de modulación para 9600 bps. V.29 es el estándar para semiduplex, V.32 se centra en la modulación full-duplex y ofrece más posibilidades de compatibilidad entre los fabricantes que V.29.

3.6 Red Digital de Servicios Integrados (RDI)

El concepto de una Red Digital Integrada (RDI) es una red que proporciona facilidades universales de comunicación entre muchos tipos diferentes de usuarios. Una RDI eficiente utiliza un sistema de transmisión común para todos los tipos de tráfico, y proporciona un acceso estándar a la red para todos los diferentes tipos de equipo terminal a los que debe servir. Las terminales existentes que no son compatibles son convertidas para que soporten este acceso estándar mediante el uso de adaptadores, mientras que las terminales que son diseñadas para la RDI automáticamente se ajustan a ella.

Las ventajas de una RDI tanto para los administradores como para los usuarios son numerosas. Una Red Digital Integrada es mucho más efectiva en cuanto a costo que el tener varias redes diferentes. Una red, utilizando equipo común para todos los tipos de tráfico, utiliza los recursos disponibles de la red más eficientemente y, de una manera adicional representa una reducción general en los costos de mantenimiento. También alcanza la meta deseable de tener capacidades de comunicación universales multi-modo, y ofrece una calidad realzada significativamente en las transmisiones comparada con el desempeño de las redes analógicas del presente. Las velocidades de transmisión más altas ofrecidas por RDI son particularmente atractivas para los servicios de transmisión de datos.

El principal esfuerzo de una RDI es proporcionar comunicación e interconexión de sistemas abiertos, y es la siguiente etapa inevitable en la evolución de las redes de telecomunicación del mundo. Es concebida para racionalizar las redes actuales, las cuales se han desarrollado y evolucionado muy independientemente las unas de las otras, y de proporcionar en una red integrada la gama de servicios comúnmente ofrecida individualmente en los diferentes tipos de redes públicas.

La primer etapa de la RDI proporcionará servicios de "narrowband" para canales de suscriptores digitales a 64 kbit/s. Subsecuentemente los servicios de "wideband" y de "broadband" son planeados, los cuales cubren velocidades de transmisión de hasta 140 Mbit/s. Una RDI de banda ancha proporcionará facilidades potenciales para TV de alta calidad, etc.

4. DISEÑO DE LA RED COORPORATIVA

4. DISEÑO GLOBAL DE LA RED CORPORATIVA

El presente capítulo trata de las consideraciones y recomendaciones generales para el diseño de la red corporativa; como es el esquema de direccionamiento, parte fundamental del funcionamiento de una red de área amplia, así como de la interacción de los diversos dispositivos que permiten la convivencia de las diferentes plataformas contempladas. También se dan las recomendaciones del uso de la topología para las diferentes redes a utilizar, así como los elementos de hardware a utilizar en el diseño de la solución al presente trabajo de tesis.

4.1 RECOMENDACIONES PARA LOS ELEMENTOS DE LA RED

Uno de los objetivos de la presente tesis es definir las recomendaciones de los elementos de la red como son los dispositivos de comunicación, sistemas operativos y protocolos. Por lo que se recomienda únicamente lo que en este capítulo se menciona y no se hace responsable del impacto que puede ocasionar la incorporación de cualquier otro elemento en la red que no cumpla con los estándares aquí mencionados y con las recomendaciones que a continuación se listan.

Topologías

La topología de la red, o el esquema de alambrado de sus nodos y líneas, afecta a la manera de como la red transmite sus datos. Una topología bien planeada utiliza de una manera eficiente los recursos como cableado, modems, enrutadores, puentes y multiplexores para crear el máximo número de enlaces lógicos posibles entre los nodos.
Las topologías seleccionadas para las redes locales son:

- Bus para Ethernet
- Ring para TokenRing

Las dos topologías recomendadas, utilizando concentradores, se ven físicamente como una estrella, aunque lógicamente conservan sus características de bus o ring.
La topología seleccionada para las redes amplias (WAN), basadas en enrutadores es:

- Multi-estrella

Hardware de red

En las recomendaciones de hardware existen algunos puntos en común que deben ser tomados en cuenta para la selección de los diferentes elementos que se integren a la red. A continuación se listan las características de hardware, así como el soporte necesario que deben brindar los proveedores; estos se tomaron en cuenta para la selección de los elementos que conforman la red de CBB, mismos que a continuación se listan:

Por parte de los proveedores deben cumplir con:

- Garantía mínima de 12 meses
- Documentación y soporte local
- Marca y fabricante confiables

Las tarjetas para las interfaces de red de las PCs que se incorporen a la red de CBB deben de cumplir con los siguientes puntos:

- Estándares Ethernet (IEEE 802.3) y Token Ring (IEEE 802.5)

- Soportar NDIS y ODI
- De 16 bits mínimo de acuerdo con la arquitectura de cada equipo
- Configurables por software
- Interface UTP

Los concentradores TokenRing deben cumplir con los siguientes puntos:
- Interfaces UTP
- 12 o más puertos
- Soportar Ring-In, Ring-Out
- LEDs indicadores de operación
  Montables en los closets de comunicaciones
- Soportar conversión de medios
- Soportar hardware y software de administración y monitoreo SNMP

Los concentradores Ethernet deben cumplir con los siguientes puntos:
- Interfaces UTP
- 8 o más puertos
- Soportar el crecimiento modular
- LEDs indicadores de operación
- Montables en los closets de comunicaciones
- Soportar conversión de medios
- Soportar el Protocolo de administración SNMP

El cableado para las redes locales debe cumplir con los siguientes puntos:

- Cable UTP nivel 5
- Rosetas con conector RJ45, etiquetadas
- IDF en cada piso, con etiquetas
- Métodos de parcheo o administración AT&T 110 o 66 Blocks
- MDF central

Los servidores de terminales deben cumplir con los siguientes puntos:

- Independientes de los hosts de la red
- Capacidad para configurarse local y remotamente
- Capacidad de soportar modems
- Capacidad para soportar los protocolos de comunicación TCP/IP, SLIP y PPP
- Capacidad de soportar el protocolo de administración SNMP
- Interfaces UTP para conectar a los usuarios
- Interface UTP o AUI para conectarse al backbone Ethernet

Los enrutadores deben soportar los siguientes puntos:

- Protocolos de usuario
  - TCP/IP
  - IPX
  - SLIP o PPP
  - SRB
  - SRT
  - SDLC
  - HDLC
  - X.25
- Protocolos de enrutamiento
  - IGRP en caso de enrutadores Cisco
  - RIP
  - OSPF
  - IS-IS
- Interfaces
  - Ethernet
  - TokenRing
  - RS-232
  - V.35
- Crecimiento modular
- Puerto de consola
- Login local y remoto (telnet) para su configuración
- Configurables para funcionar como "router", "bridge" o "brouter"
- Comandos de monitoreo
- Balanceo automático de cargas
- Recuperación en caso de falla de alguno de los enlaces
- Soporte de agentes SNMP para la administración

Los Gateways deben soportar los siguientes puntos:

- Protocolos involucrados o que se requieran convertir, como ejemplo:
  - TokenRing IPX de Novell < > TokenRing SDLC de IBM
  - TCP/IP < > SNA de IBM

- Que soporten el número de usuarios concurrentes que se requiere
- Que funcionen con sistemas operativos multiusuario y multitasking (opcional)
- Que utilicen procesadores de arquitectura RISC (opcional)
- Configuración local y a través de algún nodo de la red (telnet) (opcional)
- Soportar software para la administración de la red (opcional)

Software de red

Los Sistemas Operativos de Red deben cumplir con los siguientes requisitos generales:

- Multiusuario y multitasking
- Bibliotecas compartidas
- Soportar arreglos de discos
- Grupos de usuarios
- Espacio delimitado en disco para usuarios
- Seguridad de acceso y de archivos
- Manejo de memoria caché
- Manejo de múltiples áreas de swap
- Soportar los protocolos TCP/IP, IPX
- Servicios NFS
- Utilerías para la administración
- Soportar el SNMP para la administración
- Soportar interfaces Ethernet y/o TokenRing
- Soportar software de comunicaciones y de administración de terceros para la interconectividad con otras plataformas

El sistema operativo Unix ha sido adoptado por las organizaciones que norman los estándares, esto se debe en gran parte por la facilidad que tiene para portar aplicaciones de una plataforma unix a otra unix y la conectividad con otras plataformas través del protocolo de red TCP/IP.

Otro sistema operativo de red es Netware de Novell, que ha tenido una gran aceptación en el mundo de las redes locales y sobre todo en ambiente de oficina, y que cumple con los requisitos antes mencionados.

En los tiempos que estamos viviendo, con la tecnología tan cambiante, en el mercado aparecen cada vez más productos de software que aprovechan mejor las nuevas tecnologías de hardware, como mejores manejadores de bases de datos, interfaces gráficas, herramientas CASE, y sistemas operativos. . Mismos que tardarán algun tiempo en madurar en el mercado de las redes.
Por el momento, se han seleccionado los siguientes sistemas operativos:

- NetWare 3.1x de Novell
- HP-UX 9.0x de Hewlett Packard (Unix)
- Solaris 2.x o SunOS 4.1.x de Sun Microsystems (Unix)

El software TCP/IP para PCs seleccionado es el PC-NFS 5.0. Para esto se llevó a cabo una evaluación de diferentes TCP/IPs. En resumen el software TCP/IP para integración de PCs debe cumplir con los siguientes puntos:

- Soportar las interfaces NDIS y ODI
- Facilidad de modificar los parámetros de default del TCP/IP
- Menu de configuración
- Ambiente MS-Windows
- Soportar los servicios básicos de TCP/IP
- Soportar los comandos "r" (remote commands)
- Soportar el protocolo SNMP para la administración
- Soportar respaldos en los nodos de la red (opcional)
- Soportar el correo electrónico E-mail (opcional)
- Soportar el protocolo tftp (opcional)

4.2 CONSIDERACIONES GENERALES DE DISEÑO

En la figura 15 se muestra el esquema global y esquemático de la red de datos, haciendo notar las características principales:

- La ubicación física de los sistemas centrales de los edificios Varsovia y Platino.
- Los enlaces RDI de Telmex y de Microondas de la red de BANCOMER utilizados para comunicar los sistemas AS/400 en espejo remoto entre los edificios de Varsovia y Platino.
- Los enlaces satelitales de la red de CBB utilizados en las sucursales como transporte.(respaldo).
- Los enlaces de la red BANCOMER utilizados en la sucursales como transporte.
- Los dispositivos de comunicación a emplearse son los enrutadores.
- La localización física de los equipos AS/400
- Las redes locales de los edificios de Varsovia y Platino
- Las redes locales de las sucursales y su integración de éstas con las redes locales de CBB de los edificios de Varsovia y Platino en la Ciudad de México
- Los enlaces de RDI y satelitales de CBB como una ruta primaria y de respaldo

- Los enlaces de la red BANCOMER como ruta primaria y/o alterna
- La creación de la Terminal Universal

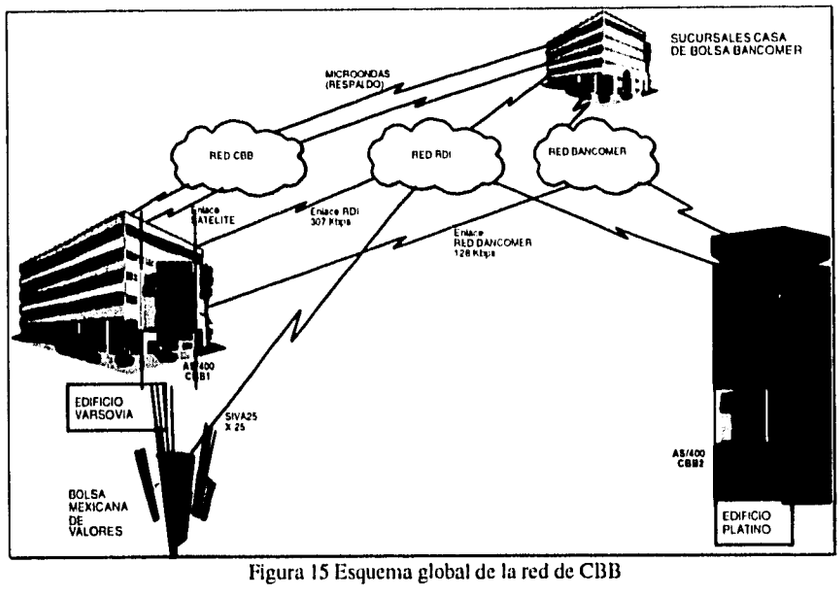

Figura 15 Esquema global de la red de CBB

En la figura 16 se muestra el diseño global de la red de datos de CBB, en la cual se aprecian los elementos que conforman la red. En este destacan los siguientes puntos:

El enlace RDI entre los edificios de Varsovia y Platino funciona actualmente como canal primario y el enlace de microondas con el edificio Roma Bancomer actúa como enlace alterno y/o respaldo. A través del uso de algoritmos de enrutamiento ambos enlaces pueden ser utilizados concurrentemente, además de proporcionar redundancia y respaldo.

A través de este esquema los equipos AS/400 estarán trabajando en espejo permitiendo que ambos sirvan de respaldo uno del otro. En la figura 18 se puede apreciar el beneficio que se obtiene al utilizar un solo esquema de comunicación para los sistemas AS/400 y la integración de las redes locales, integrando el ambiente IBM (terminales en SDLC), el ambiente TCP/IP y el ambiente Novell.

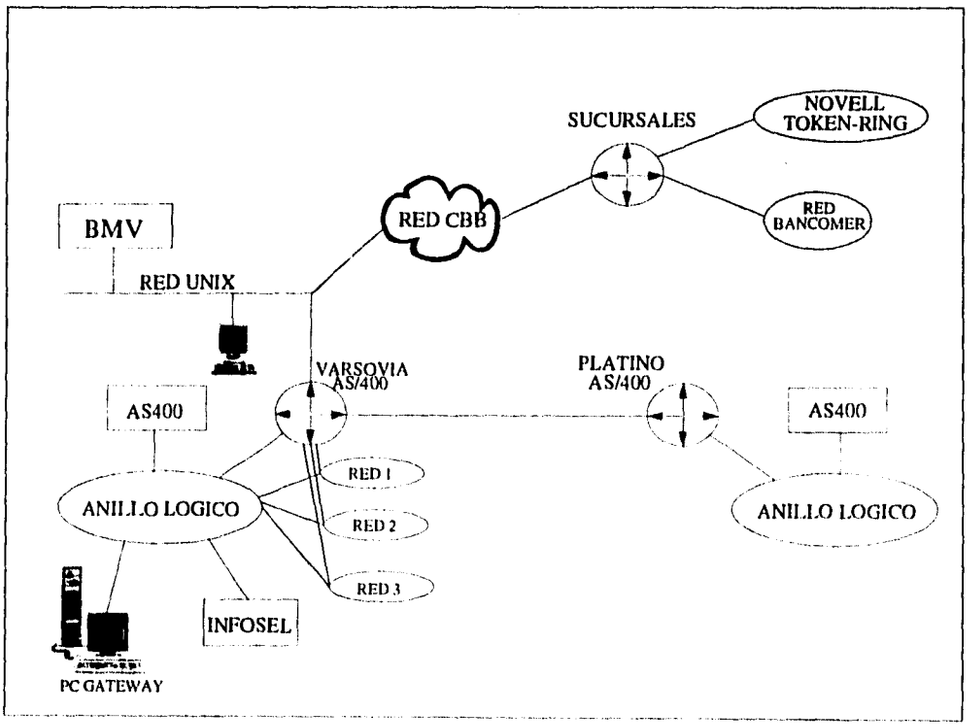
SUCURSALES
NOVELL
TOKEN-RING
RED CBB
RED
BANCOMER
BMV
RED UNIX
VARSOVIA
AS/400
PLATINO
AS/400
AS400
AS400
RED 1
RED 2
RED 3
ANILLO LOGICO
ANILLO LOGICO
INFOSEL
PC GATEWAY

fig. 16

4.3 DIRECCIONES DE RED IPX/NOVELL Y TCP/IP

DIRECCIONES IPX

Las direcciones IPX están formadas por dos componentes, el primero de ellos es el número de red y es asignado por el diseñador de la red de acuerdo a cierta nomenclatura y que permita la integración con otras redes similares. El segundo elemento es el número de nodo, también es conocido como la dirección física o "MAC address", en la siguiente figura se ilustra la forma como se identifica las direcciones IPX y TCP/IP.

Las direcciones de red Novell para CBB serán direcciones independientes, por lo que se asignarán los siguientes números de red por cada anillo de las redes TokenRing de CBB.

Red Anillo 1:	801	VARSOVIA-1
Red Anillo 2:	802	VARSOVIA-2
Red Anillo 3:	805	VARSOVIA-3
Red de Recursos:	810	
Red Platino:	803	PLATINO
Red Guadalajara:	804	GUADALAJARA

DIRECCIONES IP

En el mundo TCP/IP, los elementos de las direcciones de los nodos están formados por cuatro bytes o números separados por un punto que van de un rango de 0 a 255. A continuación se muestra la relación existente entre el direccionamiento IP y el de IPX.

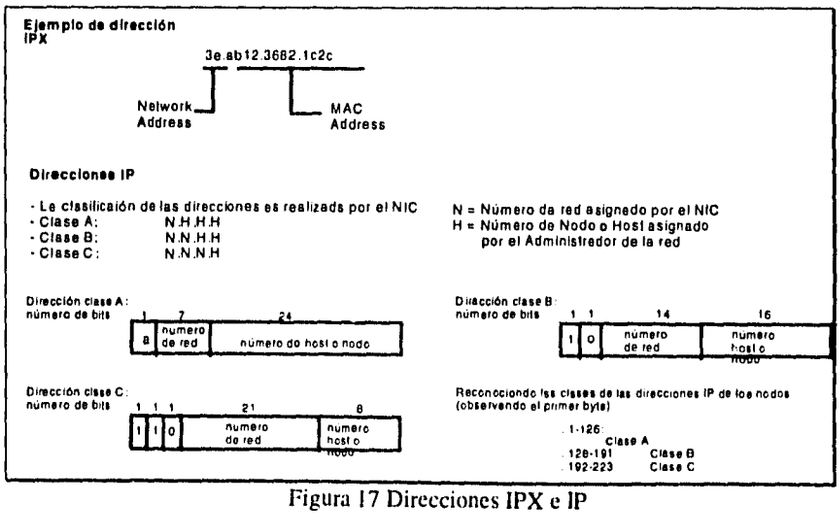

Figura 17 Direcciones IPX e IP

La clase y dirección de la red de CBB será de acuerdo a la clase seleccionada para la red Bancomer, ya que es del mismo grupo financiero, CBB podría ser una subred de la red Bancomer de acuerdo a la dirección proporcionada por Bancomer.

La clase de red para Casa de Bolsa Bancomer será una dirección de clase B.

Las direcciones IP para la red de CBB, han sido asignadas bajo los siguientes lineamientos:

Clase:	B
Dirección:	130.130
Subnet Mask:	8 bits
Broadcast:	16 bits todos 1's

Direcciones de redes:

Enlaces:	130.130.(1-135)
TokenRing:	130.130.(136-170)
Ethernet:	130.130.(171-205)
Reservados para futuro uso:	130.130.(206-254)

Direcciones de nodos:

Usuarios:	130.130.xxx.(1-200)
Servidores:	130.130.xxx.(201-220)
Puertos Ethernet y TokenRing del Cisco:	130.130.xxx.221
Otros dispositivos de comunicaciones:	130.130.xxx.(222-250)
Enlaces seriales:	130.130.xxx.(251-252)
Reservados para futuro uso:	130.130.xxx.(253-254)

En la figura 18 se pueden apreciar las direcciones IP e IPX definidas para la red de CBB.

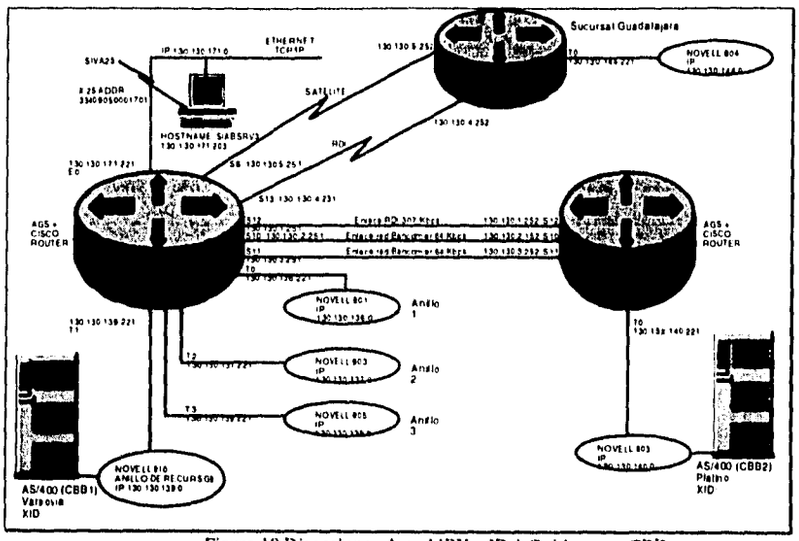

Figura 18 Direcciones de red IPX e IP definidas para CBB

REDES DE AREA LOCAL (LAN)

REDES DE AREA LOCAL (LAN)

En el presente capítulo se explica como fue estructurado el diseño de las redes de área local. Este se fué dando a través de la selección del cableado a implementar y su explicación. Posteriormente se menciona como fueron dándose las redes Token Ring y su evolución en el transcurso del proyecto. Se menciona como se integró la red Ethernet con las otras redes y la integración de ambas con el sistema AS/400. Todo lo anterior con la finalidad de llegar a tener una terminal universal que permitiera al usuario utilizar única y exclusivamente su PC como medio de trabajo integrando todas las aplicaciones, no importando donde residieran estás.

4.4 CABLEADO MODULAR Y ESTRUCTURADO

Una instalación de cableado o alambrado de comunicación de datos bien planeada es esencial para la competitividad de las organizaciones que forman redes a partir de sus recursos de hardware y software.

Cada tipo de cable o método tiene sus ventajas y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad (radio). La velocidad y la longitud del tendido son otros factores a tener en cuenta a la hora de considerar el tipo de cable a utilizar.

Entre las topologías de red más utilizadas se encuentran el Bus, el Token-Ring y la Estrella Jerárquica. Entre los estándares se encuentran el cable par trenzado (UTP y STP), fibra óptica multimodo (62.5/125 µm) y fibra óptica monomodo (9/125 µm).

En los edificios de Varsovia y Hamburgo de CBB se instalará un cableado modular y estructurado basado en el sistema SYSTIMAX de AT&T, el cual integra los datos en un "backbone" vertical de fibra óptica de 12 fibras multimodo.

El sistema de cableado seleccionado para CBB es el Sistema de Distribución Local para Edificios (PDS) Systimax de AT&T que ofrece una plataforma tecnológica de vanguardia en la cual, CBB puede desarrollar su red de área local para la convivencia de diversas arquitecturas en procesamiento de datos y conmutación de voz; también ofrece la arquitectura abierta para futuras aplicaciones sujetas a las recomendaciones de los organismos que norman los estándares como la ISO, OSF y CCITT.

La electrónica asociada y los paneles de parcheo permiten utilizar en la distribución horizontal el mismo medio de transmisión para los dos tipos de servicio.

El cableado utilizado en las redes es el UTP 1061 de AT&T, el cual soporta la velocidad de 16Mbps de Token-Ring y 10Mbps de Ethernet.

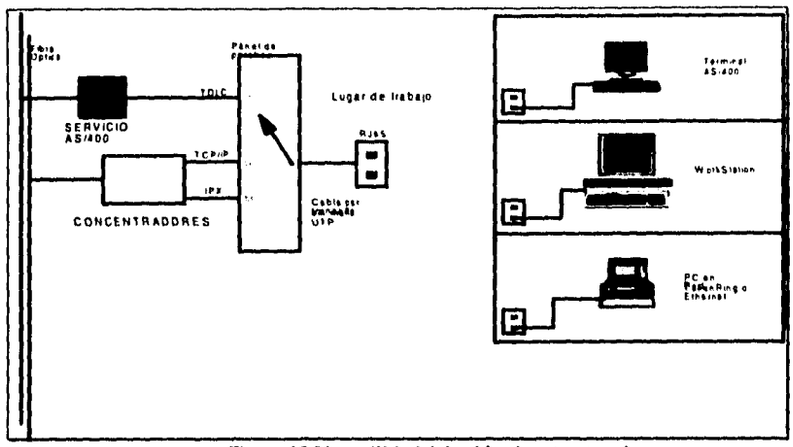

Figura 19 Versatilidad del cableado estructurado

4.5 REDES NOVELL TOKEN-RING

La primer red local diseñada y puesta en operación en CBB, fue la red Novell TokenRing del edificio Hamburgo llamada (HAMBURGO), con 40 usuarios.

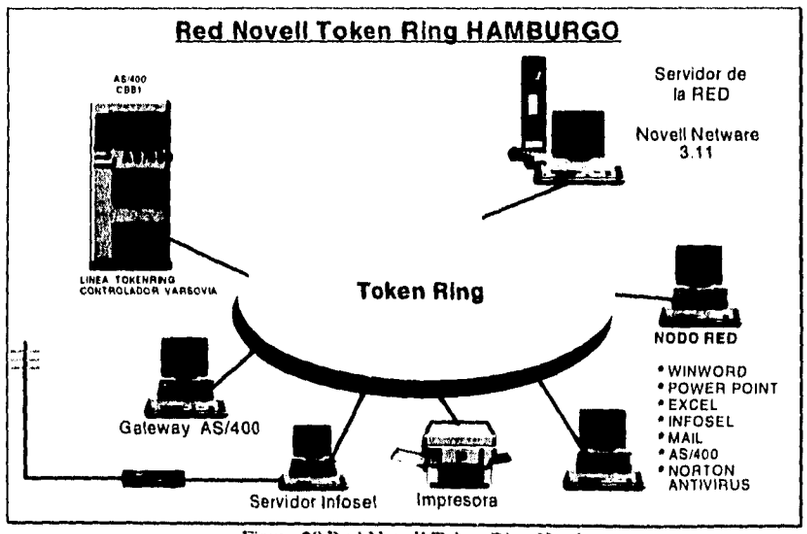

Figura 20 Red Novell Token Ring Hamburgo

La segunda red que se incorporó en CBB fue la red Novell Token-Ring del edificio Varsovia llamada (VARSOVIA-1) y servía a los pisos PB y 1, atendiendo 45 usuarios.

La tercera red Novell Token-Ring proporciona servicio a los 40 usuarios de los pisos 2, 1 y PB y también se unió al anillo de las dos redes anteriores. Para que quedara un solo anillo lógico.

Se incorporó una cuarta red considerando el crecimiento futuro de CBB la cual serviría a los pisos 4, 5 y 6.

Los anillos de cada piso fueron unidos por medio de los puertos RING-IN y RING-OUT de los concentradores SYNOPTICS, para formar un solo anillo lógico.

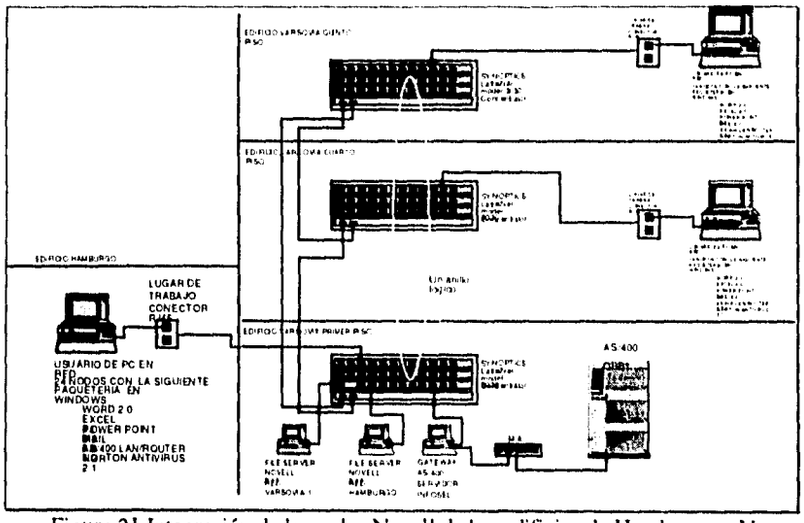

Figura 21 Integración de las redes Novell de los edificios de Hamburgo y Varsovia

Asimismo se incorporaron *puentes* que separaran los anillos para mejorar el rendimiento de la red. La separación de los anillos se llevó a cabo incorporando interfaces Token-Ring al enrutador de Varsovia para que realizará las funciones de *"puente"*.

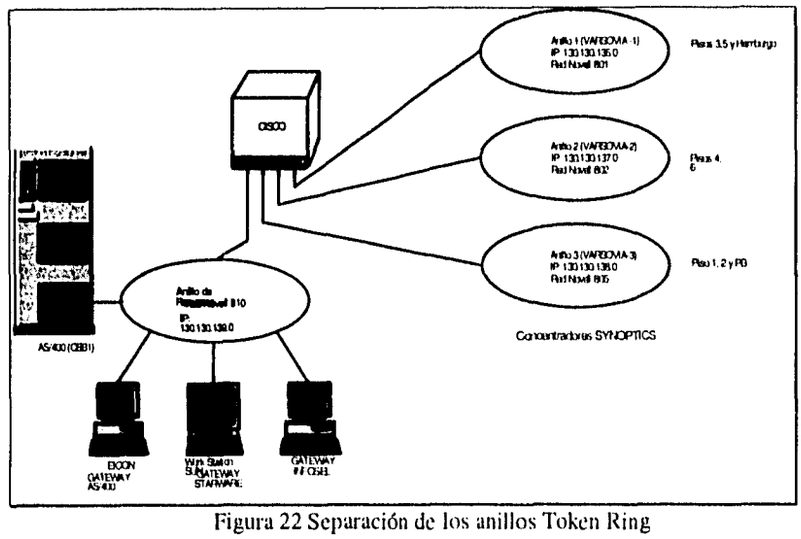

Figura 22 Separación de los anillos Token Ring

En los siguientes párrafos se comenta en forma global los elementos que conforman las redes Novell Token-Ring, así como los beneficios que ofrecen éstas. Las redes locales Token-Ring de los edificios Hamburgo y Varsovia están trabajando con el sistema operativo de red Novell Netware 3.11.

En cada uno de los nodos se instaló una tarjeta Token-Ring PROTEON 1392 con interface UTP, que es conectada directamente a la roseta del lugar. Los concentradores utilizados son SYNOPTICS MOD 3050.

Entre los principales beneficios que proporcionan las redes Novell Token-Ring para el usuario y el administrador de Redes se encuentran los siguientes:

* Compartir discos para todos los usuarios
* Servicio de impresión en red común para los usuarios
* Los usuarios trabajan bajo un sólo ambiente gráfico
* Facilita el mantenimiento a la paquetería institucional de oficina para Windows

Las PCs son conectadas a la red a tráves de la tarjeta Etherlink III 3C509-COMBO, la cual permite conectar tres diferentes tipos de interfaces (AUI, BNC y UTP), para conectarla directamente a la roseta.

Los adaptadores 3Com Etherlink III Parallel Tasking son una familia de la tercera generación de adaptadores Ethernet. Estos adaptadores incluyen una Arquitectura Industrial Standar (ISA) de 16 bits y una Arquitectura Industrial Standar Extendida (EISA) de 32 bits, ambos adaptadores para conexiones coaxial y 10BASE-T. Las especificaciones de esta

tarjeta adaptadora son las siguientes: IEEE 802.3i 10BASE-T y Ethernet IEEE 802.3 estándar industrial para una red de área local.

4.6 RED UNIX ETHERNET

El tipo de topología que utilizan las redes Unix puede ser Ethernet o Token Ring. Los equipos cliente son principalmente estaciones de trabajo PCs y estaciones de trabajo Unix, los equipos servidores están basados en Unix.

La razón de utilizar PCs como cliente y no algún otro equipo, consiste en la necesidad de muchos usuarios de poder correr las aplicaciones tradicionales del sistema operativo DOS en las PCs. El ambiente de las PCs debe consistir en un ambiente gráfico tipo MS-Windows que soporta aplicaciones tanto de DOS como de Unix. Las PCs también requieren el servicio de archivos e impresoras; es decir, el usuario de la PC deben accesar los discos e impresoras de los servidores Unix como si estuvieran localmente conectados a la PC.

La razón de utilizar servidores Unix dentro de las redes locales está principalmente en la posibilidad de correr aplicaciones de bases de datos en estos servidores conjuntamente con las demás aplicaciones desarrolladas para Unix y ambiente gráfico XWindows. El servidor Unix puede adicionalmente correr aplicaciones muy robustas. Los actuales proveedores de bases de datos, cuentan con versiones de sus productos para todas las plataformas Unix. Con estas herramientas, los usuarios pueden desarrollar con rapidez sus propias aplicaciones y correrlas en los equipos servidores de red.

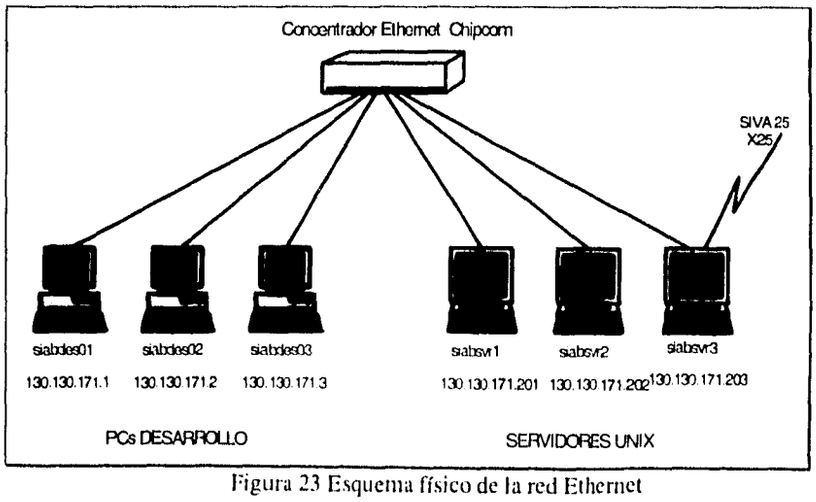

Figura 23 Esquema físico de la red Ethernet

Los servicios y aplicaciones que proporcionan los servidores Unix, son los siguientes:

Aplicaciones de bases de datos (Principalmente SQL)
Servicios de archivos e impresión
Ambiente gráfico XWindows
Comunicación TCP/IP
Comunicación X.25
Monitoreo de la red
Administración de la red
Servicios NIS

Las ventajas para los usuarios de este tipo de red local son:

Poder correr aplicaciones de DOS, aplicaciones gráficas XWindows y aplicaciones Unix en modo carácter.
Conectividad a una red Ethernet(Lan o Wan) donde se pueden conectar:
- Terminales tontas
- PCs
- Terminales X
- Workstations
- Mainframe

Heterogeneidad de marcas. Se pueden mezclar marcas diversas como son SUN, HP, IBM, DEC.

Simetría. Los clientes pueden correr aplicaciones de cualquier servidor y cualquier servidor puede ser también cliente.

Compartir recursos como: disco de gran capacidad, impresoras, dispositivos de lectura/escritura

Durante los últimos años, se ha visto un crecimiento muy fuerte en el uso de redes locales basadas en servidores Unix. Esta tendencia empezó con la introducción al mercado de las poderosas estaciones de trabajo basadas en la tecnología RISC. Los atributos de esta estación de trabajo hacen muy atractivo su uso como servidores en las redes locales, además de su tradicional orientación a aplicaciones gráficas (CAD/CAM) diseño publicitario, herramientas CASE, bases de datos.
Las características que comparten las distintas marcas de estaciones de trabajo son las siguientes:

1.- Procesador de 32 bits basado en tecnología RISC

Las worksations cuentan con un CPU de tecnología RISC que pueden proporcionar más de 70 MIPS (millones de instrucciones por segundo) y con memorias centrales de 16 a 512 Mb. Esta velocidad de proceso le permite correr aplicaciones de tipo gráfico (CAD-CAM), bases de datos, herramientas CASE, o bien mejorar muchos procesos simultáneos en modo multiusuarios.

2.- Pantallas gráficas

Todos los modelos de estaciones de trabajo cuentan con pantallas gráficas generalmente de color. Las imagenes manejadas son "bit-mapped", es decir, que lo que se ve en la pantalla es un reflejo de un arreglo de bits en la memoria principal, al modificar este arreglo, automáticamente se cambia la imagen correspondiente.

3.- Tarjetas Ethernet o Token Ring integradas.
Las estaciones de trabajo se diseñan para trabajar en red local. Tan es así que todos los modelos tienen integrada de fábrica la tarjeta de red Ethernet o Token Ring. El protocolo de comunicación más solicitado es el TCP/IP y su gran ventaja es la diversidad de distintas computadoras que lo soportan. Desde una PC con DOS hasta mainframes se pueden conectar en una misma red.

Las distintas marcas de estaciones de trabajo en el mercado tienen otro atributo que dan cierta compatibilidad, todas cuentan con sistema operativo Unix, y el sistema de ventanas XWindows. A través del sistema de ventanas XWindows, diferentes modelos de workstations pueden coexistir en la misma red local y compartir aplicaciones mutuamente. Con otro producto, NFS, una estación de trabajo en la red puede asociar el sistema de archivos de otra computadora y verlo como si fuera propio. Este producto permite ver a una red local como un sólo sistema de cómputo.

La posibilidad, de tener una aplicación corriendo en un equipo y el servidor X en otro, ha creado un nuevo concepto conocido como "grupo de trabajo", en este concepto, varias workstations de distintas marcas pueden estar conectadas en una red local y pueden contar cada uno con distintas aplicaciones. Cualquier usuario desde la red puede correr desde su equipo, cualquier aplicación que se encuentre en otro equipo, como si lo corriera en su propia computadora.

La interface Ethernet fue creada por Xerox (1970) y sus características más importantes es que es el estándar más estable, es versátil en distintos ambientes y su instalación no es compleja, sus principales especificaciones técnicas son, su velocidad de transmisión de información a través del medio de comunicación de 10 Mbits/seg, utiliza el protocolo de comunicación CSMA/CD, el número de nodos que se pueden conectar es de 1 a 1023, es posible utilizar los siguientes medios de comunicación dentro de la red basada en interfaces ethernet, cable coaxial grueso (Thick RG-11), coaxial delgado (Thin RG-58), par telefónico (Twisted Pair) y fibra óptica. Los fabricantes más importantes de interfaces ethernet se pueden resumir en los siguientes, 3 COM, EXCELAN, MICRON, NOVELL, GATEWAY, SMC e INTEL. Algunas variantes de interfaces para PCs son, tamaño del buffer de 8, 16, 40, 64 Kbytes, bus de 8, 16, 32 bits o microcanal, uso de DMA, tipo de procesador y generación de la interface

La entrada de las redes Ethernet en CBB fue empujada por el Proyecto de Análisis Bursátil, el cual tiene su origen en la plataforma Unix y las aplicaciones que corren sobre esta plataforma.
Las aplicaciones principales que marcaron la pauta para este diseño fueron; el software financiero en el tiempo real MIPS y la base de datos relacional SYBASE.
Por otro lado, el Ethernet se ha convertido en la interface preferida de los Sistemas Abiertos y son estos sistemas precisamente los que promueven al Sistema Operativo Unix.
Las Wokstations y los servidores Unix son nativos de la red Ethernet o IEEE 802.3 y del protocolo TCP/IP por lo que es muy fácil construir redes locales basadas en este tipo de equipos.

Como se muestra en la figura 24, la red está formada por tres Workstations HP 9000 modelo 720 y siete PCs Compaq 386 conectadas en un concentrador CHIPCOM, por medio de cableado UTP Systimax de AT & T.

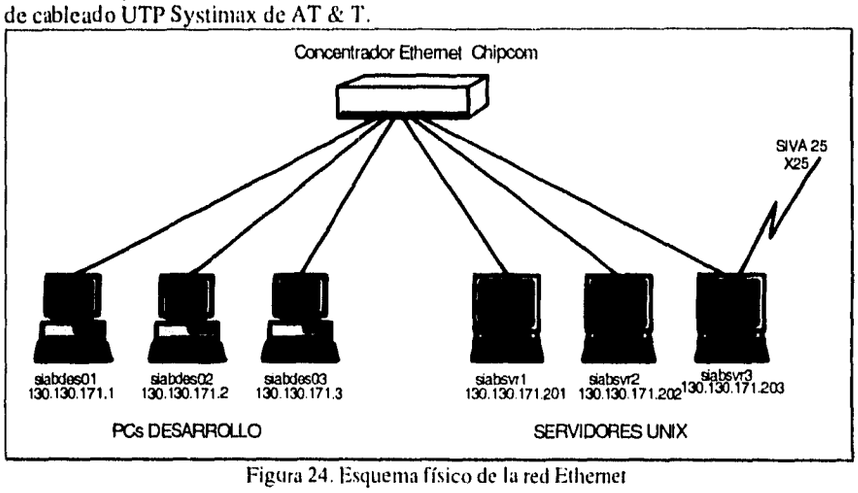

Figura 24. Esquema físico de la red Ethernet

Para conectar los equipos HP a la roseta RJ45 fue necesario incorporar un "transceiver" para cada una de las workstations. Este "transceiver" realiza la conversión de interface AUI ("thick wire") a interface UTP.

Las Pcs son conectadas a la red a través de la tarjeta Ethernet III 3C509-COMBO, la cual permite conectar tres diferentes tipos de interfaces (AUI, BNC y UTP), para conectarla directamente a la roseta.

Resulta costoso el proporcionar una Workstation a cada uno de los desarrolladores de aplicaciones para CBB bajo esta plataforma es por eso que fue necesario incorporar Pcs a estas redes de Ethernet con software TCP/IP (pc-Nfs) y de terminal Xwindows (En proceso de evaluación) para que estos Usuarios desarrollen las aplicaciones para CBB en la plataforma Unix desde su PC.

Los equipo HP funcionarán como servidores de información, uno de ellos será el servidor de comunicaciones que estará recibiendo la información del SIVA 25 de la Bolsa Mexicana de Valores, estos datos serán procesados por el software de MIPS.

La información procesada por el software MIPS es enviada al equipo HP, servidor de base de datos SYBASE.

Bajo este esquema, los usuarios podrán realizar consultas a la base de datos SYBASE desde sus nodos de trabajo a través del software de Open Client de Sybase y utilizando algún software de representación como el Excel Q+E o Power Builder.
Las Pc's de los usuarios de Análisis Bursátil se encuentran conectadas a la red TokenRing Novell, por lo que fue necesario integrar estas dos redes, dicha integración es descrita en las secciones "Integración de las redes Ethernet-TokenRing" y "Terminal Universal".

Las ventajas que representan este tipo de redes además de las comentadas en las redes Novell TokenRing, se tienen las siguientes:

Economía, ya que las interfaces y concentradores son mucho más barato que TokenRing.
Mayor flexibilidad en los servicios, con menor apilamiento en la memoria
Mayor flexibilidad en la integración con otras redes de igual o diferente topología y protocolos.
Soporte de servicios estándares como: E-mail, TCP/IP, NFS, SNMP, Xwindows.
Mayor número de aplicaciones: Bases de datos, financieras, administración.
Mayor flexibilidad de integrarse al mundo Unix.

4.7 INFOSEL

La incorporación del servicio de información de INFOSEL a las redes Token Ring de Novell se llevó a cabo instalando el receptor y el software de INFOSEL en uno de los nodos de la red. Este nodo a su vez se conectó al anillo que funciona como "backbone" o anillo de recursos. Con esto se eliminan altos costos de cableado coaxial y las posibilidades de falla al tener que instalar el receptor y el software en cada uno de los nodos de las redes.

En este esquema, cualquier usuario que se encuentre conectado en alguno de los anillos Token Ring podrán obtener el beneficio de los usos de servicio de INFOSEL con sólo adquirir la licencia de nodo adicional. El distribuidor del software lo que realiza, es instalar un terminador ("centinela") en el puerto paralelo de la PC y registra un nodo más.

Ahora resulta más fácil incorporar nuevos nodos INFOSEL y también se facilita la actualización del software realizando esta en un solo nodo de la red ahorrando trabajo a los administradores. El servidor que administra este servicio es un nodo dedicado en el anillo de recursos, por lo que reside en el Centro de Cómputo junto a los demás servidores y equipos de comunicaciones.

4.8 INTEGRACION DE LAS REDES CON EL SISTEMA AS/400

La integración de las redes locales con el sistema AS/400 será llevado a cabo a través de la incorporación de un dispositivo de red llamado GATEWAY, donde este, es la solución para comunicar redes locales a recursos remotos (mainframe, minicomputadoras ,bases de datos, otras redes locales, servicios de información). La conexión por lo general es transparente para el usuario final. La función de gateway es proporcionar a los usuarios conectados a una red local el acceso a un mainframe o minicomputador por medio de la emulación de terminales. Un genero de gateway permite accesar equipos IBM (AS/400) con protocolos SNA. En los equipos IBM se aplica el concepto System Network Arquitecture (SNA, Arquitectura para sistemas de red), para accesar redes locales, esto se logra a través de un gateway 3270 o 5250 (que depende del modelo de mainframe o minicomputador) y Advanced Program to Program Communication (APPC, Comunicación avanzada programa a programa), la arquitectura de IBM para el proceso de transacciones distribuidas. Este tipo de gateway elimina la necesidad de tener una sola línea dedicada para cada PC de la red local. Por el contrario, permite que por medio de una sola línea cualquier usuario de la red local se comunique con el mainframe o minicomputador. El gateway, tendrá la función de convertir las capas del protocolo Novel IPX a las capas del protocolo Token-Ring del AS/400 y viceversa, permitiendo así, que los usuarios puedan abrir sesiones del sistema AS/400 desde un ambiente de trabajo Windows.

Existen en el mercado gateways que se incorporan a las PCs mediante una tarjeta que se coloca en algún puerto disponible, además la PC está conectada a la red Token-Ring mediante la interface de red. En la figura 25 se muestra como están dispuestos los elementos antes descritos que nos permiten la integración de la red local con el equipo AS/400.

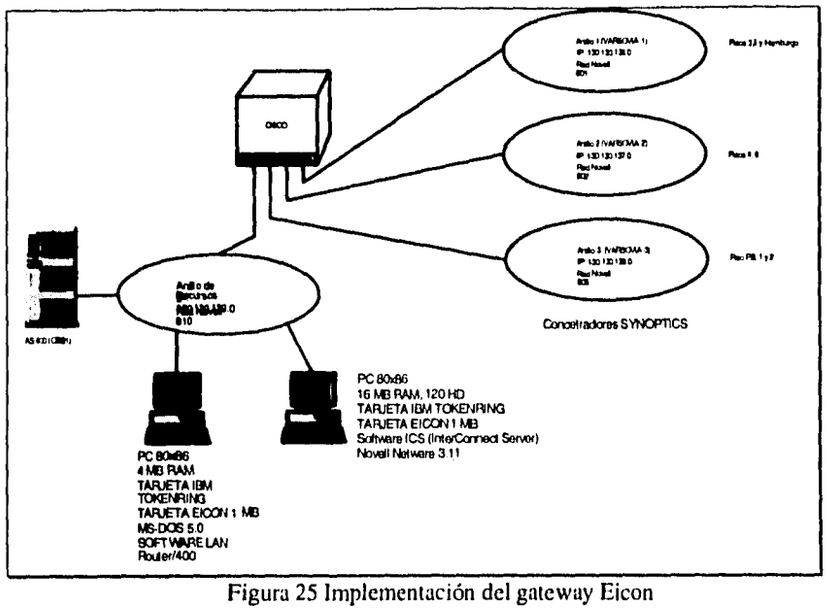

Figura 25 Implementación del gateway Eicon

Existe en el mercado un gateway que realiza las funciones antes mencionadas llamado EICON, éste dispositivo fué diseñado por EICON especificamente para dar una solución de conectividad de una red local con el equipo AS/400 utilizando como programa de emulación el software PC Support de IBM. Este gateway soporta el enlace X.25, SDLC y Token Ring, siendo este último la forma en que se configuró para esta solución.

Además del gateway EICON y el PC-Support es necesario instalar en la PC el software LAN Router/400 lo que en conjunto nos da una solución a la integración de redes locales con sistema AS/400.

El software y hardware instalados en un nodo de la red Token-Ring permitirán que este funcione como una compuerta dedicada a proporcionar acceso al sistema AS/400.

El gateway EICON físicamente es una tarjeta que se instalara en un computadora Compaq 386, la cual se recomienda para que atienda 32 sesiones AS/400 de usuarios de red. Se pueden instalar hasta 4 tarjetas EICON en una misma PC, para soportar 128 sesiones concurrentes en el sistema AS/400

Esta tarjeta junto con el software LAN Router/400 son los que ejecutan la conversión del protocolo IPX de la red Novell al protocolo Token Ring

El PC-Support (soporte de la PC) del AS/400 es un conjunto integrado de aplicaciones (software) fáciles de usar tanto para la PC como para el AS/400, este elemento permite

desempeñar funciones del AS/400 desde una PC (emulando una terminal IBM 5250), además de permitir a la PC utilizar espacio en disco del sistema AS/400, impresoras y la comunicación con otros usuarios.

Además de la tarjeta EICON, la PC debe tener instalada una tarjeta Token-Ring IBM que se conecta al anillo de soporte , que es un concentrador Synoptics, en el que también están conectadas las interfaces Token Ring del enrutador Varsovia, el cual además funciona como bridge (puente) entre las redes Novell Token Ring, por último también este anillo se encuentra conectado al AS/400.

Además de instalar y configurar el gateway AS/400, es necesario también instalar y configurar la parte correspondiente del LAN Router/400 y PC-Support en cada uno de los nodos que tienen la necesidad de accesar los servicios del AS/400.

En el ambiente Windows de las PC conectadas como nodos de la red se incorporara un icono más en la ventana de "Aplicaciones de la Red" para accesar los servicios del AS/400. Bajo este ambiente, el usuario solo seleccionara dicho icono para abrir una ventana al sistema AS/400 y aprovechar los beneficios de estar en un ambiente Windows.

La integración de las redes Token Ring con el sistema AS/400 es el primer paso para llegar al diseño de lo que hemos llamado la terminal universal.

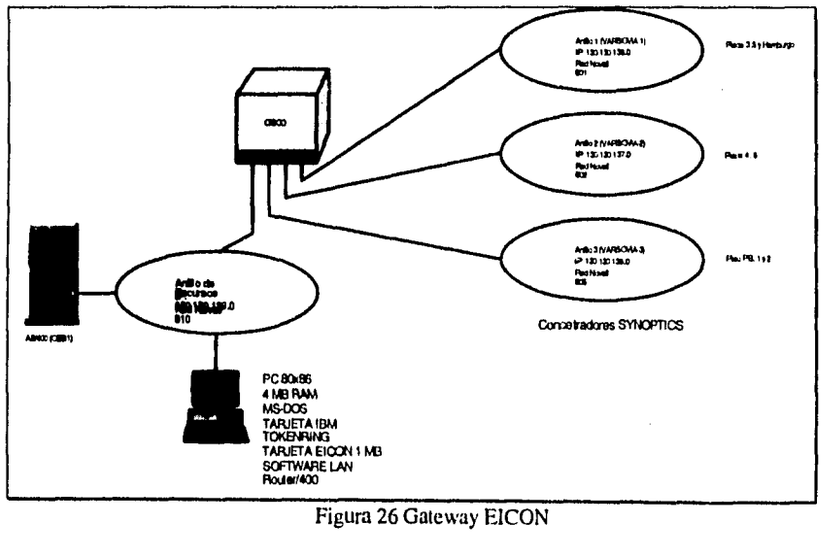

Figura 26 Gateway EICON

4.9 CONECTIVIDAD ENTRE REDES TOKEN-RING Y ETHERNET

El planteamiento consiste en el transporte local de paquetes de diferentes protocolos a través de redes locales Ethernet y Token Ring. Cuando se trata de protocolos enrutables como

TCP/IP y Novell IPX, este transporte se vuelve transparente utilizando los enrutadores CISCO para llevar a cabo el transporte entre los dos medios.

La integración de las redes de tecnología Ethernet con las redes de tecnología TokenRing es posible con la incorporación de los dispositivos de comunicación llamados enrutadores y/o puentes.

Las redes de área local se comunican a tráves de bridges. Los Bridges son una forma bastante inteligente de dirigir los paquetes de datos a los nodos de una red. Novell utiliza el IPX como protocolo común para conectar las redes del bridge. Cuando se coloca un bridge, un distribuidor (router) situado en el servidor o estación de trabajo donde está el bridge lleva a cabo las funciones de encaminamiento. Se mantiene una tabla con todas las direcciones conocidas de la red, usando esta tabla para encaminar los paquetes a su destino apropiado. Si existen varios caminos hasta un nodo, los routers de NetWare son capaces de determinar el camino más rápido. También se realiza un seguimiento de los distintos caminos, de forma que se usen los caminos alternativos si el camino principal deja de funcionar.

En general, los bridges de NetWare ofrecen un elevado rendimiento, debido a sus técnicas de filtrado y de encaminamiento de paquetes, de forma que es posible ampliar las redes con muy pocos problemas.

Los enrutadores del sistema CISCO (CISCO SYSTEMS) son multiprotocolos de red de computadoras que proveen todas las funciones de un "puente externo" de Novell más un número de locales adicionales y un área ancha de capacidad de conexión (Novell se refiere a sus enrutadores ya sean puentes "externos" o "internos", dependiendo de donde se origine la capacidad para enrutear ya sea dentro o fuera). Un bridge realizado en el servidor se denomina bridge interno. Un bridge que se situa en una estación de trabajo se denomina bridge externo. Los enrutadores CISCO incluyen la capacidad para conectar multiples Ethernets, Token-Rings y redes FDDI (Fiber Distrubuted Data Interface), ya sea directamente o a tráves de líneas seriadas de alta velocidad o X.25.
Se ha mencionado que, la red TokenRing de CBB fue concebida como solución en las integración del ambiente de oficina y correo electrónico. También se mencionó que las redes Ethernet de CBB se iniciaron con el proyecto de las aplicaciones de la Dirección de Análisis.

CBB contará con una red corporativa construida con un "backbone" de enrutadores CISCO para el transporte común de datos que utilizan diferentes protocolos de las redes Ethernet, TokenRing y las terminales AS/400.

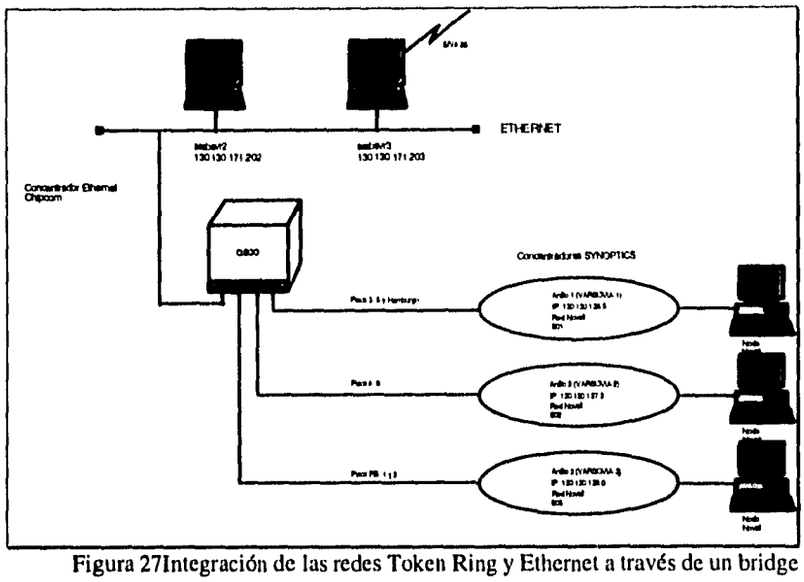

Figura 27Integración de las redes Token Ring y Ethernet a través de un bridge

4.10 DISEÑO DE LA TERMINAL UNIVERSAL

El concepto de Terminal Universal se refiere a la integración en una estación de trabajo, de los tres ambientes tecnológicos de CBB (Novell, Unix y AS/400), en otras palabras, lograr la interoperabilidad entre los diferentes equipos de cómputo, definiendo interoperabilidad como la habilidad de comunicar exitosamente computadoras de diferentes proveedores sobre una red. Esto es, permitir que los usuarios puedan abrir sesiones (ventanas) de los diferentes ambientes operativos de CBB en su computadora personal, a través de una interfase gráfica estándar (MS-Windows).

Por ejemplo, cuando un usuario de la red enciende su computadora personal, normalmente entra al ambiente gráfico de MS-Windows y podría iniciar una sesión de trabajo con el procesador de textos Word, estando en Word y sin cerrar el documento, podría abrir una sesion del sistema AS/400, disparando el icono correspondiente. Ademas también podría conectarse a cualquiera de los sistemas Unix y correr aplicaciones planas con el protocolo de emulación de terminal Telnet y/o aplicaciones gráficas con Telnet bajo ambiente Xwindows.

Esto convierte a la computadora personal en una Terminal Universal (Ver figura 28), ya que permite la integración y conmutación indistinta de los tres servicios corporativos de información como son :

- Software de oficina
- Aplicaciones del Sistema AS/400
- Aplicaciones de la plataforma Unix

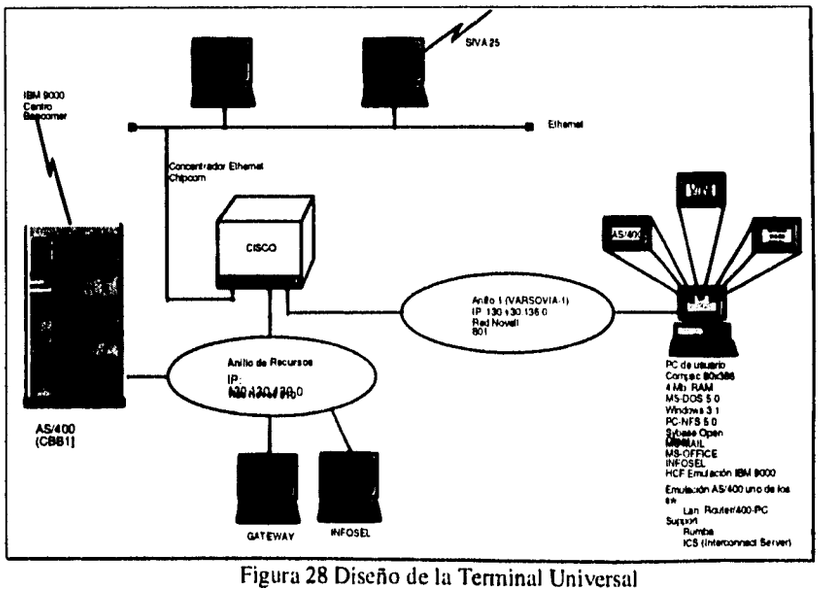

Figura 28 Diseño de la Terminal Universal

Las ventajas principales de esta solución son la reducción en los costos, ya que solo se requiere de una terminal en vez de tres, la versatilidad en la operación y el aprovechamiento de las inversiones previas.

La interoperabildad entre las distintas plataformas se explica en las siguientes secciones.

4.10.1 INTEROPERABILIDAD NOVELL-UNIX

Como se mencionó anteriormente la integración entre Token Ring y Ethernet se logra a través del uso de enrutadores CISCO como se muestra En la figura 11.
En esta integración, el enrutador CISCO juega un papel muy importante, ya que es el dispositivo que maneja el tráfico de paquetes TCP/IP a través de los anillos Token Ring y de los segmentos Ethernet.
Los servicios que corren en la plataforma Novell básicamente son el software para oficina Microsoft Office que incluye Windows, Word, Excel, PowerPoint y el correo electrónico MS-Mail.
Para accesar las aplicaciones de la plataforma Unix, como por ejemplo las del área de Análisis Bursátil, es necesario lograr la interoperabilidad entre estas dos plataformas.
Se llevó a cabo un proceso de evaluación y selección de los elementos que conforman esta solución. La siguiente figura muestra como están interconectados estos elementos, que en resumen consisten de lo siguiente:

- Tarjetas Token Ring PROTEON 1392
- Concentradores Token Ring SYNOPTICS
- Protocolo Novell IPX
- Protocolo TCP/IP (PC/NFS 5.0)
- Emulador de terminal Xwindows
- Open Client de SYBASE
- Enrutador CISCO AGS+, como "brigde" entre las dos redes

Integrando todos estos elementos se logra un paso hacia lo que es el modelo de la Terminal Universal. Hasta el momento tenemos servicios de oficina (Novell) y Unix, como se muestra en la figura 29.

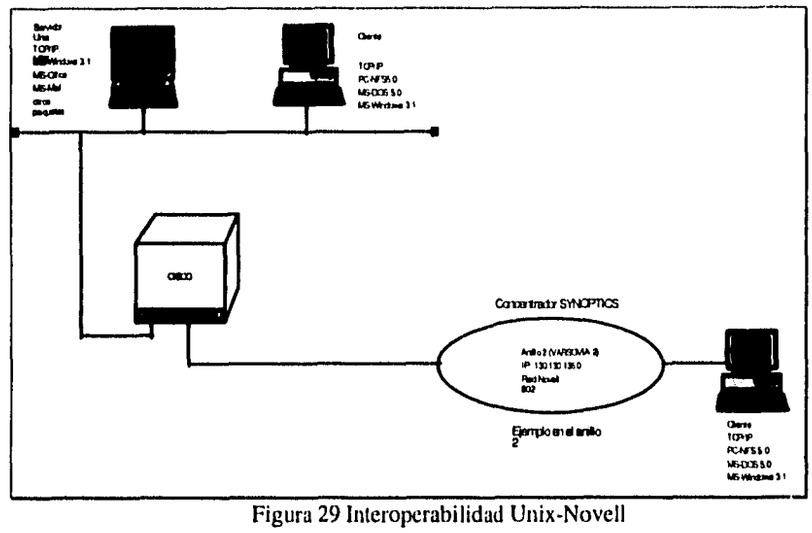

Figura 29 Interoperabilidad Unix-Novell

Entre las aplicaciones que residirán en los servidores Unix se encuentran las siguientes:

- El software MIPS
- La base de datos SYBASE
- El software INFOTRADE

En las computadoras personales que servirán como Terminales Universales se instalará y configurará el software del cliente necesario para accesar las aplicaciones de los servidores Unix. Por ejemplo el Open Client para accesar SYBASE.
La información detallada de la configuración de los nodos Novell con el protocolo PC-NFS 5.0 se encuentra en el apéndice E.
La interfase gráfica de usuarios seguirá siendo MS-Windows, y entre las herramientas para el acceso a la información de los servidores Unix, se encuentran las siguientes:

- Q+E de Excel
- Infotec(INFOTRADE para PC)
- Power Builder

Se podrán incorporar en un futuro aplicaciones que corran bajo XWindows/Motif, que se requieran ejecutar en las computadoras personales de las red. Para esto será necesario instalar y configurar el software de XWindows/Motif, además de TCP/IP en cada una de las computadoras personales.
La computadora personal trabaja en el esquema cliente-servidor como terminal X, debido a su característica de "mono-tarea", el proceso se ejecuta en el sistema Unix asociado

mediante Telnet , y el despliegue gráfico se redirecciona al monitor de la computadora personal, ejecutando el proceso remoto fuera de línea (background).
Esta solución permite utilizar la computadora personal para correr aplicaciones de la plataforma Unix, obteniendo la misma funcionalidad que la de una Workstation Unix conectada directamente en la red Ethernet. Sin embargo habrá que realizar las pruebas necesarias con las aplicaciones Unix que serán desplegadas en la PC.

4.10.2 INTEROPERABILIDAD UNIX-NOVELL

Entre las aplicaciones que correrán en la plataforma Unix, se encuentran Análisis Bursátil, Mercado de Dinero y Mercado de Capitales, entre otras.
Para que los usuarios de la red Ethernet Unix accesen aplicaciones de oficina como el MS-Office y el MS-Mail, es necesario lograr la interoperabilidad entre estas dos plataformas.
Se llevó a cabo un proceso de evaluación y selección de los elementos que conforman esta solución, a continuación se mencionan:

- Tarjetas Ethernet EtherLink III 3C509-COMBO
- Concentradores Ethernet CHIPCOM
- Protocolo TCP/IP (PC/NFS 5.0)
- Protocolo Novell IPX
- Emulador de terminal XWindows
- Open Client de SYBASE
- Enrutador CISCO AGS+, como bridge entre las dos redes

El enrutador CISCO AGS+ hará posible esta integración ya que siendo un dispositivo de enrutamiento, puede controlar y enrutar los paquetes de los protocolos IPX y TCP/IP de las redes Novell y Unix respectivamente.

La segunda alternativa consiste en utilizar como servidor de archivos y aplicaciones a los servidores Unix, entregando la misma solución de oficina de Novell pero con la ventaja de que es un ambiente más abierto que permite incorporarse a otras redes abiertas de una manera transparente para los usuarios.

Esta solución es las mas recomendable para seguir en futuras implementaciones e integración de redes locales. Incluye los elementos listados anteriormente, excepto el protocolo Novell IPX.

Entre las aplicaciones que residirán en los servidores Unix se encuentran las siguientes:

- El software MIPS
- La base de datos SYBASE
- El software INFOTRADE

En las computadoras personales que servirán como Terminales Universales se instalará y configurará el software del cliente necesario para interactuar con las aplicaciones de los servidores Unix. Por ejemplo el Open Client para accesar SYBASE.
La interfase gráfica de usuarios seguirá siendo MS-Windows, y entre las herramientas para el acceso a la información de los servidores Unix, se encuentran las siguientes:

- Q+E de Excel
- Infotec(INFOTRADE para PC)
- Power Builder

Se podrán incorporar en un futuro aplicaciones que corran bajo XWindows/Motif, que se requieran ejecutar en las computadoras personales de las red. Para esto será necesario instalar y configurar el software de XWindows/Motif, además de TCP/IP en cada una de las computadoras personales.
La computadora personal trabaja en el esquema cliente-servidor como terminal X, debido a su característica de "mono-tarea", el proceso se ejecuta en el sistema Unix asociado mediante Telnet , y el despliegue gráfico se redirecciona al monitor de la computadora personal, ejecutando el proceso remoto fuera de línea (background).
Esta solución permite utilizar la computadora personal para correr aplicaciones de la plataforma Unix, obteniendo la misma funcionalidad que la de una Workstation Unix conectada directamente en la red Ethernet. Sin embargo habrá que realizar las pruebas necesarias con las aplicaciones Unix que serán desplegadas en la PC.

4.10.3 CONCLUSIONES DE LA TERMINAL UNIVERSAL

De acuerdo a los puntos anteriores, las pruebas realizadas exitosamente indican que el modelo de la Terminal Universal es una realidad que en estos momentos los usuarios de CBB pueden aprovechar. A continuación se mencionan las ventajas mas importantes de este modelo.

- Permite a los usuarios el acceso a las tres diferentes plataformas tecnológicas (Novell, Unix, y AS/400), desde el ambiente gráfico MS-Windows, como se ilustra en la figura 10.
  a) *Novell:* Bajo esta plataforma, los usuarios pueden ejectutar las aplicaciones de oficina como Word, Excel, PowerPoint y correo electrónico.
  b) *Unix:* Bajo esta plataforma los usuarios pueden accesar los equipos Unix a través del protocolo Telnet y correr las aplicaciones Unix. También se podrían utilizar estos equipos como servidores de archivos y aplicaciones MS-DOS.
  c) *AS/400:* Bajo esta plataforma, los usuarios pueden accesar el Sistema AS/400 en una ventana, como si estuvieran trabajando en una terminal IBM 5250, con las facilidades adicionales que proporciona el ambiente Windows ("cut and paste").
- Permite establecer un ambiente gráfico de trabajo estándar entre todos los usuarios.
- Elimina la necesidad de que los usuarios tengan más de una terminal en su lugar de trabajo
- Optimiza recursos
- Aumenta la productividad de los usuarios, ya que éstos pueden tener abiertas diferentes ventanas de aplicaciones (Telnet, AS/400, Excel, etc.) y estar interactuando con cada una de ellas .
- Utilización de software de vanguardia que permite la integración de aplicaciones.
- Con el uso de la Terminal Universal se hace realidad el dicho utilizado por los sistemas abiertos que dice, "La red es la computadora".

5.8 RED LOCAL DE UNA SUCURSAL

En la figura 30 se muestra el esquema de la red local de una sucursal de CBB, podemos observar que esta basada en una red Novell Token Ring y un enrutador CISCO además de la instalación y configuración del software de red y oficina.

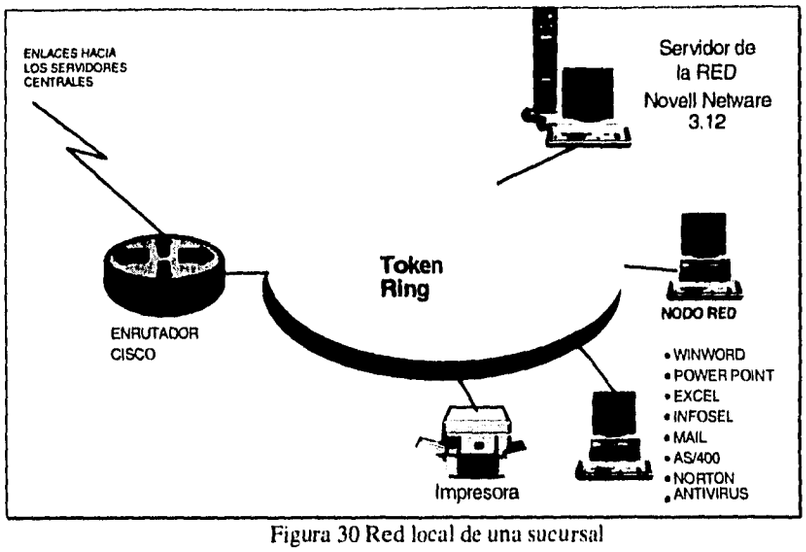

Figura 30 Red local de una sucursal

El diseño de la red local Novell Token Ring es similar a las redes Novell diseñadas para los edificios Varsovia y Hamburgo, es decir que también se utiliza tanto el cableado modular y estructurado SYSTIMAX de AT&T y la siguiente configuración de hardware y software.

Hardware

- Cableado UTP 1061
- Computadoras Compaq 386
- Concentradores Token Ring SYNOPTICS
- Tarjetas Token Ring PROTEON 1392
- Enrutador CISCO dimensionado de acuerdo al tipo de sucursal

Software

- MS-DOS 5.0
- MS-Windows 3.1
- Novell NetWare 3.11
- Lan Router/400 (la parte cliente)
- PC Support
- MS-Office
  - Word 2.0
  - Excel 4.0
  - PowerPoint
- **MS-Mail**

- PC-NFS 5.0 (*)
- Sybase Open Client (*)
- Infotec INFOTRADE (*)

(*) Solo usuarios que lo requieran

RED DE AREA AMPLIA (WAN)

RED DE AREA AMPLIA (WAN)

A través de la interconexión de redes (internetworking) se logra integrar los diferentes tipos de redes locales (LAN's), redes de área amplia (WAN's), sistemas de cómputo, software y dispositivos de comunicaciones relacionados para formar una infraestructura de comunicaciones evolutiva. Las compañías y organizaciones, que confían en el rápido y eficiente flujo de información como un activo estrategico, utilizan redes corporativas para incrementar la productividad y proveer a su organización de ventajas competitivas en un mercado global.

4.12 SITUACION PREVIA DE LA RED CBB

La figura 31 muestra el esquema anterior de la red de comunicaciones de CBB, formada principalmente por equipos AS/400 y terminales conectadas localmente con el protocolo TDLC de IBM y remotamente por medio de controladores 5394 y el protocolo SDLC.

Los sistemas AS/400 interconectados en un solo anillo local, se encontraban operando bajo un mecanismo espejo de manera que las transacciones realizadas en un sistema se reflejaban en el otro y que a través de los procesos nocturnos, por las mañanas las bases de datos de los dos sistemas AS/400 iniciaban iguales.

El mecanismo espejo será aprovechado cuando ocurra una caída de alguno de los Sistemas AS/400 y no se restableciera el servicio rápidamente. Entonces se realizaba un cambio manual de los controladores de terminales para que los usuarios críticos fueran atendidos por el otro sistema, restableciendo el servicio en cinco minutos.

Como se ha mencionado, los usuarios se encontraban trabajando en un ambiente cerrado al utilizar terminales tontas y no se tenían aplicaciones de oficina en un ambiente estándar de red. Si los usuarios utilizaban algún paquete de oficina necesitaban tener sobre su escritorio una PC aislada además de su terminal IBM para accesar el AS/400.

Existía el riesgo de tener las dos AS/400 en un mismo "site" y ocurriera algún siniestro como: temblores, incendios, sabotaje; el cableado era demasiado inflexible en los cambios de servicio, no existía integración de PCs, no se compartían recursos de software y hardware, y la infraestructura de comunicaciones estaba basada en la tecnología propietaria de IBM por lo que era muy difícil integrarla con otras tecnologías.

Por todo lo anterior, el diseño de la red amplia se llevó a cabo bajo un ambiente que cubriera todas las debilidades del esquema anterior y que la red de comunicaciones de CBB fuera posicionada en un esquema abierto de vanguardia tecnológica.

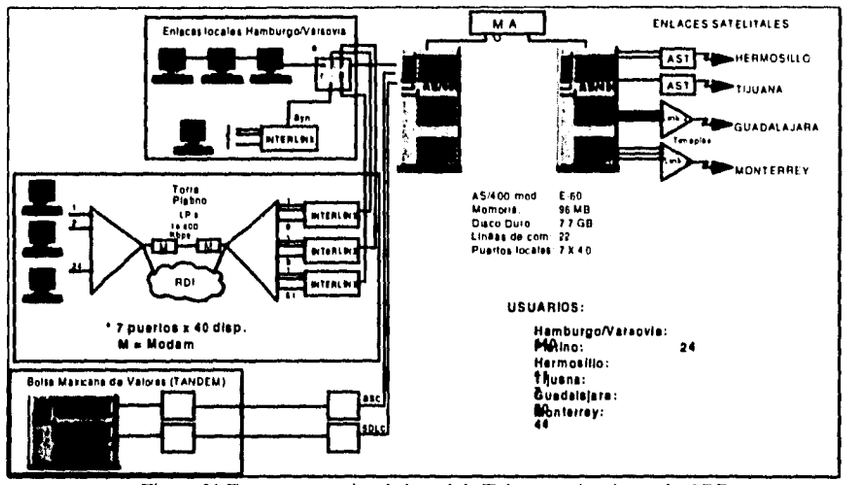

Figura 31 Esquema anterior de la red de Telecomunicaciones de CBB

4.13 DISEÑO DE LA RED WAN BASADA EN ENRUTADORES

La interconexión de redes de área local (LAN), formando lo que es llamado redes inter-LAN, se ha llegado a convertir en un elemento clave en la planeación y diseño de redes en diversas corporaciones. Las redes inter-LAN pueden ser construídas directamente a partir de la interconexión de varias LANs por medio de puentes, enrutadores o gateways, dependiendo de que tan similares son las redes en los diversos niveles. Por ejemplo, dos redes token ring pueden ser interconectadas por medio de un puente que sea una estación en ambas redes.

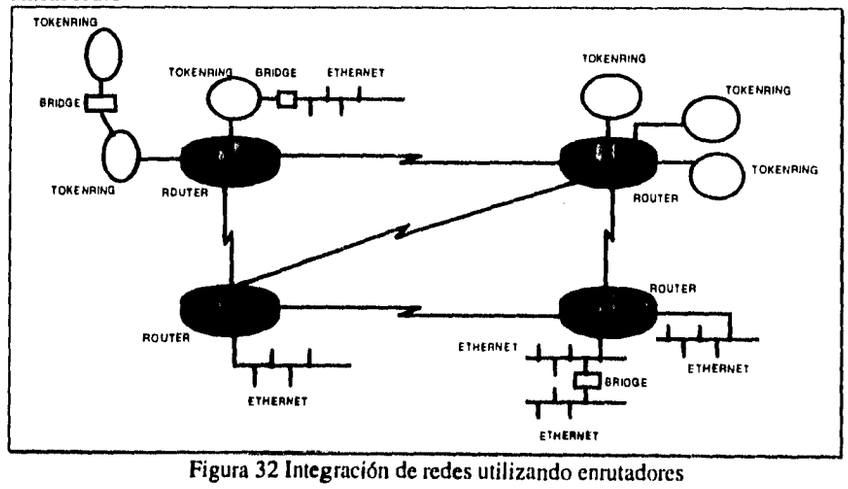

Figura 32 Integración de redes utilizando enrutadores

Otro enfoque que puede ser utilizado con las redes inter-LAN es el de emplear una red como columna vertebral, mejor conocida como *backbone*. Un backbone es una red central a la que son conectadas otras redes. Los usuarios no son conectados directamente al backbone sino, a las redes de acceso, las que a su vez son conectadas al backbone. Las redes no necesitan ser del mismo tipo para conectarse a un backbone, por ejemplo una red FDDI la cual corre a través de todo un edificio puede ser utilizada para interconectar diferentes LANs en cada piso o en el mismo departamento.

El uso de un backbone para atar varias redes de acceso pequeñas, ofrece varias ventajas sobre la opción de tener una LAN de gran tamaño. Las diferentes LAN conectadas al backbone son capaces de operar en paralelo, proporcionando mayor eficiencia de procesamiento. El enfoque de manejar múltiples redes en una estructura es más confiable, dado que cada LAN individual puede seguir operando si alguna de las otras falla. El backbone típicamente filtra el tráfico y transmite sólo aquellos mensajes destinados a una LAN diferente. Las diferentes redes pueden ser optimizadas para satisfacer diversos requerimientos. Un backbone normalmente requiere un ancho de banda alto y la habilidad para transmitir a través de distancias considerables, dado que puede ser usado para interconectar redes en un edificio o desde un edificio hacia otros ubicados a gran distancia. Un backbone debe ser también altamente confiable, dado que las grandes distancias cubiertas pueden hacer difícil el localizar y reparar las fallas. Las LAN que se conecten al backbone deben ser flexibles y de bajo costo en cuanto a instalación y a conexión de los usuarios.

Debido al requerimiento de un alto ancho de banda para transmisiones sobre distancias largas, el uso de enlaces de fibra óptica y de microondas son particularmente convenientes para formar el backbone. El hecho de que los costos de instalación y conexión sean más altos es menos importante, dado que el backbone es menos susceptible a sufrir una reconfiguración o a que se realicen cambios importantes en cuanto al número de equipos conectados directamente a él.

La conexión al backbone puede requerir de un puente, un enrutador, o de un gateway, dependiendo de las arquitecturas de las diversas LANs y del mismo backbone. Como es nuestro caso, el concepto de backbone puede ser utilizado en el nivel empresarial donde se requiere una WAN; posiblemente con enfoque internacional, sea usada para interconectar varias redes en diferentes ciudades a lo largo del país o en el extranjero.

En las últimas décadas, el ambiente de redes amplias había sido diseñado, desarrollado e implementado con soluciones de proveedores de arquitecturas propietarias con muy poca cooperación entre ellos. Las redes que habían surgido tenían muchas diferencias en cuanto a arquitecturas, topologías y protocolos de comunicaciones, hasta que a mediados de la década de los 80's surgió la necesidad de interconectar redes con diferentes características.

La integración exitosa de un ambiente de redes "multiproveedor" no es una tarea fácil, tradicionalmente las corporaciones enriquecen sus redes incorporando tecnologías que van apareciendo. Esto es relativamente sencillo cuando se trata de un sólo proveedor. Sin

embargo, la evolución tecnológica y la estrategia de cambios tecnológicos indican que no se debe depender de un sólo proveedor y que se debe seguir el camino de los sistemas abiertos.

Cuando hablamos de la conexión de dos o más redes, a la comunicación o al trabajo que se desarrolla entre estas se le conoce con el término de "internetworking", dado que el propósito de su unión es el mover información de una subred (una red conectada al backbone) a otra subred. El término segmento es utilizado para referirse a una pieza específica de la red, por ejemplo:

En el caso de una LAN, segmento podría ser un bus, una estación, etc.
Si hablamos de una WAN, puede referirse por ejemplo a un enlace de transmisión.

El "internetworking" puede darse entre dos redes de cualquier tipo, por ejemplo:

Dos LANs del mismo tipo (por ejemplo, dos Token Ring)
Dos LANs de diferente tipo (por ejemplo una Token Ring y otra CSMA/CD)
Dos LANs remotas unidas por un enlace WAN
Una LAN y WAN con otras WANs
Diferentes nodos de una WAN

Para interconectar segmentos de una red, existen tres tipos de dispositivos de interconexión:

"Bridges" (puentes)
"Routers" (enrutadores)
"Gateways"

Los anteriores elementos ya fueron mencionados en el capítulo 3. En la figura 33 se muestra el backbone de enrutadores de Casa de Bolsa de Banconer.

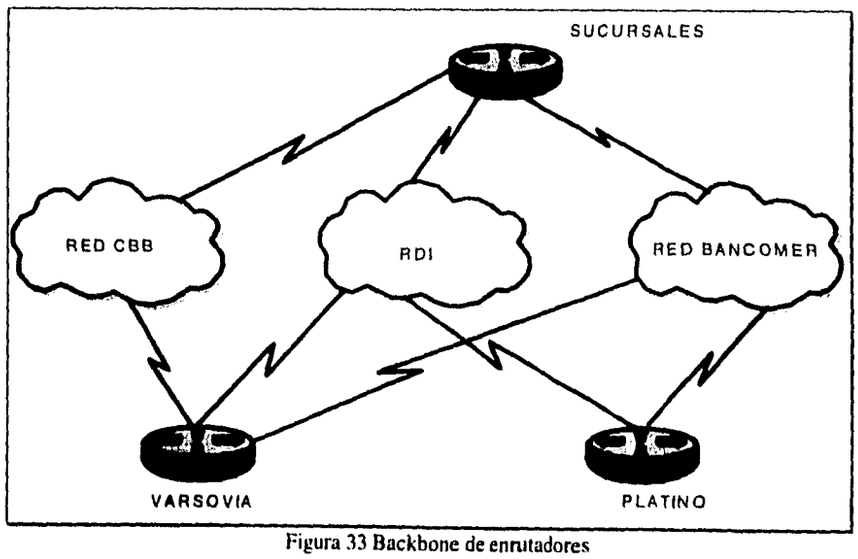

Figura 33 Backbone de enrutadores

En la figura 34 se muestra como se utilizan los enrutadores aprovechando la infraestructura de la red de Casa de Bolsa Bancomer.

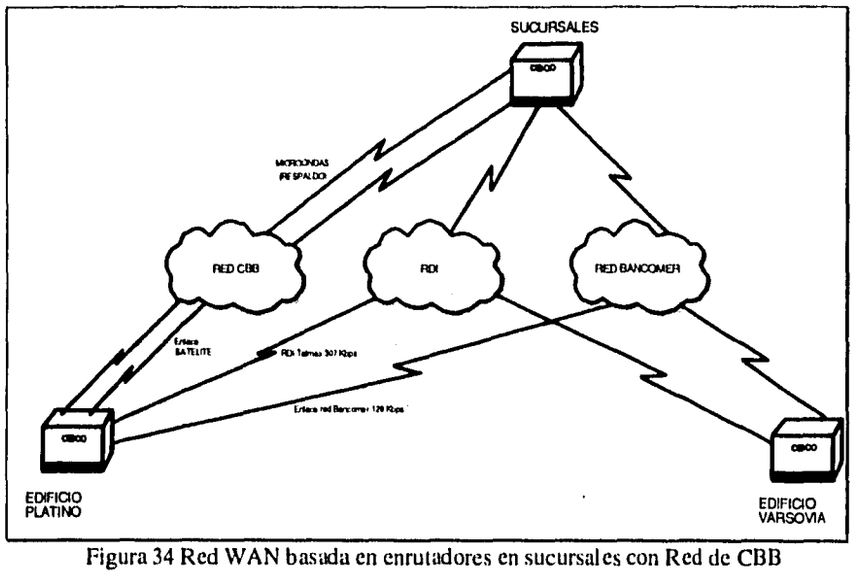

Figura 34 Red WAN basada en enrutadores en sucursales con Red de CBB

Las técnicas de ruteo permiten segmentar lógicamente diferentes tipos de redes, dejando pasar únicamente el tráfico cuyo destino sea una subred diferente eligiendo la mejor ruta de acuerdo a diversos factores. Las características principales del enrutador AGS+ de la compañía Cisco Systems Inc. Se detallan en el apéndice B, dado que es el corazón de este trabajo de tesis.

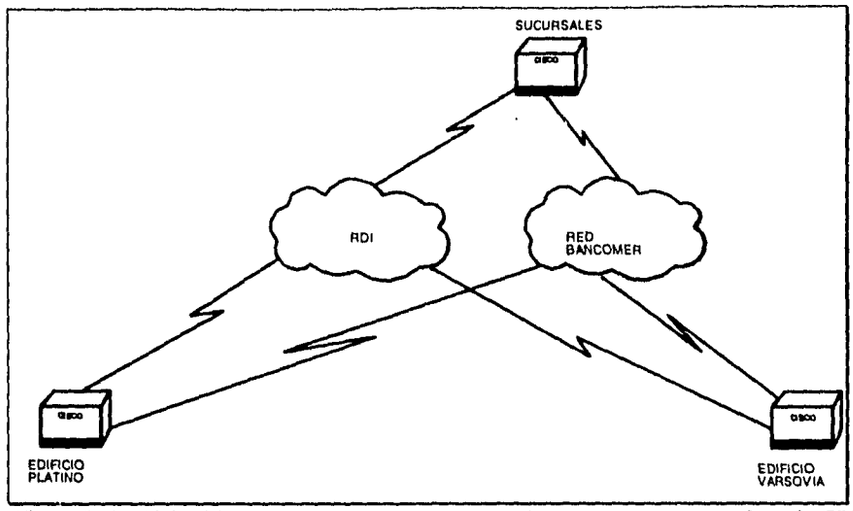

Figura 35 Red WAN basada en enrutadores en sucursales que no cuentan con Red de CBB

4.14 COMUNICACION ESPEJO REMOTO AS/400 VARSOVIA-PLATINO

La separación en edificios distantes de los equipos AS/400, es producto de la estrategia de CBB, la cual permitirá garantizar la operación y la seguridad de la información de los sistemas en producción, ofreciendo un sistema de respaldo.

Anteriormente el software espejo estaba implementado en los dos sistemas AS/400, los cuales estaban conectados físicamente en un mismo anillo dentro del centro de cómputo del edificio de Varsovia.

El planteamiento era el formar un anillo virtual entre los edificios Varsovia y Platino, los dispositivos de interconexión que hicieron posible implementar el anillo virtual entre ambos edificios y que el software espejo corriera en forma transparente, fueron los enrutadores Cisco.

La configuración en SRB en los enrutadores es la que nos permite tener el anillo virtual y que permite que el software espejo corra de igual forma como la hacía en el mismo anillo del centro de cómputo. En el apéndice A se presenta la configuración del enrutador de Varsovia.

En el enrutador de Varsovia también se conectan los controladores de terminales tontas IBM 5250, para dar servicio a los usuarios que todavía utilicen este tipo de terminales tanto en el edificio de Platino como en Varsovia. Estos controladores localizados en el edificio Varsovia, siempre están conectados al CPU alterno del equipo (CBB2) proporcionando servicio en operación normal a ingenieros de sistemas y usuarios del sistema de Nómina. En

situación de contingencia (falla del CPU primario, CBB1), estos controladores proporcionaran servicio a terminales críticas de los edificios Hamburgo y Varsovia.

4.15 COMUNICACIONES CON LAS SUCURSALES

Las redes locales de las sucursales serán integradas a la red CBB por medio de los enrutadores AGS+, el enlace primario deberá ser la red Bancomer y como canal alterno se recomienda que se utilicen enlaces RDI de Telmex como parte de la infraestructura de CBB y como tercer alternativa se utilizará un enlace de microondas ya existente.

Para el caso de las sucursales que ya contaban con enlaces de microondas y satélite, estos se deberían seguir utilizando como canales alternos y como parte de la infraestructura propia de CBB.

En la figura 36 se muestra el esquema de los casos, también se mencionó anteriormente que el ancho de banda para las sucursales dependerá del tipo de sucursal y de las aplicaciones que se vayan a incorporar a CBB y que para un ambiente cliente servidor mínimo debería de existir un ancho de banda de 64 kbps.

Con esta integración, los usuarios de las sucursales estan en posibilidades de utilizar los servicios de la red, tal y como lo hacen los usuarios de la red local de Hamburgo y Varsovia, es decir, podrán hacer uso de las aplicaciones de oficina, así como de la AS/400 y Unix. Como se explicó en la sección de la Terminal Universal.

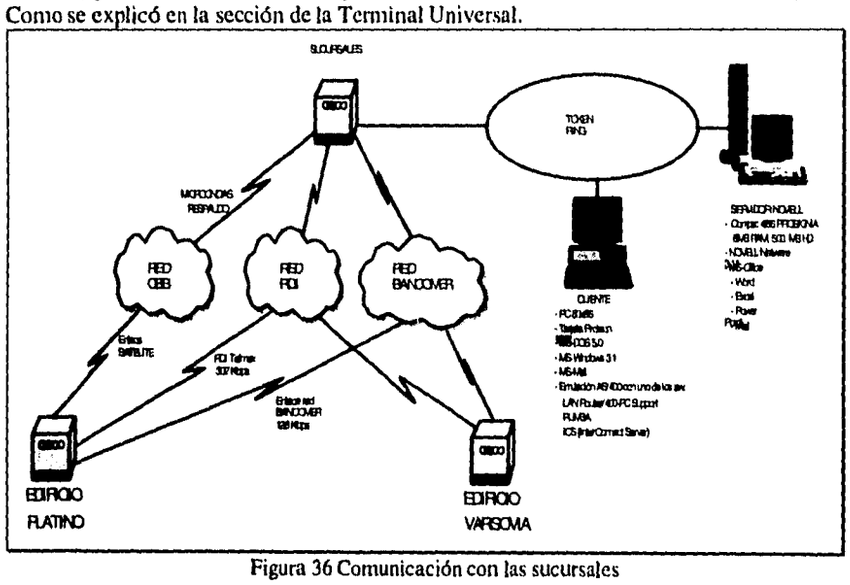

Figura 36 Comunicación con las sucursales

5. ADMINISTRACION DE LA RED

5. ADMINISTRACION DE LA RED

El uso de las redes dentro de las organizaciones y las aplicaciones que soportan crecen en escala y complejidad, de tal manera, la administración de la red es de suma importancia para el correcto funcionamiento de los sistemas de información. En esta parte final, describiremos los puntos más importantes a considerar para la administración de la red de CBB.

Dentro de las organizaciones la tendencia es crecer hacia redes mas grandes soportando un número mayor de aplicaciones y de usuarios, debido a esto, dos hechos se hacen evidentes:

- La red, sus recursos asociados y las aplicaciones distribuidas se vuelven indispensables para la organización.
- Más cosas pueden fallar, deshabilitando la red o una porción de ella, o bien degradando el rendimiento a niveles no aceptables.

De tal modo, las redes grandes no pueden ser colocadas juntas y administradas por un esfuerzo humano aislado. El tamaño de dichos sistemas requiere el uso de herramientas automatizadas para la administración de la red.

5.1 AREAS DE ADMINISTRACION DE LA RED

La necesidad de administrar la red aumenta de acuerdo con la complejidad y escala de la red. La administración de la red cubre varias áreas; las mas importantes de acuerdo a la Organización Intemacional de Estándares (ISO) se mencionan a continuación:

- *Administración de fallas:* La más importante función de la adninistración de la red es mantener una alta disponibilidad de los recursos y servicios de la red. Para este propósito, es necesario monitorear la red para detectar las fallas, aislar las fallas y restablecer el equipo.
- *Administración estadística:* En las divisiones, centros de costos ó proyectos puede ser determinado el uso de recursos de la red. Una planeación efectiva para la expansión de la red requiere del entendimiento de los patrones de uso. Para ambas áreas las estadísticas de la red son necesarias.
- *Administración de configuración y nombres:* Los recursos de la red deben ser inicializados y las relaciones entre elementos establecidas para la correcta operación de la red.
- *Monitoreo del rendimiento:* Para proveer servicios eficientes con aceptable respuesta en tiempo y flujo, es necesario monitorear el rendimiento de la red.
- *Administración de la seguridad:* Los diversos esquemas utilizados para la seguridad deben ser administrados de una manera confiable y segura.

Con el monitoreo y estadísticas de la red, se puede proceder a realizar ajustes en las configuraciones de los nodos para mejorar el tiempo de respuesta.

Estos ajustes en las configuraciones se podrían realizar desde algún nodo que sea operado por el Administrador de la Red, de esta manera se realizan los cambios desde un nodo central, optimizando los recursos al evitar el desplazamiento del administrador al lugar remoto y la pérdida de tiempo que representa el realizar los ajustes en los lugares remotos.

5.2 SISTEMAS PARA ADMINISTRACION DE REDES

En la actualidad existen diversos sistemas de administración de red que nos ofrecen las facilidades antes mencionadas, proporcionando información del estado de la red en forma gráfica, permitiendo la rápida detección de fallas.

Dentro de las diferentes arquitecturas para la administración de redes las mas importantes son:

- NetView de IBM
- Estándares ISO/OSI
- Internet TCP/IP

Considerando las características del proyecto (integración de ambientes) y el uso del protocolo TCP/IP para realizar la interconexión de los equipos, el sistema de administración de red deberá ser compatible con el protocolo SNMP (Simple Network Management Protocol) que forma parte del grupo de protocolos TCP/IP. En la actualidad la mayoría de los sistemas de administración de red soportan SNMP.

Dentro de los principales proveedores de sistemas para administración de redes que soportan SNMP se encuentran Hewlett Packard con Open View y Sun con SunNet . El protocolo SNMP establece la comunicación entre el Administrador de la Red (cliente) y el Agente de la Red (dispositivos).

En ambientes de red heterogéneos como el de CBB, se requiere de dispositivos y elementos de red que puedan ser identificados como agentes SNMP. Los dispositivos que no soporten este protocolo, deberán ser monitoreados por medio de otros sistemas.

Anteriormente, la persona responsable de administrar las redes de este tipo debería ser capaz de manejar diferentes tipos de software con diferentes interfaces. Con el aumento en la estandarización de los sistemas de administración de redes, se ha permitido que las compañías reduzcan el número de personas para la administración de sus redes.

Open View permite el control de más tipos de redes, pero es más complejo y más costoso que el SunNet Manager. SunNet Manager es un producto más simple en su uso, centrado en redes TCP/IP, corre mejor en redes con menos de 1,000 nodos, es más fácil de instalar y correr que el Open View.

Los sistemas líderes en administración de redes TCP/IP como son el SunNet y el Open View deberán ser la base para soportar software de otros proveedores que permitan administrar el ambiente heterogéneo de CBB.

CONCLUSIONES

Los sistemas líderes en administración de redes TCP/IP como son el SunNet y el Open View deberán ser la base para soportar software de otros proveedores que permitan administrar el ambiente heterogéneo de CBB.

CONCLUSIONES

El diseño de la Red Corporativa de Casa de Bolsa Bancomer, permitirá que cada usuario de la red pueda compartir información con otros usuarios y utilizar recursos que se encuentran en la red como impresoras, servicios de servidores de archivos y correo electrónico, utilizando diferentes tecnologías de diferentes proveedores.

A través del diseño propuesto se logra integrar las inversiones en tecnología realizadas previamente en un entorno corporativo. El desarrollo de estándares, tanto formales como de facto por parte de la industria, ha facilitado la interconectividad de equipos, así como la integración de sistemas de diversos ambientes. En el pasado esto era muy difícil de lograr ya que la tendencia en la innovación tecnológica era seguir con una línea de diseño que sólo contemplaba compatibilidad con equipo de la misma marca, y en algunas ocasiones siguiendo al mismo proveedor esto no se cumplía.

La administración de la red permitirá detectar cualquier falla en los equipos y dispositivos de comunicación, permitiendo una rápida corrección de las fallas evitando pérdidas de tiempo en el levantamiento de los equipos. Asimismo se podrán realizar planes de capacidad de los equipos y poder determinar de manera exacta el crecimiento que de estos debe darse. Una parte importante de esto es monitorear el tráfico en la red y evitar problemas que pudieran generarse de no tomar medidas preventivas. La idea principal es generar un ambiente de administración proactivo y no reactivo.

En lo que respecta a la seguridad de la información, se logrará tener mayor confiabilidad y confidencialidad, ya que la transmisión de los archivos se realizará a través de la red, eliminando el uso de diskettes; por otra parte al tener la información en servidores compartidos se evitará la redundancia de la misma, y también se podrán realizar los respaldos eficientemente, garantizando la integridad de la información.

Otro benificio adicional será que un mayor número de usuarios podrán tener acceso a la información de la Bolsa Mexicana de Valores, lo que les permitirá realizar de manera eficiente su trabajo.

Por último, como conclusión final podemos decir que el desarrollo de la tecnología de la información y de las comunicaciones, ha generado una nueva manera de realizar los procesos de negocios, donde la información y la tecnología son piezas fundamentales para el éxito de los mismos. Por lo tanto, podemos decir que el momento histórico que nos toco vivir contempla la integración tanto de hardware y software bajo la llamada arquitectura de sistemas abiertos.

GLOSARIO

GLOSARIO

A

access-group Suborden de la interfaz Cisco que aplica una lista de acceso a una interfaz.

access-list Lista de acceso. Lista que los enrutadores Cisco emplean para controlar el acceso desde o hacia el enrutador para servicios varios, p.ej, para impedir que paquetes con una cierta dirección IP salgan de una interfaz en particular del servidor de la red.

access-method Método de acceso. Software de un procesador SNA que controla el flujo de información a través de la red. En general, se refiere a la forma en que los dispositivos de la red tienen acceso a ella.

ACF/NCP Advanced Communications Function/Network Control Program: Función de comunicación avanzada/Programa de control de redes. Programa principal de control de redes SNA. Reside en el controlador de comunicaciones y sirve como interfaz con los métodos de acceso SNA en el procesador principal para controlar las comunicaciones de la red.

ACK Abreviatura de acknowledgment (acuse de recibo) normalmente se envían ACKs de un dispositivo a otro de la red para indicar que ocurrió algún suceso (por ejemplo, la recepción de un mensaje).

active hub Dispositivo de varios puertos que amplifica señales de transmisión de una red local, LAN.

adapter Adaptador. Tarjeta de una PC, normalmente instalada dentro de la máquina, que ofrece capacidades de comunicación de red desde y hacia la computadora. Suele usarse también en lugar del término NIC.

adaptive routing Enrutamiento adaptable.

ADCCP Advanced Data Communications Control Protocol: Protocolo de control avanzado para comunicación de datos. Protocolo ANSI estándar para control de enlaces de datos que funciona en el nivel de bits.

address Dirección. Estructura de datos empleada para identificar una entidad única, como algún proceso o la localización de una red.

adjacent nodes Nodos adyacentes. En SNA, nodos conectados a algún otro, sin nodos intermedios. En DECnet y OSI, los nodos adyacentes son aquellos que comparten un segmento común (Ethernet, FDDI, Token Ring).

administrative distance Distancia administrativa. Medida de la confiabilidad de una fuente de información sobre rutas. En los enrutadores Cisco, la distancia administrativa se expresa como un valor numérico entre 0 y 255 (mientras más alto sea el valor, menor es la confiabilidad).

ADPCM Adaptive Differencial Pulse Code Modulation: Modulación diferencial adaptable codificada por pulsos. Procedimiento mediante el cual se emplea la alta correlación estadística entre muestras consecutivas de voz para crear una escala de cuantización variable (o adaptable). Con ADPCM se pueden codificar muestras analógicas de voz en forma de señales digitales de buena calidad. **Adversing**. Anuncios. Método con el que los enrutadores mantienen listas de rutas utilizables, enviando actualizaciones de enrutamiento o de servicio en perfodos especificados de tiempo.

agent Agente. Software que procesa pedidos y devuelve respuestas en alguna aplicación. En los sistemas de administración de redes los agentes residen en todos los dispositivos de bajo control y reportan los valores de las variables especificadas a las estaciones de administración. En las arquitecturas Cisco un agente es una tarjeta individual de procesador que ofrece una o varias interfaces físicas.

AGS + Advanced Gateway Server Plus: enrutador/puente Cisco de 9 ranuras con un módulo cBus de conmutación. Cinco de las ranuras se conectan al cBus.

alarm Alarma. Alarma mensaje que avisa al operador o administrador sobre problemas en la red.

A-Law Ley-A. Estándar de compresión y expansión (companding) empleado por CCITT para la conversión entre señales analógicas y digitales en sistemas PCM. Se usa más bien en las redes telefónicas europeas y es similar al estándar norteamericano mu-law (ley-mu).

alert Alerta. En NETView, es un registro que indica al operador de la red la existencia de un problema que debe ser atendido en el punto de control.

algorith Algoritmo. Reglas o procesos bien definidos.para, alcanzar la solución de un problema.

ANSI American National Standards Institute: Instituto nacional norteamericano de estándares. Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos. ANSI es miembro de ISO (International Organization for Standarization: Organización internacional para la estandarización).

API Application Programming Interface. Interfaz para programas de aplicación. Especificación de convenciones de llamadas a funciones para definir la interfaz con un servicio.

Apollo Domain Conjunto patentado de protocolos de red desarrollados por la compañía Apollo Computer para comunicaciones en redes Apollo.

AppleTalk	Serie de protocolos de comunicaciones, relacionados, creados y mantenidos por la compañía Apple Computer. Actualmente existen dos fases: I y II. La fase II, que incluye manejo de interconexión de redes, es la versión más reciente.
application layer	Capa de aplicación. Capa 7 del modelo de referencia OSI. Está implantado en varias aplicaciones de red, como correo electrónico, transferencia de archivos y emulación de terminales.
ARPANET	Red pionera de conmutación de paquetes (packet switching) desarrollada al inicio de los años 70 por la empresa BBN y financiada por la agencia ARPA (luego DARPA). ARPANET se convirtió luego en "Internet". El término ARPANET desapareció en 1990.
ASCII	American Standard Code for Information Interchange: Código estándar norteamericano para intercambio información. Código de ocho bits para representar caracteres que emplea siete bits más paridad.
ASM	Servidor de terminales CISCO en chasis A.
ASN.1	Abstract Syntax Notation One. Notación de sintaxis abstracta número uno. Lenguaje OSI para describir tipos de datos en forma independiente de estructuras computacionales y técnicas de representación. Organización internacional de estandarización, Estándar Internacional 8824, Diciembre, 1987.
asynchronous transmission	Transmisión asincrónica. Operación de un sistema de red en el cual los acontecimientos suceden sin estar sincronizados por un reloj. En tales sistemas, los caracteres individuales suelen estar encapsulados en bits de control llamados de arranque y de parada, que designan el inicio y final de los caracteres.
ATDM	Asynchronous Time Division Multiplexing: Multiplexaje asincrónico por división de tiempo. Método de envío de información que emplea el multiplexaje usual por división de tiempo (TDM), pero que en donde se asignan ranuras de tiempo cuando se requieren, en lugar de preasignarlas a transmisores específicos.
ATM	Asynchronous Transfer Mode: Modo de transferencia asincrónico. Estándar CCITT para retransmisión de celdas (cell relay) en el cual la información para diferentes tipos de servicios (voz, video,datos) se transmite en pequeñas celdas de tamaño fijo. También, modo de transmisión BISDN en el cual se usa una versión acelerada del multiplexaje asincrónico por división de tiempo (ATDM) para transferir flujos múltiples de información en un canal de comunicación.
attenuation	Atenuación. Pérdida de energía en la señal de comunicación.

AppleTalk	Serie de protocolos de comunicaciones, relacionados, creados y mantenidos por la compañía Apple Computer. Actualmente existen dos fases: I y II. La fase II, que incluye manejo de interconexión de redes, es la versión más reciente.
application layer	Capa de aplicación. Capa 7 del modelo de referencia OSI. Está implantado en varias aplicaciones de red, como correo electrónico, transferencia de archivos y emulación de terminales.
ARPANET	Red pionera de conmutación de paquetes (packet switching) desarrollada al inicio de los años 70 por la empresa BBN y financiada por la agencia ARPA (luego DARPA). ARPANET se convirtió luego en "Internet". El término ARPANET desapareció en 1990.
ASCII	American Standard Code for Information Interchange: Código estándar norteamericano para intercambio información. Código de ocho bits para representar caracteres que emplea siete bits más paridad.
ASM	Servidor de terminales CISCO en chasis A.
ASN.1	Abstract Syntax Notation One. Notación de sintaxis abstracta número uno. Lenguaje OSI para describir tipos de datos en forma independiente de estructuras computacionales y técnicas de representación. Organización internacional de estandarización, Estándar Internacional 8824, Diciembre, 1987.
asynchronous transmission	Transmisión asincrónica. Operación de un sistema de red en el cual los acontecimientos suceden sin estar sincronizados por un reloj. En tales sistemas, los caracteres individuales suelen estar encapsulados en bits de control llamados de arranque y de parada, que designan el inicio y final de los caracteres.
ATDM	Asynchronous Time Division Multiplexing: Multiplexaje asincrónico por división de tiempo. Método de envío de información que emplea el multiplexaje usual por división de tiempo (TDM), pero que en donde se asignan ranuras de tiempo cuando se requieren, en lugar de preasignarlas a transmisores específicos.
ATM	Asynchronous Transfer Mode: Modo de transferencia asincrónico. Estándar CCITT para retransmisión de celdas (cell relay) en el cual la información para diferentes tipos de servicios (voz, video,datos) se transmite en pequeñas celdas de tamaño fijo. También, modo de transmisión BISDN en el cual se usa una versión acelerada del multiplexaje asincrónico por división de tiempo (ATDM) para transferir flujos múltiples de información en un canal de comunicación.
attenuation	Atenuación. Pérdida de energía en la señal de comunicación.

AUI Attachment Unit Interface: Interfaz de unidad de vinculación. Cable IEEE 802.3 que conecta la unidad de acceso al medio (MAU: Media Access Unit) al dispositivo en red. El término AUI también se puede usar para referirse al conector del panel trasero principal al que se puede fijar el cable AUI.

ANCHO DE BANDA Una medida de la cantidad de tráfico que el medio físico puede manejar al mismo tiempo, describe la cantidad de datos que pueden ser transmitidos sobre la línea en bits por segundo. También se conoce como la diferencia entre las frecuencias más altas y más bajas para señales de red.

ANSI American National Standards Institute. Es un miembro de la ISO.

API Aplication Programming Interface. Una especificación de convenciones de llamadas a funciones que define una interface.

ARP Address Resolution Protocol. Es un protocolo de Internet utilizado para buscar y asignar una dirección IP a una dirección Ethernet/802.3. Definido en el RFC 826.

AS/400 Sistema de IBM de cómputo multiusuario que está catalogado dentro de la familia de mini-computadoras y es conocida como una computadora de base de datos de propósito general.

AT&T American Telephone and Telegraph

AUI La abreviación para Attachement Unit Interface. Un cable IEEE 802.3 que conecta el MAU al nodo. También se conoce como el conector del host al que se conecta el cable AUI (también conocido como cable de tranceiver).

B

backbone network Red fundamental. Actúa como conducto primario ("o espina dorsal") de tráfico que usualmente viene de, o va hacia, otras redes.

back channel Canal secundario. Empleado para enviar datos en dirección opuesta a la del canal primario. Los canales secundarios suelen usarse para enviar información de control. Mediante ellos, la información puede enviarse aunque el canal primario falle. También llamado canal en reversa.

back door route Ruta secundaria alterna hacia una red no local (especificada por un IPG) que debe ser usada por un enrutador de frontera. Los enrutadores Cisco permiten la especificación de rutas secundarias alternas mediante una variación de la suborden network.

back end Nodo o programa que ofrece servicios a un front end.

Balanced configuration Configuración balanceada. En HDLC, una configuración de red punto a punto con dos estaciones combinadas.

Balun Balanced, unbalanced.. Balanceado, desbalanceado. Dispositivo empleado para igualar impedancias entre una línea balanceada; normalmente entre par trenzado y cable coaxial.

Bandwith Ancho de banda. Diferencia entre la frecuencia más alta y la más baja de las señales de una red. También describe la capacidad establecida de un protocolo o un medio de datos para una red.

Baseband Banda base. Característica de la tecnología de redes en donde sólo se emplea una frecuencia portadora. La banda base se diferencia de una banda amplia (broadband), en la cual se emplean múltiples frecuencias portadoras. Ethernet es un ejemplo de red en banda base.

Basic rate Interface	Interfaz de tasa básica. Interfaz ISDN (Integrated Services Digital Network: Red digital de servicios integrados) compuesta de 2B + 1D canales.
Baud	Unidad de velocidad de señalización igual al número de condiciones discretas o sucesos en la señal por segundo. Los bauds son equivalentes a los bits por segundo cuando cada suceso en la señal representa un exactamente un bit.
Binary synchronous communication	Comunicación binaria sincrónica. Protocolo de enlace de datos por caracteres que se emplea en aplicaciones half-duplex. Se conoce simplemente como bisync.
Border gateway	Intercomunicación de frontera. Enrutador que comunica con otros sistemas autónomos (AS).
Bridge	Puente. Dispositivo que conecta dos segmentos de una red y pasa paquetes entre ellos. Los puentes operan en el nivel 2 del modelo de referencia ISO (capa de enlace de datos: link layer) y no son sensibles a los protocolos de niveles superiores.
Broad band	Banda amplia. En contraposición con la banda base (baseband), es un sistema de transmisión que multiplexa varias señales independientes en un solo cable. En la terminología de las telecomunicaciones, se refiere a cualquier canal que tenga un ancho de banda mayor que el requerido para transmitir voz (4 KHz). En la terminología de las redes locales, se refiere a un cable coaxial que maneja señales de tipo analógico.
Broadcast address	Dirección para difusión. Dirección reservada para realizar envíos simultáneos a todas la direcciones en una red.
Broadcast storm	Disturbios por difusión. Acontecimiento indeseable en una red, en el cual se envían muchas difusiones a la vez, empleando para ello considerable ancho de banda y, normalmente, causando además interrupciones en la red.
Buffer	Amortiguamiento. Zona temporal de almacenamiento empleada para el manejo de datos transitorio. Los buffers suelen emplearse para compensar las diferencias de velocidad de procesamiento entre dispositivos de la red. Las emisiones rápidas de datos se almacenan en un buffer hasta que los pueda procesar el dispositivo que funciona más lentamente.
Bus topology	Topología de bus. Arquitectura LAN lineal en la cual las transmisiones de las estaciones de la red se propagan a lo largo de todo el medio de comunicación y son recibidas por todas las demás estaciones.
BACKBONE	Una configuración de red que conecta varias LANs en una red integrada, por ejemplo en un campus.
BALUN	Balanced, unbalanced. Dispositivo utilizado para igualar impedancias entre una línea balanceada y una línea desbalanceada, generalmente entre cable par trenzado y cable coaxial.
BGP	Border Gateway Protocol. Es un protocolo de enrutamiento entre dominios que bien puede reemplazar al protocolo de enrutamiento BGP.
BNC	Conector estándar utilizado para conectar cable coaxial IEEE 802.3 10 base 2 a un transceiver.
BROUTER	Dispositivo de red que realiza las funciones de bridge y router simultanéamente.

C

Capa de aplicación	Capa de aplicación. Capa 7 del modelo de referencia OSI. Está implantado en varias aplicaciones de red, como correo electrónico, transferencia de archivos y emulación de terminales.
Capa de enlace	Capa 2 del modelo de referencia OSI, que toma un medio de transmión de datos y lo transforma en un canal que, desde el punto de vista de la capa de red: network layer, está libre de errores de transmisión . Los servicios principales de la capa de comunicación o enlace de datos son el direccionamiento, la detección de errores y el control de flujo. DATANET IPSN importante de los Países Bajos.
Capa de red	Capa 3 del modelo de referencia OSI. La capa 3 es en donde ocurre el enrutamiento.
Capa de transporte	Capa 4 del modelo de referencia OSI. Es la responsable de la comunicación confiable entre nodos terminales de la red. Realiza los controles de flujo y de errores y suele usar circuitos virtuales para asegurar entrega confiable de datos.
Capa física	Capa 1 del modelo OSI. La capa física define las interfaces eléctricas,mecánicas y físicas a la red, así como los aspectos del medio de red
Carrier	Portadora. Señal propia para ser modulada por otra señal que contiene información a ser transmitida.
CBB	Casa de Bolsa Bancomer
cBus	Tecnología de canal (bus) de medio Gigabit por segundo, patentada, desarrollada y distribuida por Cisco System, Inc.
cBus controller	Procesador de conmutación. En la arquitectura de hardware Cisco, es un tarjeta de procesador de un bit (bit-slice) que actúa como administrador de todas las actividades del cBus. También se conoce como cBus controller.
CCITT	Comite Consultant International Telegraphique et Telephonique y el inglés International and Telephone Consultative Commitee, el cual es el responsable para el desarrollo de las recomendaciones relacionadas con las telecomunicaciones incluyendo las comunicaciones de datos.
Cell relay	Transmisión por celdas. tecnología de redes basada en el uso de pequeños paquetes de tamaño fijo, llamados celdas. Las celdas contiene un identificador que especifica el flujo de datos al que pertenecen. Como son de tamaño fijo, el hardware puede procesarlas y conmutarlas a muy altas velocidades. Este método es la base de muchos protocolos de red de alta velocidad, incluyendo IEEE 802.6, DQDB, ATM y el protocolo de interfaz SMDS.
Chaining	Encadenamiento. Concepto de SNA en donde las unidades de pedido/respuesta (RU) se agrupan para propósitos de recuperación de errores.
Channel	Canal. Línea de comunicaciones. En algunos entornos se puede multiplexar varios canales en un solo cable. El término también se refiere al conducto específico entre computadoras grandes y sus periféricos.
Cheapernet	Término empleado en la industria para referirse al estándar IEEE 802.3 10BASE2 o al cable especificado en ese estándar. Thinnet, que también se refiere a ese estándar, especifica una versión más delgada y barata de cable Ethernet.
Checksum	Suma de control. Méetodo para verificar la integridad de los datos transmitidos. Es un número entero calculado a partir de una secuencia de octetos por medio de una serie de operaciones aritméticas. El valor se calcula en el lado del receptor y se compara para verificarlo.

Circuit switching Circuitos conmutados. Sistema de conmutación en el que debe existir un circuito físico dedicado entre el emisor y el emisor durante la llamada. De amplio uso en la red telefónica, los circuitos conmutados se contrastan con los métodos de competencia (contention) y token pasing para acceso al canal, y con la conmutación de paquetes (packet swiching) como técnica de conmutación.

CISCO AGS + Advanced Gateway Server Plus. Es un enrutador/bridge de nueve slots con un bus cisco de alta velocidad. Cinco de los slots se conectan al bus de alta velocidad.

Client Cliente. Nodo o programa de software que requiere servicios de un servidor.

Client-server computing Computación en modo cliente-servidor. Término empleado para describir sistemas de redes de procesamiento distribuido en donde las responsabilidades de las transacciones se dividen en dos partes: el cliente (front end) y el servidor (back end). Ambos terminos se pueden aplicar tanto a programas como a dispositivos de cómputo.

CLIENTE Un sistema que requiere servicio de otro systema

CLIENTE/SERVIDOR Modelo de computación en el cual sistemas (clientes) requieren servicios de otros sistemas (servidores) a través de una red.

CMOTCMIP over TCP. Uso del protocolo de manejo de redes OSI (CMIP) sobre las capas de protocolo Internet (TCP/IP).

CODEC *Coder-Decoder:* Codificador-decodificador. Dispositivo que normalmente emplea modulación codificada por pulsos para transformar voz analógica en un tren de bits y viceversa.

Common carrier Portador común. Compañía particular que tiene licencia para ofrecer servicios de comunicaciones al público a precios regulados.

Communication controller Controlador de comunicaciones. En SNA, nodo de subárea que contiene un programa NCP. Normalmente es un dispositivo IBM 3745.

Compression Compresión. Paso de los datos por un algoritmo que reduce el espacio/ancho de banda requerido para almacenar/transmitir el conjunto de datos.

Concentrator Concentrador. Dispositivo que sirve como centro de una red con topología tipo estrella. También se refiere a un dispositivo que contiene múltiples módulos de equipos de redes.

Configuration management Manejo de configuración. Una de cinco categorías de manejo de redes definidos por ISO para el manejo de redes OSI. Los subsistemas de manejo de configuración son los responsables de detectar y determinar el estado de la red.

Congestion Congestionamiento. Tráfico excesivo en la red.

CONP/CONS Connection/Oriented Netwok Protocol/ Connection Oriented Network Service. Protocolo/servicio OSI que ofrece operaciones por conexión a protocolos de las capas superiores.

Console Consola. DTE a través del cual se ingresan ordenes a una máquina anfitriona.

CSMA/CD *Carrier sense Multiple Access with Collision Detection:* Acceso múltiple coin detección de portadora y detección de colisiones. Mecánismo de acceso al canal en el cual los dispositivos que desean transmitir primero verifican la existencia de portadora en el canal. Si no se detecta portadora en un cierto lapso los dispositivos pueden transmitir. Si dos de ellos transmiten a la vez, ocurre una colisión, que es detectada por dispositivos especiales, que entonces retardan la retransmisión durante un período aleatorio. El acceso CSMA/CD es empleado por Ethernet y por IEEE 802.3.

D

Data link control layer	Capa de control de enlace de datos. Capa 2 del modelo de arquitectura SNA.
Datagram	Datagrama. Agrupamiento lógico de información enviada como unidad de la capa de red (network layer) en un medio de transmisión, sin el establecimiento previo de un circuito virtual. Los términos paquete, marco, (frame), segmento y mensaje también se emplean para describir agrupaciones lógicas de información en varios niveles del modelo de referencia OSI y en otras áreas de la tecnología. Los datagramas IP son las unidades primarias de información en Internet.
DDN	*Defense Data Network:* Red de datos de la defensa. La sección MILNET y otras partes asociadas de Internet que conectan instalaciones militares.
DDN X.25	Protocolo del Departamento de la Defensa de los Estados Unidos muy similar a X.25 y que es empleado en comunicaciones de la red DDN
DECnet	Una línea de productos que implenta la arquitectura de la red de Digital con un conjunto de protocolos, desarrollados por Digital Equipment Corporation. Su más reciente DECnet fase V está basada en los protocolos OSI.
DECnet routing Introducido en DECnet fase III	Es el esquema propio de enrutamiento de DEC. En DECnet phase V, completó la transición a los protocolos de enrutamiento OSI (ES-IS y IS-IS).Dedicade line. Línea dedicada. Línea de comunicaciones que no es conmutada. Cuando la línea nos es propiedad del usuario suele emplearse el término leased line: línea arrendada.
Defaul route	Ruta por omisión. Entrada de la tabla de rutas empleada para dirigir los marcos (frames) para los cuales no existe un trayecto (hop) explícitamente definido.
Designated router	Enrutador designado. En OSPF, cada red multiacceso con al menos dos enrutadores conectados tiene un enrutador designado, que genera un anuncio de estado de enlace para la red multiacceso y tiene otras responsabilidades en la ejecución del protocolo. El enrutador designado es elegido con el protocolo Hello OSPF. El concepto de enrutador designado permite una reducción en el número de adyacencias requeridas en una red multiacceso, lo cual a su vez reduce el tráfico de protocolos de enrutamiento y el tamaño de la base de datos de la topología.
Destination address	Dirección destino. Dirección de un dispositivo de recepción de la red.
Device	Dispositivo. Entidad que puede tener acceso a la red. Se emplea en forma intercambiable con nodo.
Dijkstra algorithm	Algoritmo de Dijkstra. Algoritmo de enrutamiento de trayectoria mínima que itera sobre la longitud del camino para determinar el árbol abarcador (spanning tree) de trayectoria mínima. Es de uso común en los algoritmos de estado de enlace.
DLC	*Data Link Control Layer:* Capa de control de enlace de datos. Capa SNA responsable de la transmisión de datos entre dos nodos, empleando un enlace físico.
DLCI	*Data Link Connection Identifier:* Identificador de conexión de enlace de datos. Valor Frame Relay (retransmisión de marcos) que identifica una conexión lógica.
DME	Distribuited Management Environment. Es un marco neutral del OSF que define la administración de un ambiente distribuido para los sistemas abiertos, independiente de los de los proveedores.

DNA	*Digital Network Architecture:* Arquitectura Digital de Red. Arquitectura de las redes de la compañía Digital Equipment Corporation. Se emplea el término DECnet para referirse a los productos DNA (que incluyen protocolos de comunicaciones).
Drop	Punto de enlace. Lugar de un canal multipunto en donde se hace una conexión a un dispositivo de la red.
Drop cable	Cable de punto de enlace. Cable corto que conecta un dispositivo de la red (como una computadora) a un medio físico.
DSU	*Data Service Unit:* Unidad de servicio de datos. Dispositivo empleado en la transmisión digital para conectar un CSU a un DTE.
DTE	*Data Terminal Equipment:* Equipo terminal de datos. Parte de una estación de datos que sirve como fuente o destino de los datos, o ambos, y que ofrece las funciones de control de comunicación de datos de acuerdo con los protocolos. DTE incluye computadoras, traductores de protocolo y multiplexores.
Dynamic address resolution	Resolución dinámica de direcciones. Uso de un protocolo de resolución de direcciones para determinar y almacenar información de direcciones que se solicita.
Dynamic routing	Enrutamiento dinamico. Enrutamiento que se ajusta en forma automática a cambio de tráfico o de topología de la red.

E

E1	El ancho de banda más grande (2.048 Mbits) disponible en la infraestructura digital de RDI de Telmex.
EBCDIC	*Extended Binary Coded Decimal Interchange Code:* Código extendido de intercambio decimal codificado en binario. Código de caracteres de ocho bits desarrollado por IBM para representación de datos en sus grandes sistemas de cómputo.
EGP	External Gateway Protocol. Un protocolo de Internet para intercambio de información entre sistemas autonómos. Documentado en el RFC 904.
EICON	Tarjeta que se inserta en un slot de una PC corriendo MS-DOS, para proporcionar las sesiones AS/400.
Error control	Control de errores. Técnica para asegurar que las transmisiones de la fuente sean recibidas en el destino sin errores.
Error-correcting code	Código de corrección de errores. Código con la suficiente inteligencia y dotado con la suficiente información de señalización para permitir la detección y corrección de muchos errores en el lado receptor.
Error-detecting code	Código de detección de errores. Código que puede detectar errores de transmisión mediante el análisis de los datos recibidos, basado en el grado de adhesión a gufas estructurales apropiadas que tengan.
ES-IS End System to Intermediate System.	De sistema final a sistema intermedio. Protocolo OSI que define la forma en los sistemas finales (anfitriones) se presentan a los sistemas intermedios (enrutadores).
ETHERNET	Un protocolo de red de área local que utiliza el método de acceso CSMA/CD. Desarrollado por Xerox y Digital Equipment para correr en cable coaxial. Ethernet es similar a una serie de estandares producidos por la IEEE conocido como IEEE 802.3.

Ethernet Especificación Ethernet Especificación de red LAN de banda base inventada por la corporació Xerox y desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet operan a 10 megabits por segundo utilizando CSMA/CD sobre cable coaxial. Es similar a una serie de estándares producidos por IEEE y conocidos como IEEE 802.3.

Event Suceso, Acomecimiento. Mensaje de la red que indica irregularidades operacionales en los elementos físicos de una red, o la respuesta ante la ocurrencia de una tarea significativa, que normalmente es el cumplimiento de un pedido de información.

EXCEL Software de Microsoft de hoja electrónica

Expansion Expansión. El paso de datos comprimidos a través de un algoritmo que los restituye a su tamaño original.

Exterior gateway protocol. Protocolo de servidor de interconexión externo. Cualquier protocolo de interconexión de redes empleado para intercambiar información de rutas entre sistemas autónomos. No debe confundirse con EGP, que es una instancia particular de uno de ellos.

F

Fan-out unit Unidad de frente de salida. Dispositivo que permite que múltiples dispositivos se comuniquen.

FCS *Frame Check Sequence:* Secuencia de verificación de marcos. Término HDLC adoptado por las siguientes capas de enlace de los protocolos que se refieren a los caracteres extra que se añaden al marco para propósitos de control de errores.

FDDI *Fiber Distributed Data Interface:* Interfaz de datos distribuidos por fibra. Estándar distribuido por ANSI que especifica una red tokenpassing de 100 Mbps empleando cable de fibra óptica.

FEP *Font End Processor:* Procesador frontal. Dispositivo o tarjeta que ofrece a un dispositivo capacidades de interfaz de red. En SNA, normalmente es un dispositivo 3745.

Fiber-optic cable Cable de fibra óptica. Medio flexible y delgado capaz de conducir transmisiones de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más caro, no es sensible a la interferencia electromagnética y es capaz de mayores velocidades de manejo de datos.

File transfer Transferencia de archivos. Una de las aplicaciones de redes más populares, en la que se llevan archivos de un dispositivo de la red a otro.

Filter Filtro. En forma genérica, se refiere a un proceso o dispositivo que filtra la información que le llega, permitiendo sólo el paso de algún subconjunto de ella que tenga ciertas características.

Flooding Inundación. Técnica de enrutamiento en la que la información de enrutamiento que recibe el dispositivo enrutador se manda por cada una de sus interfaces, exceptuando (normalmente) la interfaz por la cual se recibió. Flow control. Control de flujo. Técnica para asegurar que una entidad transmisora no abrume a una entidad receptora con datos.

FOIRL *Fiber-Optic Inter Repeater Link:* Enlace inter-repetidor de fibra óptica. Metodología de señalización de fibra óptica basada en la especificación de fibra óptica IEEE 802.3.

Forwarding Envío. La expedición de un marco (frame) hacia su destino último por medio de un dispositivo de intercomunicación entre redes.

Fragment Fragmento. Parte de un paquete (packet) mayor que se ha partido en unidades más paqueñas.

Fragmentation Fragmentación. Proceso de partir un paquete en unidades menores cuando se transmite en un medio de redes que no maneja el tamaño original del paquete.

Frame relay Retransmisión de marcos. Protocolo empleado en la interfaz entre dispositivos de usuario (por ejemplo, máquinas anfitrionas y enrutadores) y equipos de redes (por ejemplo, nodos de conmutación). Es más eficiente que X.25, protocolo del cual generalmente se considera como reemplazo.

Frame. Marco. Agrupamiento lógico de información enviado a un medio de transmisión como una unidad de la capa de enlace (link layer). Los términos paquete, datagrama, segmento y mensaje también se emplean para describir agrupamientos lógicos de información en varias capas del modelo de referencia OSI y en círculos técnicos.

Frequency Frecuencia. Medida en hertz (Hz), es el número de ciclos de una señal de corriente alterna por unidad de tiempo.

Front end Nodo o programa que solicita servicios de un back end.

FTP *File Transfer Protocol:* Protocolo de transferencia de archivos. Protocolo de aplicación IP para transferir archivos entre nodos de la red.

FTP File Transfer Protocol. Es un protocolo de aplicación del conjunto de protocolos TCP/IP, utilizado para la transferencia de archivos entre nodos de la red.

Full duplex Capacidad de transmisión simultánea de datos en ambas direcciones.

G

GATEWAY En LANs, un sistema y software asociado que permite que dos redes utilizando diferentes protocolos se puedan comunicar una a la otra. Un gateway traduce todos los niveles del protocolo desde el nivel físico hasta el nivel de aplicación, y puede ser utilizado para interconectar redes que difieran en cada detalle.

Gateway host Servidor de intercomunicación anfitrión. En SNA, nodo anfitrión que contiene un servidor de intercomunicación SSCP.

GFB Grupo Financiero Bancomer

GGP *Gateway-to-Gateway Protocol:* Protocolo de servidor a servidor de intercomunicaciones. Protocolo MILNET que especifica la forma en que los servidores (o los enrutadores) básicos (core gateway) deben intercambiar información sobre rutas y enlaces.

H

Half duplex Capacidad de transmitir datos en sólo una dirección a la vez.

Half gateway Medio gateway. Literalmente, dispositivo que efectúa las funciones de medio servidor de intercomunicaciones, pues éstos suelen dividirse en dos mitades funcionales para facilitar su diseño y mantenimiento.

Handshake Secuencia de mensajes que dos o más dispositivos de la red intercambian para asegurar sincronización en la transmisión.

Hardware address Dirección de hardware. También conocida como physical address: dirección física o MAC layer address: dirección de la capa de control de acceso. Capa de enlace de datos asociada con un dispositivo particular de la red. Contrasta con una dirección o protocolo de red, que es una dirección de la capa de red (network layer).

HDH HDLC *Distant host:* Anfitrión remoto HDLC. Forma de ejcutar el protocolo 1822 sobre enlaces serie sincrónicos en lugar de sobre hardware especial 1822. HDH es esencialmente header (encabezados) 1822 y datos encapsulados en paquetes LAPB (X.25 nivel 2).

HDLC *High-level Data Link Control:* Control de enlace de datos de alto nivel. Protocolo de capa de enlace OSI estándar por bits de uso común, derivado de SDLC. Especifica un método de encapsulamiento de datos de enlaces serie sincrónicos. El servicio HDLC de Cisco sólo maneja la creación de marcos y funciones de suma de control (checksum).

Headend El punto terminal de una red broadband (de banda amplia), todas las estaciones transmiten hacia ese punto, para que luego éste transmita hacia las estaciones destino.

Header Encabezado. Información de control que se añade a los datos antes de encapsularlos para su transmisión en la red.

HELLO Protocolo de enrutamiento empleado principalmente por los nodos NSFnet. Permite a conmutadores confiables descubrir rutas de retraso mínimo. Por otro lado, el protocolo HELLO (sin relación con HELLO de NSFnet) es empleado por sistemas OSPF para establecer y mantener relaciones de vecindad.

Hierarchical routing Enrutamiento jerárquico. Enrutamiento basado en un sistema de direccionamiento jeráquico. Por ejemplo, los algoritmos de enrutamiento IP emplean direcciones IP, que contienen números de la red, números de máquinas anfitrionas y (posiblemente) números de subredes.

HOP La visita de un paquete de datos a través de un enrutador.

Hop count Cuenta de trayecto. Métrica de enrutamiento usada para medir la distancia entre una fuente y un destino. Cada hop equivale al paso de un paquete por un enrutador.

Host Anfitrión. Sistema de cómputo en una red. Es similar a los términos device (dispositivo) o node (nudo), excepto que usualmente implica un sistema de cómputo, mientras que dispositivo y nodo generalmente se aplican a cualquier sistema de red, que incluye terminal servers (servidores de terminales) y enrutadores.

Host node Nodo anfitrión. Nodo de subárea SNA que contiene un SSCP.

HP-UX Sistema operativo Unix de Hewlett Packard, derivado del Unix System V.

Hub Concentrador. En forma genérica, término que describe un dispositivo que sirve como centro de una red con topología de estrella. En la terminología Ethernet/IEEE 802.3 se refiere a un repetidor multipuerto, que a veces también se conoce como concentrador. El término también se usa para el dispositivo de hardware/software que contiene múltiples módulos independientes, aunque conectados, de equipo de redes e interconexión entre redes. Los concentradoeres pueden ser activos (que repiten las señales que les llegan) o pasivos (que no repiten, sino sólo reparten las señales que les llegan).

Hybrid network Red híbrida. Término usado para describir una interconexión entre redes hecha con más de un tipo de tecnología de redes, que incluye la LAN y WAN.

I

IBM International Bussiness Machine

IDF Intermediate Distribution Frame. Panel de distribución por piso.

IEEE	*Institute of Electrical and Electronic Engineers:* Instituto de Ingenieros Eléctricos y Electrónicos. Organización profesinal que define estándares de redes. Los estándares LAN de IEEE son los predominantes en la actualidad, e incluyen protocolos similares o virtualmente equivalentes a Ethernet y Token Ring.
IEEE 802.2	Protocolo LAN de IEEE que especifica la implantación de la subcapa de control de enlace lógico de la capa de enlace. Se encarga del manejo de errores, creación de marcos y flujo de control, es interfaz de servicio con la capa 3. Se emplea en redes LAN tales como IEEE 802.3 e IEEE 802.5.
IEEE 802.3	Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza accesos CSMA/CD en varias velocidades usando varios medios físicos. Una variante física de IEEE 802.3 (10BASE5) es muy similar a Ethernet.
IEEE 802.3	El protocolo IEEE para LANs que especffica una implementación del nivel físico y el sub-nivel MAC del nivel Data Link. IEEE utiliza el método de acceso CSMA/CD y es muy similar a Ethernet.
IEEE 802.4	Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso Tokenpassing sobre una topología de bus.
IEEE 802.5	Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso Tokenpassing a 4 o 16 Mbps sobre cable de par trenzado blindado y es muy similar a Token Ring de IBM.
IEEE 802.5	El protocolo IEEE para LANs que especffica una implementación del nivel físico y el sub-nivel MAC del nivel Data Link. IEEE 802.5 Utiliza el método de acceso "token passing" a 4 o 16 Mbps sobre cableado STP y es muy similar al TokenRinng de IBM.
IEEE 802.6	Especificación IEEE de red de área metropolitana (Metropolitan Area Network:: MAN) basada en la tecnología DQDB.
IGP	Interior Gateway Protocol. Un protocolo de Internet utilizado para el intercambio de información dentro de un sistema autónomo. Entre los protocolos IGPs están el RIP, IGRP, Y EL OSPF.
INFOSEL	Sistema de información finaciera proporcionado por radio frecuencia y RDI.
INFOTRADE	Software de análisis financiero.
Interfaz	Conexión entre dos sistemas o dispositivos. En la terminología de enrutadores es una conexión de la red. También se refiere a la frontera entre capas adyacentes del modelo OSI. En telefonía, es una frontera compartida que está definida por características de interconexión física comunes, características de la señal y significados de las señales intercambiadas.
Interference	Interferencia. Ruido indeseado en el canal de comunicación.
Intermedlate system	Sistema intermedio. Nodo de enrutamiento en una red OSI.
Internet	Término empleado para referirse al sistema de interconexión de redes más grande del mundo, que conecta miles de redes en todo el planeta y que desarrolló una "cultura" basada en simplicidad, investigación y estandarización fundamentada en el uso real. Buena parte de la tecnología de punta en redes vino de esta comunidad. Internet evolucionó a partir de ARPANET.

Internet address Dirección Internet. También llamada "dirección IP", es una dirección de 32 bits asignada a máquinas anfitrionas que emplean TCP/IP. La dirección se escribe como cuatro octetos separados con puntos (formato decimal con punto), formados por la sección de la red, una sección opcinal de subred y una sección del anfitrión.

Internetwork Redes interconectadas. Conjunto de redes interconectadas por enrutadores y que en forma genérica funciona como una sola. A veces se le llama internet, lo cual no debe confudirse con la palabra Internet.

Internetworking Interconexión de redes. Término genérico usado para referirse a la industria que surgió alrededor del problema de conectar redes. El término se puede referir tanto a productos como a procedimeintos y a tecnologías.

INTEROPERABILIDAD La habilidad de que todos los elementos de un sistema intercambien información entre equipo de multiple vendedores. También llamada comunicaciones abiertas.

Intra-area routing Enrutamiento entre áreas. Término empleado en los enrutadores DECnet para describir enrutamiento dentro de un área.

IP Internet Protocolo. Un protocolo de nivel 3 que contiene información de direccionamiento y algún control de información que permite a los paquetes sean enrutados. Documentado en RFC 791.

IP address dirección IP. Vease Internet Address

IP Internet Protocol Protocolo Internet. Protocolo de capa 3 (capa de red) que contiene información de direccionamiento y de control para permitir el enrutamiento de paquetes. Está documentado en RFC 791.

IPX *Internetworking Packet Exchange:* Intercambio de paquetes de interconexión de redes. Protocolo Novell de capa 3, similar a XNS e IP que se emplea en redes NetWare.

IS Intermediate System. Un nodo de enrutamiento en una red OSI.

IS-IS *Intermediated System to Intermediate System:* Sistema intermedio a sistema intermedio. Protocolo jerárquico de enrutamiento OSI de estado de enlace (link-state), basado en enrutamiento DECnet Phase V, en donde los sistemas intermedios (enrutadores) intercambian información basada en una sola métrica, para determinar la topología de la red.

ISDN *Integrated Services Digital Network:* Red Digital de Servicios Integrados. Protocolos de comunicación propuestos por las compañías telefónicas para lograr que las redes de teléfono transmitan datos, voz y otro materiales de la fuente.

ISO *International Organization for Standarization:* Organización internacional para la estandarización. Organización internacional responsable de una amplia gama de estándares, incluyendo aquellos relevantes para las redes. ISO la es responsable del modelo de referencia de redes más popular: el modelo de referencia OSI.

J

Jabber Balbuceo. Condición de error en la cual un dispositivode la red continuamente transmite "basura" a la red. En IEEE 802.3 se refiere a un paquete de datos cuya longitud excede a la preescrita en el estándar.

Jitter Distorsión de las líneas de comunicación analógicas causada por una variación en las posiciones de referencia temporal de una señal. Puede causar pérdida de datos, particularmente a latas velocidades.

L

LAN	*Local Area Network:* Red de área local. Red que cubre una área geográfica relativamente pequeña (usualmente no mayor que un grupo local de edificios) Comparadas con las redes WAN, las redes LAN suelen caracterizarse por velocidades de transferencia de datos relativamente altas y una relativamente baja incidencia de errores.
LAN Manager	Sistema de archivos distribuidos desarrollado y manejado por Microsoft.
LAN Network Manager	Paquete de manejo Token Ring y source-bridge ofrecido por IBM. Normalmente opera en una PC y verifica los puentes de rutas fuente (source-route bridges) y los dispositivos Token Ring, y puede pasar mensajes de alerta a NetView.
LAN ROUTER/400	Software que corre en la tarjeta EICON, para proporcionar el Gateway al sistema AS/400.
LAN Server	Sistema de archivos distribuido derivado de LAN Manager, desarrollado y manejado por IBM.
LAPB	*Link Access Procedure Balanced:* Procedimiento balanceado de acceso de enlace. Derivado de HDLC, es una versión CCITT X.25 de un protocolo de enlace de datos por bits.
LAPD	*Link Access Protocol D:* Protocolo d de acceso de enlace. Protocolo ISDN de capa de enlace (link layer) para el canal D. Se derivó del protocolo LAPB CCITT X.25 y está diseñado primordialmente para satisfacer los requerimientos de señalización del acceso básico ISDN. Está definido por las recomendaciones Q.920 y Q.921 de CCITT.
LASER	*Light Amplification by Stimulated Emission of Radiation:* Amplificación de luz por emisión estimulada de radiaciones. Dispositivo analógico de transmisión en el cual un material activo adecuado es excitado por un estímulo externo para producir un estrecho haz de luz coherente, que puede ser modulado en pulsos para transmitir datos. Las redes basadas en tecnología laser están apenas comenzando, pero parecen prometedoras debido a anchos de banda potencialmente amplios y una relativa resistencia a la interferncia.
LAT	*Local Area Transport:* Transporte de área local. Protocolo de terminal virtual de red desarrollado por Digital Equipment Corporation.
LATA	*Local Access and Transport Area:* Area de transporte y acceso local. Area de marcaje telefónico atendida por una sola compañía telefónica local. Las llamadas dentro de una área LATA se conocen como llamadas locales. Hay más de estas áreas en los Estados Unidos.
Leased line	Línea arrendada o privada. Línea de transmisión reservada por un portador de comunicaciones para uso privado de un cliente.
LIne conditioning	Acondicionamiento de línea. Uso de equipo, en líneas de voz arrendadas, para mejorar las características analógicas, permitiendo así mayores velocidades de transmisión.
Line driver	Dispositivo manejador de la línea. Convertidor de señal/amplificador poco costoso que acondiciona las señales digitales para garantizar una transmisión confiable a largas distancias.
Line of sight	Línea de vista. Característica de ciertos sistemas de transmisión, como el láser, las microondas y los sistemas infrarojos, en donde no puede existir obstrucción en el camino directo entre el transmisor y el receptor.
Line turnaround	Tiempo de cambio en la línea. Tiempo requerido para guardar la dirección de la transmisión de datos en una línea de telefóno.

Link Enlace. Canal de comunicaciones de la red consistente en un circuito o una trayectoría de transmisión, incluido el equipo existente entre el transmisor y el receptor. Suele usarse para referirse a una conexión en una red WAN.

Link layer Capa de enlace.

Link-state routing algorithm Algoritmo de estado de enlace. Algoritmo de enrutamiento en el que cada enrutador difunde a todos los nodos la información del costo de acceso a cada uno de sus vecinos. Estos algoritmos crean una vista consistente de la red y por ello no son propensos a caer en ciclos de enrutamiento, aunque logran esto a costa de una relativamente mayor dificultad computacional y de un tráfico un tanto más diseminado (en comparación con los algoritmos de enrutamiento de vector de distancias).

Load balancing Balanceo de carga. En enrutamiento se refiere a la capacidad de un enrutador para distribuir el tráfico a todos sus puertos de la red que estén a la misma distancia de la dirección de destino. Los buenos algoritmos de balanceo de cargas usan información sobre la velocidad de la línea y sobre su confiabilidad. El balanceo de la carga incrementa la utilización de los segmentos de la red y aumentan el ancho de banda efectivo de la red.

Local bridge Puente local. Puente que directamente interconecta redes en la misma área geográfica.

Local loop Ciclo local. La línea que va de las instalaciones del abonado del teléfono a la oficina central (CO) de la compañía telefónica.

Local talk Protocolo de red de banda base CSMA/CD de 230 Kbps patentado por Apple.

Logical channel Canal lógico. Trayectoría de comunicaciones no dedicada, para conmutación de paquetes, entre dos o más nodos de la red. Mediante conmutación de paquetes pueden existir varios canales lógicos simultáneamente en un mismo canal físico.

Loop Ciclo. Ruta en la cual los paquetes nunca llegan a su destino, sino que sólo recorren un ciclo o bucle a través de una serie constante de nodos de la red.

Loopback test Prueba de ciclos. Prueba en la cual se envían y regresan señales hacia la fuente en algún punto del trayecto de comunicaciones. Suelen emplearse para probar qué tan utilizables son las interfaces de la red.

LU 6.2 Logical Unit 6.2. Unidad lógica que gobierna las comunicaciones SNA entre nodos equivalentes (peer-to-peer).

M

MAC Media Access Control. El sub-nivel de Data Link responsable de la programación, transmisión y recepción de datos en un medio compartido de una LAN.

MAC sublayer *Media Access Control sublayer:* Subcapa de control de acceso al medio. Como está definida por la IEEE, se trata de la porción baja de la capa de enlace de datos del modelo OSI. La subcapa MAC se encarga de los asuntos de acceso al medio de las comunicaciones, como por ejemplo determinar si se usará token passing (paso de estafeta) o contention (competencia).

MAN *Metropolitan Area Network:* Red de área metropolitana. En términos generales se refiere a una red que ocupa una área metropolitana, geográficamente mayor que la ocupada por una red local (LAN), pero menor que la de una red amplia (WAN).

Managed object Objeto de manejo. En manejo de redes se refiere a un dispositivo de la red que es tratado por un protocolo de manejo de la red.

Management services Servicios de manejo. Funciones SNA distribuidas entre componentes de la red para manejar y controlar una red SNA.

MAU *Medium Attachment Unit (IEEE 802.3):* Unidad de vinculación, o Multistation Access Unit (IEEE 802.5): Unidad de acceso a estaciones múltiples. En el primer caso, es un dispositivo que realiza las funciones de la capa 1 de IEEE 802.3, que incluyen la detección de colisiones y la inyección de bits a la red. Una unidad MAU se conoce como transceiver (transmisor/receptor) en la especificación Ethernet. En el segundo caso (a veces llamadas también MSAU para que no se confundan con las primeras), se trata de concentradores de cables a los cuales se conectan los nodos de Token Ring.

Media Medios. Entorno físico mediante el cual pasan las señales de transmisión. Los medios usuales en redes son el par trenzado, el cable coaxial, la fibra óptica y la atmosfera (a través de la cual viajan las microondas, el láser y la transmisión infraroja).

Message Mensaje. Agrupamiento lógico de información en la capa de aplicación (application-layer).

Message-switching Conmutación de mensajes. Técnica de conmutación que transmite mensajes de nodo a nodo en una red. El mensaje se almecena en cada nodo hasata que llega el momento en el que se consigue una trayectoría de envío.

MIB Management Infomation Base. Una base de datos de información de los objetos que pueden ser accesados por medio de los protocolos de administración como SNMP o CMIP.

Microwave Microondas. Ondas electromagnéticas en la gama de 1 a 30 Gigahertz. Las redes basadas en microondas constituyen una naciente tecnología que gana campo debido a su alto ancho de banda y su relativamente bajo costo.

MIPS Software de información finaciera que llega a CBB por X.25.

MIT Massachusets Institute of Technology

MODEM *Modulator/Demodulator:* Modulador/Demodulador. Dispositivo que convierte señles digitales a una forma adecuada para transmisión sobre medios de comunicación analógicos, y viceversa.

Modulation Modulación. Proceso por el cual se transforman las caracter•lsticas de las señalles para presentar información. Los tipos de modulación incluyen frecuencia modulada (FM), en donde señales de diferentes frecuencias representan valores de datos diferentes, y amplitud modulada (AM), en donde la amplitud de la señal varía para representar diferentes valores de datos.

MOTIF Interface gráfica estándar promovida por el OSF

MS-MAIL Correo electrónico de Microsoft

MSAU *Multistation Access Unit:* Unidad de acceso a estaciones múltiples.

Multimode fiber Fibra multimodal. Fibra que mane ja la ropagación de múltiples patrones de campo electromagnético.

Multipoint line Línea multipunto. También llamada multidrop line: línea de múltiples puntos de enlace. Línea de comunicaciones con multiples puntos de acceso al cable.

Multivendor network Red de varios fabricantes. Red que utiliza equipo de más de un fabricante. Estas redes tienen más problemas de compatibilidad que las de un solo fabricante o distribuidor.

N

Name server Servidor de nombres. servidor que la red ofrece para resolver nombres de la red y asociarlos con localidades (direcciones) de la red.

Narrow band Vease baseband.

NAU Network Addressable Unit: Unidad direccionable en la red. Término SNA para las entidades direccionables. Entre los ejemplos se incluye PU, LU y SSCP.

NCP *Network Control Program:* Programa de control de la red. En SNA, se refiere a los programas que asignan rutas y controlan el flujo de datos entre un controlador de comunicaciones (en el cual residen) y otros recursos de la red.

NDIS Network Driver Interface Specification. Una especificaicón producida por Microsoft para manejar un driver genérico en las tarjetas NIC (Network Interface Card), independiente del proveedor y protocolo.

Neighboring routers Rutadores vecinos. En OSPF, se refire a dos enrutadores que tienen interfaces a una red común. En redes de acceso múltiple, los vecinos se descubren en forma dinámica mediante el protocolo Hello de OSPF.

NETBIOS Network Basic Input/Output System. Una interface del nivel de sesión para redes de PCs de IBM y Microsoft

NETWARE Desarrollado y vendido por Novell. Netware proporciona servicio de archivos.

Network Red. Conjunto de computadoras y otros dispositivos que son capaces de comunicarse entre sí empleando un medio reticular.

Network address Dirección de la red. También llamada protocolo de la red (network protocol), es una dirección de la capa de red (network layer) que se refiere a un dispositivo lógico, no físico, de la red.

Network administrator Administrador de la red. Persona que ayuda a mantener la red.

Network analyzer. Analizador de la red. Dispositivo de hardware/software que ofrece algunas características de solución de problemas de la red, incluidos decodificadores de paquetes de protocolos específicos, pruebas de errores preprogramadas, filtrado y transmisión de paquetes.

Network layer Capa de red. Capa 3 del modelo de referencia OSI. La capa 3 es en donde ocurre el enrutamiento.

Network management Manejo de red. Término genérico que describe sistemas o acciones que ayudan a mantener, caracterizar o arreglar una red. Es un tópico importante en el campo más general de las redes.

NFS *Network File System:* Sistemas de archivos en red. Como se emplea normalmente, es un conjunto de protocolos de sistemas de archivos distribuidos desarrollado por la empresa Sun Microsystems, que permite el acceso remoto a archivos en una red. En realidad, NFS es uno de los protocolos del conjunto, que incluye NFS, XDR (External Data Representation: Representación externa de datos), RPC (Remote Procedure Call: Llamada remota a procedimientos), y otros. Esos protocolos son parte de una arquitectura mayor que la empresa Sun nombra como ONC (Open Network Computing).

NIC Network Information Center.Un centro que proporciona acceso a los RFCs y otra información relacionada con Internet.

Node Nodo. Término genérico que se refiere a una entidad que puede tener acceso a una red. Se usa también el término device: dispositivo.

Noise Ruido. Señales indeseadas en el canal de comunicaciones.

NOS *Network Operating System:* Sistema operativo de red. Término genérico para referirse a lo que en realidad son sistemas distribuidos de archivos.Ejemplo de esto incluyen NetWare, VINES de Banyan, NFS y LAN Manager.

Nyquist Sampling Theorem. Teorema de muestreo de Nyquist. Teorema demostrado por H. Nyquist que indica que es posible reconstruir señales analógicas a partir de muestras si se toman suficientes de ellas.

O

ODI Open Data-link Interface. La especificaión de Novell proporcionando una forma de estandarizar el acceso a las redes.

OFFICE Software de oficina de Microsoft que consiste el los paquetes Word, Excel, PowerPoint y Mail.

OIM OSI *Internet Management:* Manejo Internet OSI. Grupo de trabajo para la especificación de formas en que pueden usarse protocolos de manejo de red OSI en redes TCP/IP.

ONC *Open Network Computing:* Computación en redes abiertas. Arquitectura de aplicaciones distribuidas fundada por la empresa Sun Microsystem y actualmente controlada por un consorcio encabezado por Sun. Los protocolos NFS son parte de ONC.

Open architecture Arquitectura abierta. Arquitectura para la cual terceros pueden desarrollar productos legalmente, y de la que existen especificaciones de dominio público.

Open circuit Circuito abierto. Trayectoria cortada en un medio de transmisión. Normalmente impide la comunicación en la red.

OPENVIEW Software para administración de la red de Hewlett Packard

Optical fiber Fibra óptica. Vease fiber-optic cable.

OSF Open Software Fundation. Una corporación independiente creada para desarrollar especificaciones abiertas y tecnología para un ambiente de sistema operativo y aplicaciones.

OSI *Reference Model:* Modelo de referencia OSI. Modelo de arquitectura de redes desarrollado por ISO y CCITT. Consiste en siete capas, cada una de las cuales especifica funciones particulares de la red, tales como direccionamiento, control de flujo, control de errores, encapsulamiento, transferencia confiable de mensajes y muchas otras. La capa más alta (application layer: capa de aplicación) es la más cercana al usuario. La capa más baja (phycal layer: capa física) es la más cercana a la tecnología del medio físico. El modelo de referencia OSI es universalmente usado como método de enseñar y entender la funcionalidad de las redes.

OSPF *Open Shortest Path First:* La trayectoria abierta más corta primero. Algoritmo de enrutamiento jerárquico IGP de estado de enlace propuesto como sucesor de RIP en la comunidad Internet. Sus características incluyen enrutamiento de costo mínimo, enrutamiento de camino múltiple y balanceo de cargas. Se deriva de una versión inicial del protocolo OSI IS-IS.

Out-of-band signaling Señalización fuera de banda. Transmisión que usa frecuencias o canales fuera de los empleados para transferencia de información. Suele usarse para reporte de errores en situaciones en las que la señalizació dentro de banda puede ser afectada por los problemas que la red esté experimentando.

P

Packet Paquete. Agrupamiento lógico de información que incluye un encabezado (header) y (normalmente) datos del usuario.

Packet buffer Buffer de paquetes.

Packet switching	Conmutación de paquetes. Red en la cual los nodos comparten el ancho de banda porque mandan unidades lógicas de información (packets) en forma intermitente. En contraste, un red de conmutación de circuitos (circuit switching) dedica un circuito a la vez para la transmisión de datos.
PAD	*Packet Assembles/Disassembler:* Ensamblador/Desensamblador de paquetes. Dispositivo usado para conectar dispositivos simples (como por ejemplo, terminales que trabajan en modo de caracteres) que no tienen capacidad de ensamblar ni desensamblar paquetes, a redes X.25. El PAD sirve como buffer para datos enviados entre las máquinas anfitrionas y las terminales de una red X.25, como se define en las recomendaciones CCITT X.3, X.28 y X.29.
PAM	*pulse Amplitude Modulation:* Amplitud modulada por pulsos. Esquema de modulación en el cual se hace que la onda moduladora module la amplitud de un tren de pulsos.
parallel transmission	Transmisión paralela. Transmisión simultánea de todos los bits que forman un byte o un carácter.
Parity check	Verificación de paridad. Proceso para verificar la integridad de un carácter. Consiste en añadir un bit que haga el número total de bits binarios en "1" en un carácter o en una palabra (excluyendo al bit de paridad) sea impar (en "odd parity": paridad impar) o par (en "even parity": paridad par).
Path control layer	Capa de control de trayectoria. Capa 3 en el modelo arquitectónico SNA. Se trata de la capa SNA que enruta paquetes en una interconexión entre redes.
Path control network	Red de control de trayectorias. Concepto SNA consistente en componentes de menor nivel que controlan el enrutamiento y el flujo de datos a través de una red SNA, y que maneja la transmisón física de datos entre los nodos SNA. Contrasta con las NAU, que ofrecen servicios de más alto nivel.
PC SUPPORT	Software que reside en el sistema AS/400 y una parte en las PCs que requieren emular terminales IBM 5250
PCM	*Pulse Code Modulation:* Modulación por código de pulsos. Transmisión de información analógica en forma digital mediante muestreo y codificación con un número fijo de bits.
PDN	*Public Data Network:* Red pública de datos. Red operada por el gobierno (como en Europa) o en forma privada para ofrecer comunicaciones por computadora al público, normalmente cobrando una cuota. Las redes PDN permiten a las organizacines pequeñas crear una red WAN sin todo el costo del equipo de circutos de larga distancia.
PDS	Premises Distribution System. Sistema de cableado desarrollado y vendido por AT&T.
PDU	*Protocol Data Unit:* Unidad de datos de protocolo. Término equivalente a packet (paquete), definido por OSI. Los dispositivos los intercambian dentro de un nivel específico del modelo de referencia OSI.
Peer-to-peer computing	Computación entre nodos similares o equivalentes. En contraste con la computación en modo cliente-servidor, la computación entre nodos equivalentes pide a cada dispositivo ejecutar ambas porciones, cliente y servidor de una aplicación. La frase también puede emplearse para describir la comunicación entre implantaciones de la misma capa del model OSI en dos diferentes dispositivos de la red.

Performance management Manejo del desempeño. Una de las cinco categorías de manejo de redes definidas por ISO para el manejo de las redes OSI. Los subsistemas de manejo del desempeño son responsables de analizar y controlar el desempeño de la red, incluyendo su capacidad y las tasas de error.

Peripheral node Nodo periferico. En SNA, es un nodo que usa direcciones locales y por tanto no es afectado por cambios a las direcciones de la red. Los nodos perifericos requieren de la asistencia de funciones cercanas de un nodo de una subárea adyacente.

Physical address Dirección física. Término empleado algunas veces para referirse a la dirección de la capa de enlace (link-layer) de un dispositivo de la red. Contrasta con una dirección de red o de protocolo (network protocol), que son direcciones de la capa de la red.

Physical control layer Capa física de control. Capa 1 en el modelo arquitectónico SNA.

Physical layer Capa física. Capa 1 del modelo OSI. La capa física define las interfaces eléctricas, mecánicas y físicas de la red, así como los aspectos del medio de red.

Physical medium Medio físico.

Port Puerto. Interfaz en un dispositivo de interconexión de redes (como por ejemplo, un enrutador). En terminología IP, puerto también se usa para especificar el proceso de recepción de las capas superiores.

POWER BUILDER Herramienta de desarrollo de 4a. generación

POWERPOINT Software de Microsoft que permite desarrollar presentaciones y gráficos.

PPP *Point-to-point Protocol:* Protocolo de punto a punto. Sucesor de SLIP, este protocolo ofrece conexiones de enrutador a enrutador y de anfitrión a red empleando circuitos sincrónicos y asincrónicos.

Presentation layer Capa de presentación. Capa 6 del modelo de referncia OSI. Esta capa se encarga de la sintaxis de los datos intercambiados entre dos entidades de la capa de aplicación.

Presentation services layer. Capa de presentación de servicios. Capa 6 del modelo arquitectónico SNA.Vease presentation layer.

PRI *Primary Rate Interface:* Interfaz de tasa primaria. Interfaz ISDN de acceso a la tasa primaria. Este acceso consiste en un único canal D de 64 Kbps más 23 (en el caso de 1.56 Mbps) ó 30 (en el caso de 2.048 Mbps) canales B para voz o datos.

Primary station Estación primaria. En los protocolos sincrónicos por bits de la capa de enlace, tales como HDLC y SDLC, es la estación que controla las actividades de transmisión de los secundarios y efectúa otras funciones, tales como control de errores, mediante encuestas (polling) u otros medios. Los primarios envían ordenes a los secundarios y reciben las respuestas.

Print server Servidor de impresoras. Sistema de computación en red que recibe, maneja y ejecuta (o envía para su ejecución) los pedidos de impresión de otros dispositivos de la red.

Propagation delay Tiempo de propagación. Tiempo requerido para que los datos en una red viajen desde el origen hasta el destino final.

Protocol Protocolo. Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.

Protocol address Dirección de protocolo. Vease network address.

Protocol stack Pila de protocolos. Capas de software de protocolo relacionadas que juntas funcionan para realizar una arquitectura específica de comunicaciones. Los ejemplos incluyen Apple Talk, DECnet y muchos otros.

Protocolo translator Traductor de prtocolos. Dispositivo o software de la red que convierte de un protocolo a otro similar, por ejemplo, el CPT Cisco efectúa conversiones entre X.25, PAD y Telnet.

PSN *Packet Switch Node:* Nodo de conmutador de paquetes. Conmutador de paquetes Internet, también se refiere a un nodo de conmutación en la arquitectura X.25. Usualmente, el PSN es un DCE (Data Communication Equipment: Equipo de comunicación de datos) que permite conexión a un DTE (Data Terminal Equipment: Equipo terminal de datos). El acr•2nimo se también se usa comunmente como expansión de "packet-switched network": red de paquetes conmutados.

PSTN *Public Switched Telephone Network:* Red pública telefónica conmutada. Se refiere a la red telefónica.

PU *Physical Unit:* Unidad física. Componente SNA que maneja los recursos físicos de un nodo, como lo pide un SSCP. Existe un PU por nodo.

PVC *Permanent Virtual Circuit:* Circuito permanente virtual. En forma genérica se refiere a un circuito virtual establecido en forma permanente. Los PVC ahorran ancho de banda asociado con el establecimiento y eliminación del circuito en situaciones en donde ciertos circuitos virtuales deben existir todo el tiempo.

Q

QOS *Quality of service:* Calidad del servicio. Medida del desempeño de un sistema de transmisión que considera la calidad de la transmisión y la disponibilidad del servicio.

Query Pregunta. Mensaje usado (usualmente en un protocolo de pregunta-respuesta) para preguntar el valor de alguna variable o serie de variables.

Queueing theory Teoría de colas. Pricipios científicos que gobiernan la formación o falta de formación de congestionamiento en una red o en una interfaz.

R

RDI Red Digital Integrada de Telmex (Telefónos de México)

Reassembly Reensamble. La reconstitución de un datagrama IP en el destino luego de que se fragmentó en la fuente o en un nodo intermedio.

Redirect Redirigir. Parte de los protocolos ICMP y ES-IS que permite a un enrutador avisar a la máquina anfitriona que sería más efectivo usar otro enrutador.

Redirector Redirector. Software que intercepta los pedidos de recursos en una computadora y analiza sus requerimientos de acceso remoto. Si hace falta acceso remoto para satisfacer el pedido, el redirector forma una RPC y la manda al protocolo de software de las capas inferiores para que se transmita en la red hasta el nodo que puede satisfacer el pedido.

Redistribution Redistribución. El permitir que la información de enrutamiento descubierta mediante algún protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento.

Redundancy Redundancia. En telefonía, es la parte de la información total contenida en un mensaje que se puede eliminar sin pérdida de información o significado esencial. En computación, son los elementos múltiples (redundantes) de un sistema que efectúan la misma función.

Relay Relevador. Terminología OSI para el dispositivo que conecta dos o más redes o sistemas de redes. Un relevador de la capa 2 es un puente. Un relevador de la capa 3 es un enrutador.

Remote bridge Puente remoto. Puente que conecta segmentos físicamente diferentes de la red mediante enlaces WAN.

Repeater	Repetidor. Dispositivo que regenera y propaga señales eléctricas a entre dos segmentos de la red.
RFC	Request For Comments. Documentos utilizados como el medio principal para proporcionar la información acerca de del Internet.
RG-58	Cable coaxial de 50 Ohms de impedancia. Es empleado por 10BASE2 de IEEE 802.3.
RG-62	Cable coaxial de 93 Ohms de impedancia. Es empleado por ARcnet.
Ring group	Grupo de anillo. Conjunto de interfaces Token Ring en uno o en más enrutadores Cisco, que son parte de una red Token Ring con puentes.
Ring latency	Espera en el anillo. Tiempo requerido para que una señal se propague una vez alrededor de un anillo en una red Token Ring o IEEE 802.5.
Ring topology	Topología de anillo. Topología en la que la red consiste en una serie de repetidores conectados entre sí por enlaces de transmisión unidireccional para formar un anillo cerrado único. Cada estación en la red se conecta con un repetidor.
RIP	Routing Information Protocol. Un protocol IGP proporcionado con los sistemas Unix de Berkeley. El IGP más común en el Internet utiliza "hop count" como métrica y la métrica más grande permitida por RIP es 16.
RISC	Reduced Intruction Set Computer. Nueva generación de procesadores de conjunto de instrucciones reducidas y qite ejecutan una o más instrucciones por cada ciclo de reloj.
RJ-11	Conectores estándar de 4 hilos para líneas telefónicas.
RJ-45	Conectores estándar de 8 hilos para redes 1BASE5 de IEEE 802.3 (StarLAN). También usan se usan como líneas de telefóno en algunos casos.
RJ45	Conector estándar de 8 hilos para redes IEEE 802.3 1 Base 5 (redes estrella). También utilizado en líneas telefónicas en algunos casos.
Rlogin	Programa de emulación de terminales, similar a Telnet, que se ofrece en la mayoría de los sitemas Unix.
Route processor	Procesador de ruta. En la arquitectura de hardware Cisco, es una tarjeta de procesador que determina rutas y ejecuta procesos de configuración, seguridad, contabilidad, correción de errores y manejo de red. También es llamado procesor supervisor. El equipo CSC/3 es un procesador de ruta.
Routed protocol	Protocolo enrutado. Protocolo que puede ser enrutado por un enrutador. Para enrutarlo, el enrutador debe entender la interconexión lógica entre redes como la percibe el protocolo. Ejemplos de protocolos enrutados incluyen DECnet, Apple Talk e IP.
Router	Enrutador. Dispositivo de la capa 3 OSI que puede decidir cuál de varios caminos debe seguir el tráfico de la red, basándose en alguna métrica óptima. También se conoce como gateway: servidor de intercomunicaciones (aunque esta definición de gateway ya casi no se usa). Los enrutadores envían paquetes de una red a otra, basados en la información de la capa de red.
Routing	Enrutamiento. Proceso de encontrar un camino hacia el anfitrión de destino. En las grandes redes el enrutamiento es muy complejo debido a los muchos destinos intermedios potenciales que un paquete puede alcanzar antes de llegar a su anfitrión de destino.
Routing bridge	Puente enrutador. Puente de la capa MAC que usa métodos de la capa de red para determinar la topología de la capa dered.
Routing protocol	Protocolo de enrutamiento. Protocolo que hace enrutamiento mediante la implantación de un algoritmo específico. Ejemplos de protocolos de enrutamiento son RIP, OSPF e IGRP.

Routing table Tabla de enrutamiento. Tabla almacenada en un enrutador o en algún otro dispositivo de las redes, que lleva cuenta de las rutas (y, en algunos casos, de su métrica) hacia destinos particulares en la red.

Routing update Actualización de enrutamiento. Mensaje enviado desde un enrutador para indicar el grado de enlace de la red y la información de costos asociada. Las actualizaciones de enrutamiento sualen enviarse a intervalos regulares, y luego de un cambio en la topología de la red.

RS-232 Interface física popular, virtualmente idéntica a la especificación V.24.

RS-232C Interfaz de capa física bastante popular. Es virtualmente idéntica a la especificación V.24.

RS-422 Realización eléctrica balanceada de RS-449 para transmisión de datos a alta velocidad.

RS-423 Realización eléctrica no balanceada de RS-449 para compatibilidad con RS-232C.

RS-449 Interfaz de capa física bastante popular. Se trata esencialmente de una versión más rápida (hasta 2 Mbps) de RS-232C con capacidad de manejar cables más largos.

RTMP *Routing Table Maintenance Protocol:* Protocolo de mantenimiento de tablas de rutas. Protocolo de enrutamiento propio de las computadoras Apple. Es un derivado de RIP.

RUB *Router hub:* Concentrador-enrutador. Producto que será desarrollado en forma conjunta por Cisco y SynOptics Communications y que combina las capacidades de un enrutador y de un concentrador.

S

Sampling rate tasa de muestreo. Tasa a la cual se toman muestras de la amplitud de alguna forma de onda en particular.

SAP Service Access Point. Una interface entre los niveles OSI.

Satellite communications Comunicaciones por satélite. Uso de satélites en órbita geoestacionaria para transmitir datos entre múltiples estaciones terrenas. Las comunicaciones por satélite ofrecen gran ancho de banda, costo no relacionado con la distancia entre las estaciones terrenas, retardos de propagación relativamnete grandes, y capacidad de difusión (broadcast).

SDLC *Synchonous Data Link Control:* Control sincrónico de enlace de datos. Protocolo IBM sincrónico por bits de la capa de enlace que ha dado lugar a numerosos protocolos similares, incluyendo HDLC y LAPB.

SDLC transport Transporte SDLC. Característica de los enrutadores Cisco mediante la cual es posible integrar diferentes entornos en una sola red empresarial amplia de alta velocidad. Los enrutadores Cisco pueden hacer pasar el tráfico SDLC original a través de enlaces serie de punto a punto, y multiplexan el demás tráfico de protocolo sobre los mismos enlaces. Esos enrutadores también pueden encapsular marcos SDLC dentro de datagramas IP para transportarlos a redes arbitrarias (que no sean SDLC).

Security management Manejo de la seguridad. Una de las cinco categorías de manejo de redes definida por ISO para el manejo de redes OSI. Los subsistemas de manejo de la seguridad son responsables de controlar el acceso a los recursos de la red.

Segment Segmento. Término usado en la especificación de TCP para describir una unidad de información de la capa de transporte.

Serial transmission Transmisión serie. Método de transmisión en el cual los bits del caracter de datos se transmiten secuencialmente en un canal. Vease paralell transmission.

Server	Servidor. Nodo o programa de software que ofrece servicios a un cliente. Vease back end y client.
Session	Sesión. Conjunto de transacciones relacionadas que suceden entre dos o más dispositivos de la red. En SNA, es una conexión lógica que permite a dos unidades NAU comunicarse entre sí.
Session layer	Capa de sesión. Capa 5 del modelo de referencia OSI. Coordina las actividades de la sesión entre aplicaciones, incluyendo control de errores del nivel de aplicación, control de dialogos y llamadas remotas a procedimientos.
Shielded cable	Cable blindado. Cable con una capa de aislamiento para reducir la interferencia electromagnética (EMI).
Shortest path routing	Enrutamiento de camino mínimo. Enrutamiento que mediante la aplicación de un algoritmo minimiza el costo de la distancia o de la trayectoria.
Single mode fiber	Fibre de modo único.Fibra de diámetro relativamente angosto, a través de la cual sólo se propaga un modo. Tiene un ancho de banda mayor que la fibra multimodal, pero requiere una fuente de luz de espectro reducido (por ejemplo, un laser).
SLIP	Serial Line Internet Protocol. Utilizado para correr IP en lineas seriales como telefónicas.
SMTP	Simple Mail Transfer Protocol. Un protocolo Internet que proporciona servicios de correo electrónico.
SNA	*System Network Architecture:* Arquitectura de redes de sistemas. Arquitectura grande, compleja y con múltiples características, desarrollada en la década de 1970 por IBM. Systems Network Architecture. La definición de IBM de como deben ser manejadas las comunicaciones entre sistemas y otros sistemas o terminales remotas.
SNMP	Simple Network Management Protocol. Un protocolo de alto nivel basado en estándares para la administración de la red, generalmente utilizado en redes TCP/IP.
Socket	Receptáculo. Estructura de software que opera como punto final de comunicaciones en un dispositivo de red.
Solaris	Sistema operativo de Sun Microsystems, tiende a reemplazar al SunOS, este sistema está basado en system VR4.
Source address	Dirección fuente. Dirección de un dispositivo de la red que hace envíos.
Source-route translational bridging	Puenteo de rutas fuente con traducción. A veces conocido como SR/TLB, es un método de puenteo en el cual las estaciones de rutas pueden comunicarse con estaciones de puente transparentes con el auxilio de un puente intermedio que traduce entre los dos protocolos de puenteo.
Source-route transparent bridging	Puenteo transparente de rutas fuente. Esquema de puenteo propuesto por IBM, que intenta reunir las dos estrategias prevalecientes de puenteo (transparente, y de rutas fuente). SRT, como a veces se le conoce, emplea ambas tecnologías en un mismo dispositivo para satisfacer las necesidades de todos los nodos finales. No se hace traducción entre los protocolos de puenteo, a diferencia de lo que sucede con source-route translational bridging (SR/TLB).
Source-route bridging	Puenteo de rutas fuente. Método de puenteo originado por IBM en el cual la ruta completa a un destino se predetermina en tiempo real antes del envío de datos al destino. Esto es en contraste con transparente bridging: puenteo transparente, en donde el puenteo ocurre trayecto (hop) por trayecto. También conocido por las siglas SRB, es más popular en las redes Token Ring.

Span	Tramo. Línea de transmisión digital full duplex entre dos medios digitales.
Spanning tree	Arbol abarcador. Subconjunto sin ciclos de la topología de una red.
Spanning tree algorithm	Algoritmo de arbol abarcador. Algoritmo, cuya versión original fue inventada por DEC, usado para impedir ciclos de puenteo mediante la creación de un arbol abarcador. Está documentado en la especificación IEEE 802.1d, aunque en realidad el algoritmo de DEC y el algoritmo IEEE 802.1d no son el mismo ni son compatibles.
SPARC	Scalable Processor Architecture. Procesador diseñado por Sun Microsystems de arquitectura RISC.
Spooler	Aplicación que maneja pedidos o trabajos que se le pasan para su atención. Los pedidos recibidos se procesan en forma ordenada a partir de una cola. El print spooler (sistema de colas de impresión) es tal vez el ejemplo más común. [N. del T. SPOOL es el acrónimo de Simultaneus Peripheral Operations On Line: Operación simultánea de periféricos en línea.]
SRB	Source Route Bridging. Método de puenteo original de IBM, donde la ruta completa a un destino es predeterminada, en tiempo real antes del envío de los datos al destino. Contrasta con el "transparent bridging" que es llevado a cabo por "hop count". SRB es más popular en las redes TokenRing.
STACK	Término empleado para referirse a los niveles o capas de los protocolos.
Standard	Estándar. Conjunto de reglas o procedimientos comúnmente usados o especfficados oficialmente.
Star topology	Topología de red. Topología LAN en la cual los puntos finales de la red se conectan a un conmutador central mediante enlaces de punto a punto.
Star-stop transmission	Transmisión de arranque-parada. Veáse asynchronous transmission.
StarLAN	Otro nombre para 1BASE5 de IEEE 802.3. Es una red local LAN CSMA/CD promulgada por AT&T.
Static route	Ruta estática. Ruta que se ingresa manualmente en la tabla de rutas.
Store and forward	Almacena y envía. Técnica de conmutación de mensajes en la cual éstos se almacenan temporalmente en puntos intermedios entre la fuente y el destino, hasta que llegue el momento en que haya recursos de la red (como por ejemplo enlaces libres) disponibles para su envío.
STP	Shielded Twisted Pair.
Subarea node	Nodo de subárea. Controlador de comunicaciones o anfitrión SNA que maneja direcciones completas de la red.
Subarea.	Subárea. Porción de una red SNA que consiste en un nodo de subárea y sus enlaces y nodos periféricos asociados.
Subnet mask	Máscara de subred. Máscara de direcciones de 32 bits usada en IP para especificar una subred en particular.
Subnetwork Subred	Término empleado a veces para referirse a un segmento de la red. En redes IP es una red que comparte una dirección de subred particular. En redes OSI es un conjunto de ES e IS bajo el control de un dominio administrativo único, y que emplea un único protocolo de acceso a la red.
SunNet	Software de administración de redes TCP/IP que junto con el OpenView son los líderes en el mercado.
SunOS	Sistema operativo de Sun Microsystems, se ha caracterizado por ser uno de los mejores Unix derivados de Berkeley, además soporta el system V.

SVC — *Switched Virtual Circuit:* Circuito virtual conmutado. Circuito virtual que puede establecerse en forma dinámica por demanda. Se contrasta con PVC.

Switch processor — Procesador de conmutación. En la arquitectura de hardware Cisco, es una tarjeta de procesador de un bit (bit-slice) que actúa como administrador de todas las actividades del cBus. También se conoce como cBus controller.

SYBASE — Base de Datos Relacional. Se ha convertido en una de las bases de datos líderes en el mercado por su origen que fue diseñado para trabajar en cliente-servidor y sistemas abiertos.

Synchronization — Sincronización. El establecimiento de tiempos en común para el emisor y el receptor.

Synchronous transmission — Transmisión sincrónica. Operación de un sistema de red en donde los acontecimientos suceden en tiempos precisos.

T

T-carrier — Portadora-T. Método de transmisión de multiplexación por división de tiempo que usualmente se refiere a una línea o cable que lleva una señal DS-1.

T-connector — Conector-T. Dispositivo en forma de T con dos conectores BNC hembra y uno macho.

T1 — Termilogía Bell que se refiere a un sistema de portadora digital usada para la transmisión de datos a través de la jerarquía telefónica.

T3 — Servicio digital WAN que opera a 44 Mbps.

TAC — *Terminal Access Controller:* Controlador de acceso a las terminales. Anfitrion Internet que acepta conexiones terminales de líneas conmutadas.

TACACS — *Terminal Access Controller Access System:* Sistema de acceso al controlador de acceso a las terminales. sistema desarrollado por la comunidad de la red de datos de la defensa de los Estados Unidos para controlar el acceso a sus TAC. Los producto Cisco lo manejan.

TCP/IP — *Transmission Control Protocol/Internet Protocol:* Protocolo de control de transmisiones/Protocolo Internet. Los dos protocolos Internet más conocidos, que erroneamente suelen confundirse con uno solo. TCP corresponde a la capa 4 (capa de transporte) del modelo de referencia OSI y ofrece transmisión confiable de datos. IP corresponde a la capa 3 (capa de red) del modelo de referencia OSI, y ofrece servicios de datagramas sin conexión. TCP/IP fue desarrollado por el Departamento de la Defensa de los Estados Unidos en los años 70 como apoyo a la construcción de interconexión de redes a escala mundial.

TCU — *Trunk Coupling Unit:* Unidad de acoplamiento troncal. En redes Token Ring, es un dispositivo físico que conecta una estación al cable troncal.

TDM — *Time Division Multiplexing:* Multiplexaje por división de tiempo. Técnica en la que puede asignarse ancho de banda a información de múltiples canales en un solo cable, basándose en distribución de intervalos de tiempo.

Telecommunications — Telecomunicaciones. Término referido a las telecomunicaciones (que normalmente involucran sistemas de cómputo) en la red telefónica.

TELENET — Red pública para transporte de datos. Una de las más grandes en Estados Unidos.

TELMEX — Proveedor en México de las líneas públicas y privadas de comunicaciones.

Terminal emulation	Emulación de terminales. Aplicación usual de redes en la cual una computadora ejecuta programas que la hacen aparecer, ante una máquina anfitriona de la red, como si fuera una terminal simple conectada directamente.
Terminal server	Servidor de terminales. Procesador de comunicaciones que conecta dispositivos asincrónicos a una red LAN o WAN mediante software emulador de terminales y de redes.
TERMINAL UNIVERSAL	Modelo que permite la presentación de diferentes ambientes operativos utilizando una interface única.
Terminator	Terminador. Resistencia eléctrica al final de una línea de transmisión, que absorbe las señales, evitando así que reboten y sean oídas de nuevo por las estaciones de la red.
TFTP	*Trivial File Transfer Protocol:* Protocolo trivial de transferencia de archivos. Versión simplicada de FTP que permite transferencia de archivos de una computadora a otra de la red. THC over X.25THC sobre X.25. Característica que ofrece transmisión de encabezados TCP/IP en líneas X.25 para propositos de eficiencia en los enlaces.
Throughput	Producción, trabajo útil. Cantidad de información que llega, y posiblemente pasa, a un punto particular en un sistema de red.
Time-out	Suspensión por tiempo terminado. Acontecimiento que ocurre cuando un dispositivo de la red espera escuchar a otro dentro de un período especificado, pero eso no sucede. La suspensión resultante normalmente causa una retransmisión de la información o bien la disolución del circuito virtual entre los dos dispositivos.
Token	Ficha. Marco (frame) de información de control cuya posesión da a un dispositivo de la red el derecho a transmitir.
Token bus	Arquitectura de red LAN que emplea acceso tipo token passing en la topología de bus. Esta arquitectura es la base de la especificación LAN IEEE 802.4.
Token passing	Paso de fichas. Método de acceso en el cual los dispositivos de la red tienen acceso al medio físico en un orden definido por la posesión de un pequeño marco (frame) llamado token (ficha).
TOKENRING	Red de área local basada en el estándar IEEE 802.5 en el cual las estaciones son conectadas serialmente para formar un anillo con acceso controlado por el Token.
Topology	Topología. Arreglo físico de los nodos y el medio de la red dentro de una estructura empresarial de red.
Trailer	Elemento de la cola. Información de control añadida a los datos en un paquete.
Transaction	Transacción. Unidad de procesamiento de comunicaciones orientada hacia los resultados.
Transaction services layer.	Capa de servicios de transacciones. Capa 7 en el modelo de arquitectura SNA. Veáse application layer.
Transceiver	Transmisor/receptor. Veáse MAU.
Transceiver cable	Cable transmisor/receptor. Veáse drop cable y AUI.
Transit bridging	Puenteo de tránsito. Puenteo que emplea encapsulamiento para enviar un marco (frame) entre dos redes similares, pasando por una red diferente.
Translation bridging	Puenteo con traducción. Puenteo entre redes con protocolos de subcapa MAC diferentes.
Transmission control layer.	Capa de control de transmisiones. Capa 4 del modelo de arquitectura SNA. Es la responsable de establecer, mantener y terminar las sesiones SNA, de secuenciar los mensajes de datos, y del flujo de control de la sesión.

Transmission group Grupo de transmission. En enrutamiento SNA, es uno o más enlaces paralelos de comunicación que se tratan como una entidad de comunicaciones.

Transparent bridging Puente transparente. Esquema de puenteo preferido por redes Ethernet y IEEE 802.3, en el cual los puentes pasan los marcos un trayecto (hop) a la vez, basados en tablas que asocian nodos terminales con puertos del puente. Se llama así porque la presencia de los puentes es transparente para los nodos terminales de la red.

Transport layer Capa de transporte. Capa 4 del modelo de refencia OSI. Es la responsable de la comunicación confiable entre nodos terminales de la red. Realiza los controles de flujo y de errores y suele usar circuitos virtuales para asegurar entrega confiable de datos.

Traps Trampas. Mensajes no solicitados enviados por un agente SNMP a un sistema de manejo de red (NMS) que indican la ocurrencia de un acontecimiento significativo.

Tree topology Topología de árbol. Topología LAN similar a la de bus, excepto que las redes tipo árbol sí pueden conectar ramas. Como en la topología de bus, las transmisiones de una estación se propagan por todo el medio y son recibidas por todas las otras estaciones.

TRouter Producto de Cisco capaz de dar servicio de enrutador y de terminal.

Trunk Troncal. Canal de transmisión que conecta dos dispositivos de conmutación.

Twisted pair Par trenzado. Medio de transmisión de relativa baja velocidad que consiste en dos cables aislados, en forma de espiral. Los cables pueden o no estar blindados. Es muy común en aplicaciones de telefonía y cada vez más usual en redes de datos.

U

UDP User Datagram Protocol. Protocolo de nivel 4 sin conexión que pertenece a la familia de protocolos de Internet.

Unbalanced configuration Configuración desbalanceada. Configuración HDLC con una estación primaria y múltiples estaciones secundarias.

Unicast address la red.

Unipolar Unipolar. Literalmente significa una sola polaridad. Es la característica eléctrica fundamental de señales internas en los equipos de comunicacion digitales. En contraste con bipolar.

UNIX Sistema operativo multiusuario y multitasking, ideal para una ambiente de red en cliente-servidor, ha sido el sistema que ha marcado el rumbo de los sistemas abiertos.

Unnumbered frames Marcos sin numeración. Marcos HDLC usados para propositos de mantenimiento, incluyendo el arranque y terminación de enlaces y la especificación de nodos.

UTP Unshielded Twisted Pair. Tipo de cable utilizado en las instalaciones con redes LAN y sistemas de cableado estructurado.

V

V.24 Interfaz de capa física comunmente empleada en muchos países. Muy similar a EIA-232D y RS-232C.

Vector Vector. Segmento de datos de un mensaje SNA. Etsá compuesto por un campo de longitud, una llave que describe el tipo de vector, y los datos específicos del vector.

Virtual route Ruta virtual. Terminología SNA para circuito virtual. Es una conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita particular.

W

WAN Wide Area Network. Una red grande de expansión geográfica entre dispositivos en un ambiente regional, nacional o internacional.

Wideband Banda amplia. Veáse broadband.

WINDOWS NT Sistema operativo de Microsoft para la inicativa de ACE (Advanced Computing Environment)

Wiring closet Cuarto de conexiones. Cuarto diseñado específicamente para el cableado de redes de voz y datos. Sirve como punto de unión para los cables y equipo que se usan para interconectar dispositivos.

WORD Software de Microsoft para el procesamiento de texto.

X

X Windows Sistema gr•Ofico y de ventanas distribuido, multitarea, Independiente de los dispositivos, y transparente a la red, originalmente desarrollado por el MIT para comunicaciones entre terminales X y estaciones de trabajo UNIX.

X.21 Una recomendación de la CCITT que define un protocolo para la comunicación entre una red de circuito conmutado y un dispositivo de usuario.

X.25 Recomendación CCITT que define el formato de los paquetes para transferencia de datos en redes públicas de datos. Muchos establecimientos tienen redes X.25 que les dan acceso a terminales remotas. Esas redes se pueden usar para otros tipos de datos, incluyendo los protocolos Internet, DECnet y XNS.

X.28 Una recomendación de CCITT que define la interface de terminal PAD.

X.29 Una recomendación de CCITT que define la interface de terminal PAD.

X.3 Una recomendación de CCITT que define varios parámetros de PAD.

X.400 Una recomendación de CCITT que especifica un estándar para transferencia de correo electrónico.

X.500 Una recomendación de CCITT que especifica un estándar para el mantenimiento de archivos y directorios.

X11 Un sistema de ventanas estándar del nivel 7 de aplicación del modelo OSI.

X3T9.5 Número asignado al grupo de trabajo del comité de acreditación de estándares para su documento interno de trabajo que describe la interfaz de datos distribuida por fibra. Veáse FDDI.

XNS Xerox Network Systems. Un conjunto de protocolos originalmente diseñado por Xerox. Muchas compañias como Ungermann-Bass, Novell, Banyan y 3Com, utilizaron o actualmente utilizan una variante de XNS como su "stack" principal de protocolos.

XRemote Protocolo desarrollado específicamente para optimizar el manejo de X Windows en enlaces de comunicación serie.

XTI X/Open Transport Interface. es un API (independiente del "stack" de la red).

XWindows Sistema de ventanas desarrollado por el MIT en el proyecto Athena.

APENDICES

APENDICES

APENDICE A - Configuración Enrutador de Varsovia

```
!
hostname ciscotr
!
enable-password net
!
!
!
!
no ip forward-protocoll udp
!
novell routing 000.0c06.3ce9
!
!
source-bridge ring-group 10                    Configuración SRB
source-bridge remote-peer 10 tcp 140.240.30.1        para el anillo virtual
source-bridge remote-peer 10 tcp 140.240.10.1
!
stun peer-name 140.240.30.1                    configuración Serial Tunel
stun protocol-group 100 sdlc                   para los controladores
stun protocol-group 101 sdlc                   de terminales
stun protocol-group 102 sdlc
stun protocol-group 103 sdlc
stun protocol-group 104 sdlc
stun protocol-group 105 sdlc
!
!
interface TokenRing 0
description CONTROLADOR SYNOPTICS ANILLO 1
ip address 200.0.10.18 255.255.255.0
ring-speed 16
novell network 801
novell helper-list 901
novell helper-address - 1.ffff.ffff.ffff
clns mtu 8136
!
interface TokenRing 1
description ANILLO DE RECURSOS
ip address 140.240.30.1 255.255.255.0
ring-speed 16
novell network 810
clns mtu 8136
source-bridge 2 1 10                  Anillo que participa en el SRB
source-bridge spanning                     para formar el anillo virtual
```

```
multiring all
!
interface TokenRing 2
description CONCENTRADOR SYNOPTICS ANILLO 2
ip address 200.0.8.18 255.255.255.0
ring-speed 16
novell network 803
novell helper-list 901
novell helper-address - 1.ffff.ffff.ffff
clns mtu 8136
!
interface TokenRing 3
description CONCENTRADOR SYNOPTICS ANILLO 3
ip address 200.0.11.18 255.255.255.0
ring-speed 16
novell network 805
!

interface Ethernet 0
description RED DE ANALISIS
ip address 200.0.0.147 255.255.255.0
novell network AA
no mop enabled
!
interface Serial 0
description SOS1-CTRL          Controlador de terminales
no ip address
encapsulation stun
stun group 100
stun route address 4 tcp 140.240.10.1
stun route address 3 tcp 140.240.10.1
stun route address 2 tcp 140.240.10.1
clockrate 19200
!
interface Serial 1
description SOS2-CTRL          Controlador de terminales
no ip address
encapsulation stun
stun group 101
stun route address 3 tcp 140.240.10.1
stun route address 2 tcp 140.240.10.1
clockrate 19200
!
interface Serial 2
description SOS3-CTRL          Controlador de terminales
```

```
no ip address
encapsulation stun
stun group 102
stun route address 2 tcp 140.240.10.1
stun route address 3 tcp 140.240.10.1
clockrate 19200
!
interface Serial 3
description CTRL-BMV            Controlador de terminales
no ip address
shutdown
encapsulation stun
stun group 103
stun route address 1C tcp 140.240.10.1
!
interface Serial 4
description CTRL-MONTERREY I        Controlador de terminales
no ip address
encapsulation stun
stun group 104
stun route address C1 tcp 140.240.10.1
!
interface Serial 5
description CTRL-MONTERREY II           Controlador de terminales
no ip address
shutdown
encapsulation stun
stun group 105
stun route address 2 tcp 140.240.10.1
clockrate 19200
!
interface Serial 6                  Enlace de Guadalajara
description SATELITE GUADALAJARA        Controlador de terminales
ip address 140.240.28.2 255.255.255.0
bandwidth 32
keepalive 4
shutdown
!
interface Serial 7
no ip address
shutdown
encapsulation stun
stun group 104
stun sdlc-role primary
sdlc address C1
```

```
stun route address C1 tcp 140.240.10.1
!
interface Serial 8
no ip address
keepalive 4
shutdown
!
interface Serial 9
no ip address
keepalive 4
shutdown
!

interface Serial 10                    Enlace red Bancomer
description TIMEPLEX 6-A
ip address 140.240.20.2 255.255.255.0
bandwidth 64
keepalive 4
!
interface Serial 11
description TIMEPLEX 6-B
ip address 140.240.21.2 255.255.255.0
bandwidth 64
keepalive 4
!
interface Serial 12                    Enlace red RDI Telmex
description Enlace MEGAMUX (R.D.I)
ip address 140.240.22.2 255.255.255.0
bandwidth 307
keepalive 4
novell network 1A
novell output-stap-filter 1000
!
interface Serial 13                    Enlace red Guadalajara
description ENLACE GUADALAJARA (R.D.I.)      por RDI de Telmex
ip address 140.240.23.2 255.255.255.0
bandwidth 115
keepalive 4
novell network 2A
novell output-sp-filter 1000
!
!
router igrp 10
timers basic 5 15 15 30
no metric holddown
```

```
network 140.240.0.0
netwrok 200.0.8.0
network 200.0.9.0
passive-interface TokenRing0
passive-interface TokenRing2
!
!
!
!
!

!
ip name-server 255.255.255.255
ip host PLATINO 140.240.10.1
ip host GUADALAJARA 140.240.23.1
ip host GUA 140.240.28.1
ip host PLA 140.240.20.1
snmp-server community
snmp-server community public RW
access-list 901 permit 0 803 5252
access-list 901 permit 0 801 5252
access-list 1000 deny FFFFFFFF 30C
access-list 1000 deny FFFFFFFF 47
access-list 1000 permit FFFFFFFF
!
!
line vty 0 4
login
line con 0
exec-timeout 0 0
line aux 0
line vty 0
exec-timeout 5 0
password net
line vty 1
exec-timeout 5 0
password net
line vty 2
exec-timeout 5 0
password net
line vty 3
exec-timeout 5 0
password net
line vty 4
exec-timeout 5 0
```

```
password net
!
end
```

APENDICE B - Arquitectura del ruteador AGS+

El AGS+ incorpora una arquitectura de multiprocesador la cual emplea un diseño que se ha llamado Palabra de Instrucción Muy Larga (VLIW) además del Bus de rápida conmutación de Cisco para enviar el potencial de proceso y el ancho de banda necesario para dar soporte a enlaces de alta velocidad múltiples. Las características clave de la arquitectura de Cisco incluyen las siguientes:

- El diseño de la VLIW facilita la ejecución de operaciones múltiples y paralelas, en un mismo ciclo de reloj, permitiendo un mayor *throughput.*
- Un Bus con estructuras de alta velocidad y caches permiten el rápido envío de paquetes necesario para enrutar entre múltiples interfaces de FDDI y redes Ethernet interconectadas.
- Procesadores distribuídos, con capacidad de 16 millones de instrucciones por segundo (MIP) e interfaces de enlace, manejan medios específicos (como: fibra óptica, coaxial grueso) y optimizan el ruteo del tráfico. Estos procesadores, junto con el microcódigo de ruteo de paquetes de Cisco, facilitan la operación eficiente de las funciones del software tales como construir marcos de información dependientes del medio y del protocolo, así como conmutar información de una interface a otra.
- El controlador del Bus de Cisco dirige todas las actividades del Bus y proporciona memoria para una precisa sincronicación del proceso.

Bus de alto desempeño

El trasfondo de alto desempeño del Bus del AGS+, en combinación con el switcheo independiente entre los procesadores de las interfaces, proporciona una tasa de switcheo sostenida sobre un 1/2 Gbps entre las múltiples interfaces Ethemet, FDDI, y otros medios de alta velocidad.

Un sistema de bus estándar maneja la interacción entre interfaces de red de menor densidad, tales como las Ethernet, Token Ring, e interfaces seriales síncronas, y el procesador del sistema y monitor del medio ambiente.

Confiabilidad

Para asegurar que el AGS+ contribuya a la confiabilidad general de la red, cada AGS+ incluye una tarjeta monitora que lo protege de condiciones de alta temperatura o un sobrevoltaje monitoreando continuamente el flujo de aire, la temperatura, y el voltaje del sistema.

Se ha diseñado una confiabilidad más amplia en el software de Cisco para asegurar una operación contínua de la red. Las características de ruteo alterno y de distribución de carga aseguran que la información es ruteada a través del camino más eficiente. Además, todo el software de Cisco incluye comandos para el sistema de administración que permite a los administradores monitorear fácilmente y detectar una falla específica de la red.

Administración local y remota de la red

Los administradores de la red pueden monitorear y controlar el AGS+ desde una terminal local, o sobre la red desde ubicaciones remotas, utilizando el protocolo de operación de mantenimiento (Maintenance Operation Protocol) ya sea de Telnet o de DEC.

El AGS+ incluye una base de información de administración estándar (Management Information Base), el cual es agente del protocolo SNMP. El agente SNMP del AGS+ incluye un conjunto extendido de variables MIB que pueden ser consultados por cualquier estación de administración SNMP de la red.

Puenteo y ruteo multiprotocolo

Una de las consideraciones principales para todos los dispositivos de interconexión son los protocolos de comunicación. Como en los capítulos anteriores ya se ha tocado el punto con mayor profundidad, sólo haremos algunos comentarios al respecto.

Entre los comentarios sobresalientes debemos recordar la necesidad de integrar diversos ambientes y protocolos, por lo que es necesario que entre las características del equipo que se considerará el corazón de la WAN, se encuentre la de poder manejar diversos protocolos, es decir sea multiprotocolo.

Los enrutadores AGS+ de Cisco Systems, son computadoras de red multiprotocolo que proporcionan todas las funciones de un "puente externo" de Novell, además de un buen número de capacidades de conexión para redes de área tanto local como amplia. Los enrutadores Cisco incluyen la habilidad para conectar múltiples redes Ethernet, Token Ring y FDDI (Interface de Datos Distribuídos por Fibra), ya sea directamente o a través de líneas seriales de alta velocidad (hasta una razón de T1/E1) o redes de paquetes de datos X.25.

Para profundizar un poco en el punto del manejo de múltiples protocolos, podemos tomar como caso de estudio la forma en que los enrutadores Cisco enrutan el protocolo Novell IPX, (Internet Packet eXchange que es el protocolo de Novell en el nivel OSI de red). Existe una discrepancia entre el formato de un paquete IPX y de otro correspondiente al estándar IEEE 802.3. Novell no incluye la información de IEEE 802.2 en sus paquetes. La consecuencia de esta decisión (tomada antes de la estandarización oficial de IEEE 802.2) es que los dispositivos de IEEE 802.3 sobre una red, no puedan interpretar los paquetes Novell dado que ellos esperan la información de los 802.2 siguiendo inmediatamente al campo de "longitud". En algunas implementaciones, los paquetes son simplemente descartados sin efectos dañinos, exceptuando algunos ciclos de CPU desperdiciados. En otras implementaciones, es posible para el paquete Novell dañar algunas partes internas de algún dispositivo del tipo 802.3.

Los enrutadores Cisco no son confundidos por el desorden de la información en los paquetes de IPX.. El ruteo de IPX es manejado de manera simple y fácil al encontrar correctamente el campo de la "red destino", decodificando su contenido, y ruteando el paquete congruentemente. Un enrutador Cisco puede apreciar la diferencia entre un paquete IPX y otro paquete perteneciente al estándar 802.3, de tal manera que puede manejar efectivamente el ruteo del protocolo IPX en un ambiente multiprotocolo.

El AGS+ puede concurrentemente rutear y puentear tráfico de la red, y es capaz de soportar simultáneamente más de 20 de los protocolos de comunicaciones más ampliamente usados hoy en día. Los protocolos soportados con el software estándar incluyen: OSI, TCP/IP, DECnet Phase IV y Phase V, XNS, Novell IPX, Banyan VINES, 3Com 3+, Apple Talk Phase 1 y Phase 2, Apollo Domain, y transporte SDLC para ambientes SNA. Las opciones de software proporcionan soporte para DDN X.25, X.25, Frame Relay y redes SMDS.

El AGS+ soporta una gran variedad de interfaces para WAN y diferentes servicios, incluyendo líneas privadas, servicios de conmutación de circuitos y de conmutación de paquetes. El AGS+ puede ser equipado con interfaces seriales síncronas capaces de transmitir datos a razones de hasta 52 Mbps y permitiendo acceso a servicios de 9.6, 48, 56, 64, y 384 Kbps, así como servicios de T1 (1.544 Mbps), E1 (2.048 Mbps), y T1 fraccionales.

El AGS+ no sólo proporciona las interfaces físicas para conectarse a redes de área amplia, sino que incluye el software necesario para explotar los servicios de las redes WAN. Las capacidades clave (entre otras) para el "internetworking" en una WAN soportadas por el enrutador AGS+ de Cisco incluyen:

- Interconexión sobre enlaces punto a punto (point-to-point).
- Servicios de conmutación de paquetes, incluyendo X.25, servicio de conmutación multimegabit de datos (SMDS), y Frame Relay.
- Servicios de conmutación de circuitos, incluyendo redes digitales de servicios integrados (ISDN), interfaz de tasa básica (BRI) e interfaz de tasa primaria (PRI), y servicios de conmutación de circuitos digitales tales como enlaces conmutados a 56 Kbps.
- Establecimiento automático de enlaces por vía telefónica secundarios en el evento de una falla en el enlace primario.
- Múltiples protocolos de WAN corriendo concurrentemente.
- Distribución de la carga sobre cualquier número de enlaces.
- Uso optimizado de las diversas rutas redundantes.
- Compresión de datos.
- Enrutamiento por prioridad.
- Reconocimiento de los diversos dispositivos conectados a la red, por lo que puede realizar la actualización de las tablas de ruteo de forma dinámica.

El AGS+ puede ser conectado a otros rutedores para formar un backbone privado, o puede ser combinado con hardware adicional para proporcionar un backbone para la integración de voz, datos y video.

Además, el AGS+ puede actuar como un gateway entre diversos servicios. Por ejemplo, el AGS+ puede rutear paquetes desde un servicio de Frame Relay a un servicio de SMDS, o a cualquier otra combinación de servicios de WAN soportados.

El AGS+ incluye dos aplicaciones estratégicas para servicios de conmutación de circuitos, estos son la recuperación en caso de desastre y la distribución automática de la carga. Cuando los servicios de conmutación de circuitos se utilizan conjuntamente con líneas privadas punto a punto, el AGS+ puede detectar una "caída de la línea" y automáticamente establecer una línea de respaldo. Similarmente, el AGS+ puede detectar condiciones de sobrecarga, automáticamente accesar a un ancho de banda adicional y distribuir la carga entre las dos líneas. También soporta una amplia variedad de protocolos de WAN. El protocolo High-Level Data Link Control (HDLC) de Cisco, proporciona alto desempeño en los servicios de enlace de punto a punto, mientras da soporte al estándar de la industria (Point to Point Protocol) para proporcionar interoperabilidad a los enrutadores de los diversos fabricantes. El AGS+ soporta también el ruteo multiprotocolo sobre X.25, DDN X.25, protocolo para interface SMDS, Frame Relay, y el control síncrono para enlace de datos (SDLC) de IBM para ambientes bajo la arquitectura de sistemas en red (SNA).

A diferencia de los puentes remotos que dependen exclusivamente del algoritmo de árbol abarcador (Spanning Tree Algorithm) para manejar enlaces redundantes, el AGS+ permite distribuír la carga sobre rutas múltiples para optimizar el ancho de banda disponible. El AGS+ puede así maximizar el uso de los recursos de la WAN que tengan un costo considerable.

En una red basada en enrutadores, el ancho de banda de todos los enlaces en una configuración de rutas redundantes puede ser utilizado continuamente. Los enrutadores no requieren soluciones no-óptimas, tales como el uso de un algoritmo como el Spanning Tree para eliminar ciclos.

Para líneas más lentas, tales como las de 9.6, 48, 56, 64 Kbps y otras, el AGS+ soporta la compresión de datos y el manejo de colas con prioridad. La implementación de Cisco para el algoritmo de compresión de datos reduce el encabezado estándar de TCP/IP de 48 bytes a sólo 8 bytes. Esta reducción resulta en ahorros de costo substanciales, especialmente en transferencias de datos interactivas. En algunas redes, esto puede duplicar efectivamente la capacidad de acarreo de una línea.

Igualmente importante para algunas aplicaciones es el control del tráfico con manejo de colas con prioridad. Cisco soporta 4 niveles de prioridad en colas (alta, mediana, normal y baja). La prioridad en colas puede controlar el tráfico basado en el tipo de protocolo o de interface. El tamaño de la cola y los valores de default para el manejo de paquetes no identificados por el mecanismo de colas pueden ser dados de alta por medio de software. El manejo de colas basado en prioridad es a veces necesario para enlaces de baja velocidad con protocolos sensibles al retardo, y para reducir los cuellos de botella cuando el ancho de banda se encuentra en gran demanda.

APENDICE C - Protocolos utilizados en el ruteador AGS+

A continuación se exponen como ejemplo dos de los protocolos manejados por el enrutador Cisco AGS+ que ayudan para la interconectividad de redes. Debe advertirse al lector que existen otros aparte de éstos.

RIP

Antecedentes

El Protocolo de Información de Ruteo (RIP) es un protocolo de ruteo originalmente diseñado por Xerox donde fue llamado GWINFO y utilizado en la suite de protocolos en los Sistemas de Red de Xerox (XNS). El RIP llego a ser asociado tanto con UNIX como con TCP/IP en 1982 cuando la versión para UNIX de Berkeley empezó a embarcarse con una implementación del RIP a la que se refería como *routed* (pronunciado como "route dee"). Siendo aún un protocolo de ruteo muy popular en la comunidad Internet, el RIP es formalmente definido en la publicación de XNS *Internet Transport Protocols* (1981) y en *Request for Comments* (RFC) 1058 (1988).

El RIP ha sido ampliamente adoptado por los fabricantes de computadoras personales para su uso en los productos de red. Por ejemplo, el protocolo de ruteo de Appletalk (Routing Table Maintenance Protocol, también conocido como RTMP) es una versión modificada del RIP. RIP fue también la base para los protocolos de ruteo de Novell, 3Com, Ungermann-Bass, y Banyan. El RIP de Novell y 3Com es basicamente el RIP estándar de Xerox. Ungermann-Bass y Banyan hicieron modificaciones menores al RIP para servir a sus porpias necesidades.

Formato de la Tabla de Ruteo

Cada entrada en una tabla de ruteo de RIP proporciona cierta variedad de información, incluyendo el último destino, el salto siguiente en el camino al destino, y una *métrica*. La métrica indica la distancia en el número de saltos hacia el destino. Puede estar presente otro tipo de información en la tabala de ruteo, incluyendo por ejemplo los diferentes timers asociados con la ruta. Una tabla de ruteo de RIP típica se muestra a continuación:

Destino	Proximo salto	Distancia	Timers	Banderas
Red A	Enrutador 1	3	11, 12, 13	x, y
Red B	Enrutador 2	5	11, 12, 13	x, y
Red C	Enrutador 3	2	11, 12, 13	x, y

El RIP mantiene sólo la mejor ruta para un destino. Cuando una información nueva proporciona una mejor ruta, esta información remplaza a la anterior. Los cambios en la topología de la red provocan cambios en los enrutadores, causando, por ejemplo, que una ruta se convierta en la mejor ruta hacia un destino en particular. Cuando ocurre el cambio en la topología de la red, estos cambios son reflejados en los mensajes de actualización de la red. Por ejemplo, cuando un enrutador detecta una falla en algún enlace o en algún enrutador, recalcula sus enrutadores y envía mensajes de actualización de ruteo. Cada

enrutador que reciba un mensaje de actualización de ruteo que incluya un cambio actualiza sus tablas y propaga el cambio.

Formato del paquete (implementaciones IP)
La siguiente figura muestra el formato del RIP para implementaciones IP, tal como se especifica por RFC 1058.

longitud del campo, en bytes

1	1	2	2	2	4	4	4	4
A	B	C	D	C	E	C	C	F

A = Comando (petición o respuesta)
B = Número de versión
C = Cero
D = Identificador de familia de dirección
E = Dirección
F = Métrica

El primer campo en el paquete RIP es el campo de *comando*. Este campo transporta un entero indicando ya sea una petición o una respuesta. El comando de petición solicita al sistema que responde el envío de parte o de la totalidad de su tabla de ruteo. los destinos para los que es solicitada una respuesta se encuentran listados después en el paquete. El comando de respuesta representa una contestación a una solicitud o, más frecuentemente, una actualización a la tabla que es regular y no es solicitada. En el paquete de respuesta, un sistema que contesta incluye toda o parte de su tabla de ruteo. Los mensajes regulares para la actualización de la tabla de ruteo contienen la totalidad de la tabla de ruteo.

El campo de *versión* especifica la versión del RIP que está siendo implementada. Con el potencial para muchas implementaciones del RIP en una interred, este campo puede ser usado para señalar versiones diferentes y potencialmente incompatibles.

Siguiendo a un campo de 16 bits, todos en cero, está el campo de identificador de familia de dirección. Este campo especifica la familia de dirección en particular que está siendo usada. En la Internet esta familia de dirección es tipicamente IP (valor = 2), pero otros tipos de redes pueden ser representados.

Después de otro campo de 16 bits, todos ellos también en cero, se encuentra el campo de dirección con 32 bits de longitud. En las implementaciones del RIP en Internet, este campo contiene tipicamente una dirección IP.

Siguiendo dos campos más de 32 bits de ceros está la *métrica* del RIP. Esta métrica es una *cuenta de saltos*. Indica cuantos saltos de interred (enrutadores) deben ser cruzados antes de que pueda ser alcanzado el destino.

Hasta 25 ocurrencias del identificador de la familia de direcciones a través de los campos de métricas son permitidos que sucedan en un sólo paquete RIP. En otras palabras, se pueden listar hasta 25 destinos en cualquier paquete RIP. Se utilizan varios paquetes RIP para transportar información de las tablas de ruteo que son grandes.

Como otros protocolos de ruteo, el RIP usa ciertos timers para regular su desempeño. El timer de actualización de ruteo es generalmente ajustado a 30 segundos, asegurando que cada enrutador enviará una copia completa de de su tabla de ruteo hacia sus vecinos cada 30 segundos. El timer de enrutador inválido determina cuánto tiempo debe transcurrir sin haber escuchado algo acerca de una ruta en particular antes de que esa ruta sea considerada inválida. Cuando una ruta es marcada como inválida, los vecinos son notificados de este hecho. Esta notificación debe ocurrir con anterioridad a que expire el timer de limpieza de rutas. Cuando expira el timer de limpieza de rutas, la ruta es removida de la tabla de ruteo. Los valores iniciales para estos timers es de 90 segundos para el tinmer de ruta inválida y de 270 segundos para el de limpieza de rutas.

Características de estabilidad
El RIP especifica ciertas características diseñadas para hacer más estable su operación para lograr hacer rápidamente los cambios en la topología de la red. Estas características incluyen la actualización en el límite en la cuenta de saltos, detenciones, horizontes fraccionados, y en envenenamientos de reversas.

Límite en la cuenta de saltos
El RIP permite una cuenta de saltos máxima de 15. Cualquier destino mayor a 15 saltos es etiquetado como inalcanzable. La cuenta de saltos del RIP restirnge grandemente su uso en interredes grandes, pero previene queun problema llamado *cuenta hasta el infinito* cause ciclos de ruteo que no tienen fin. El problema de cuenta hasta el infinito se muestra en la figura C2

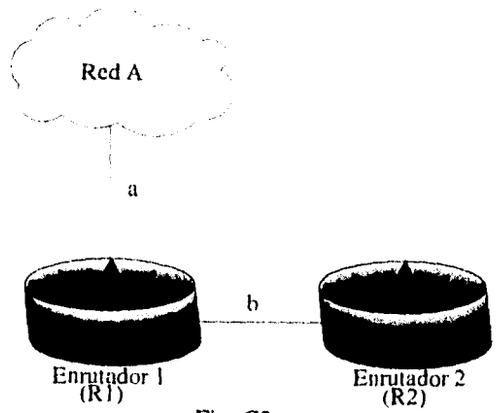

Fig. C2

En la figua C2, considera que ocurriría si el enlace del enrutador 1 (enlace a) hacia la Red A falla. R1 examina su información y ve que el R2 tiene un enlace de un salto hacia la Red A. Dado que R1 sabe que está conectado directamente a R2, advierte un camino de dos saltos hacia la Red A y comienza a dirigir todo el tráfico de la Red A hacia el enrutador 2. esto crea un loop de ruteo. Cuando R2 ve que R1 puede alcanzar ahora la Red A en dos saltos, cambia su propia tabla de ruteo para mostrar que tiene una ruta de 3 saltos hacia la Red A. Este problema, y el loop de ruteo, continuarán infinitamente, o hasta que alguna condición externa de frontera sea impuesta. Esa condición de frontera es la cuenta de saltos máxima del RIP. Cuando la cuenta de saltos exceda de 15, la ruta es marcada como inalcanzable. Sobre el tiempo, la ruta es removida de la tabla.

Detenciones (hold-downs)

Las detenciones son usadas para prevenir que los mensajes regulares de actualización instalen una ruta que ha fallado. Cuando una ruta se cae, los enrutadores vecinos lo detectan. Estos enrutadores pueden calcular nuevas rutas y enviar mensajes de actualización de ruteo para informar a sus vecinos del cambio de ruta. esta actividad comienza una onda de actualizaciones de ruteo que se filtra a través de la red.

Las actualizaciones no llegan instantáneamente a cada dispositivo en la red. Es posible por lo tanto que un dispositivo que ha sido informado de una falla en la red pueda enviar un mensaje regular de actualización (indicando que una ruta que acaba de caerse es aún válida) a algún dispositivo que ha sido notificado de la falla en la red. En este caso, el último dispositivo contiene ahora (y potencialmente sus anuncios) información de ruteo incorrecta.

Las detenciones le dicen a los enrutadores que detengan cualquier cambio que pueda afectar a los enrutadores recientemente removidos, por un tiempo determinado. El período de detención es usualmente calculado para ser un poco mayor que el tiempo necesario para actualizar a la red entera con un cambio en el ruteo. Las detenciones previenen del problema de la cuenta al infinito.

Horizontes fraccionados

Los horizontes fraccionados toman ventaja del hecho de que nunca es útil enviar información de una ruta por la misma dirección en la que vino. Para ilustrarlo, considera la figura C3.

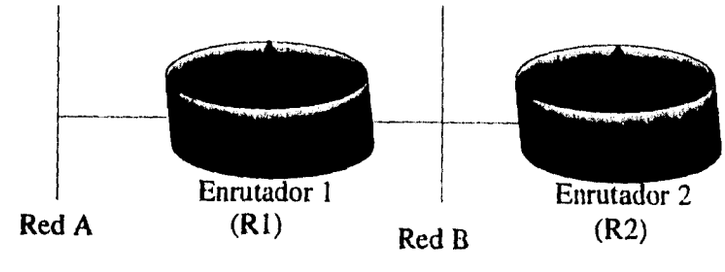

Fig. C3

El enrutador 1 (R1) inicilamente advierte que tiene una ruta hacia la Red A. No hay razón para que el enrutador 2 (R2) incluya esta ruta en su actualización hacia R1, dado que R1 está más cerca de la Red A. La regla del horizonte fraccionado dice que R2 debe quitar esta ruta de cualquier actualización que envíe a R1.

La regla del horizonte fraccionado ayuda a prevenir los loops del ruteo de dos nodos. Por ejemplo, considera el caso donde la interface de R1 hacia la Red A llega a fallar. Sin los horizontes fraccionados, R2 continúa informando a R1 de que puede alcanzar la Red A a través de R1. Si R1 no tiene la inteligencia suficiente, puede tomar la ruta de R2 como una alternativa a su conexión directa que ha fallado, provocando un loop de ruteo. Aunque las detenciones previenen esto, los horizontes fraccionados proporcionan un algoritmo de estabilidad extra.

Actualizaciones de envenenamiento en reversa

Mientras que los horizontes fraccionados previenen loops entre los enrutadores adyacentes, las actualizaciones de envenenamiento en reversa son pensados para deshacer loops de ruteo mayores. La idea es que los incrementos en la métrica de ruteo indican loops de ruteo. Las actualizaciones de envenenamiento en reversa son enviadas para remover la ruta y colocarla como detenida.

Protocolo EGP

Antecedentes

El Protocolo de Gateway Exterior (EGP) es un protocolo de alcance entre dominios usado en la Internet. El EGP está documentado en la RFC 904, publicado en abril de 1984.

El EGP fue el primer protocolo de gateway exterior que ganó amplia aceptación en la Internet sirviendo a un valioso propósito. Desafortunadamente, las dolencias del EGP han sido más visibles al ir creciendo y madurando la Internet. Debido a estas dolencias, el EGP está actualmente siendo eliminada de la Internet, y sustituido por otros protocolos de gateway exterior tales como el Protocolo de Gateway de Frontera (Border Gateway Protocol, BGP), y el Protocolo de Ruteo Entre-Dominios (Inter-Domain Routing Protocol, IDRP).

Tópicos básicos de tecnología

El EGP fue originalmente diseñado para comunicar el alcance hacia y desde los enrutadores núcleos de ARPANET. La información era pasada desde los nodos fuentes individuales en distintos dominios administrativos de Internet llamados *systemas autónomos (ASs)* hasta los enrutadores núcleo, los cuales pasaban la información a través del backbone hasta que ésta podía pasarse a la red destino mediante otro AS. Esta relación entre el EGP y otros componentes de ARPANET se muestra en la figura C4.

Aunque el EGP es un protocolo de ruteo dinámico, utiliza un diseño muy simple. No usa métricas y por lo tanto no puede realizar verdaderas decisiones de ruteo inteligentes. Las actualizaciones de ruteo del EGP contienen información del alcance de una red. En otras palabras, especifica que ciertas redes son alcanzables a través de ciertos enrutadores.

El EGP tiene tres funciones primarias. La primera, los enrutadores corriendo EGP establecen un set de *vecinos*. Estos vecinos son simples enrutadores con los cuales un

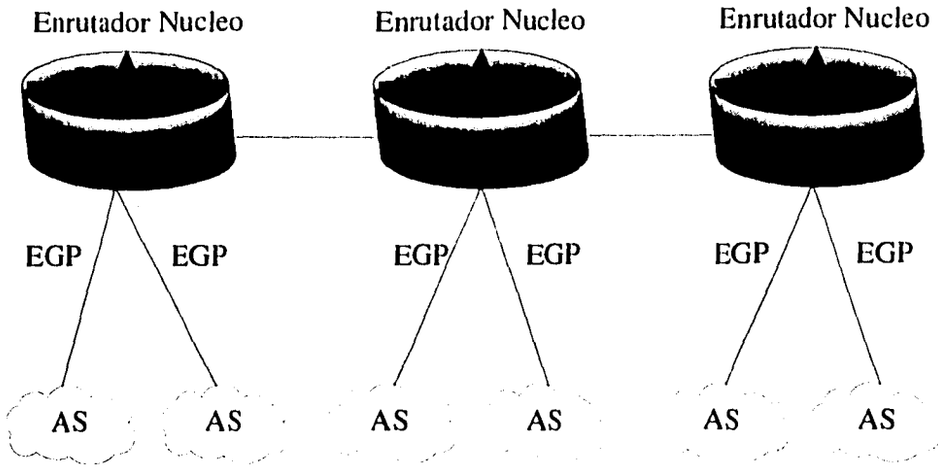

Fig. C4

enrutador EGP desea compartir información del alcance; no hay implicación de proximidad geográfica. Segunda, los enrutadores EGP encuestan a sus vecinos para ver si están vivos. Tercera, los enrutadores EGP envían mensajes de actualización conteniendo información acerca del alcance de redes con sus ASs.

Formato de los paquetes

El paquete del EGP se muestra a continuación:

longitud del campo, en bytes

1	1	1	1	2	2	2	variable
número de versión EGP	Tipo	Código	Estado	Checksum	número de Sistema Autónomo	Número de secuencia	Datos

El primer campo en el encabezado del paquete del EGP es el campo de número de versión del EGP. Este campo identifica el la versión actual del EGP y es revisado por los receptores para determinar si tanto el número de versión del que recibe como del envía son iguales.

El campo siguiente es el campo del *tipo*, el cual identifica el tipo de mensaje. El EGP define cinco tipos de mensajes. Estos se muestran a continuación:

Mensaje	Función
Adquisición de vecinos	Establece y desestablece vecinos
Alcance de vecinos	Determina si los vecinos se encuentran vivos
Encuesta	Determina el alcance de una red en particular
Actualización	Proporciona actualizaciones de ruteo
Error	Indica condiciones de error

Siguiendo al campo de tipo se encuentra el campo de *código*. Este campo distingue entre subtipos de mensajes.
A continuación está el campo de *estado*, el cual contiene información del estado dependiente del mensaje. Los códigos de estado incluyen: recursos insuficientes, problema de parámetro, violación de protocolo, y otros.
Después del campo de estado está el de *checksum*. El checksum es usado para detectar posibles problemas que pueden haberse desarrollado en el tránsito del paquete.
Un campo de *número de sistema autónomo* sigue al de checksum. Este identifica el AS al que pertenece el enrutador que lo envía.
Finalmente, el último campo en el paquete del EGP es el de *número de secuencia*. Este campo permite a dos enrutadores EGP intercambiar mensajes para hacer parejas de peticiones con respuestas. El número de secuencia es inicializado a cero cuando un vecino es establecido y es incrementado en uno con cada transacción de petición-respuesta.
Siguen al encabezado del EGP varios campos adicionales. El contenido de estos campos varía, dependiendo del tipo de mensaje (como se especifica por el campo de tipo).

Tipos de mensajes
Adquisición de vecinos
El mensaje de adquisición de vecinos incluyen un campo de *intervalo de hello* y otro de *intervalo de encuesta*. El intervalo de hello especifica el intervalo para probar si los vecinos están vivos. El campo de intervalo de encuesta especifica la frecuencia de actualización del ruteo.

Alcance de vecinos
El mensaje de alcance de vecinos no agrega campos extra al encabezado del EGP. Estos mensajes usan el campo de código para indicar si el mensaje es un mensaje de hello o una respuesta a un mensaje de hello. El separar la función de avalúo del alcance de la función de actualización de ruteo, reduce el tráfico en la red debido a que los cambios en el alcance de la red usualmente ocurren más frecuentemente que los cambios en los parámetros de ruteo. Sólo después de que un porcentaje específico de mensajes de alcance no han sido recibidos produce a un nodo EGP declarar que un vecino está abajo.

Encuesta
Para proporcionar un ruteo correcto entre ASs, el EGP debe conocer la ubicación relativa de los hosts remotos. El mensaje de *encuesta* le permite a los enrutadores EGP adquirir información del alcance acerca de la redes en las cuales residen esos hosts. Estos mensajes

sólo tienen un campo después del encabezado común - el campo de *red fuente IP*. Este campo especifica la red a ser usada como punto de referencia para la petición.

Actualización de ruteo

Los mensajes de *actualización de ruteo* porporcionan una manera para los enrutadores EGP de indicar la ubicación de varias redes con sus ASs. Además del encabezado común, estos mensajes incluyen muchos campos adicionales. El campo de *número de gateways interiores* indica el número de gateways interiores que aparecen en el mensaje. El campo de *número de gateways exteriores* indica el número de gateways exteriores que aparecen en el mensaje. El campo de *red fuente de IP* proporciona la dirección IP de la red de donde es medido el alcance. Siguiendo a este campo se encuentra una serie de *bloques de gateways*. Cada bloque de gateway proporciona la dirección IP de un gateway y una lista de redes y sus distancias asociadas con el alcance de esas redes.

Con el bloque de gateway, el EGP lista las redes por sus distancias. En otras palabras, a una distancia de tres, puede haber cuatro redes. Estas redes son listadas entonces por dirección. El próximo grupo de redes pueden ser aquellas que se encuentren a una distancia de cuatro, y así continúa.

El EGP no interpreta las métricas de distancia que están contenidas en los mensajes de actualización de ruteo. En esencia, el EGP usa el campo de distancia para indicar si existe un camino; el valor de la distancia sólo puede ser usado para comparar caminos si aquellos caminos exsten completamente en un AS en particular. Por esta razón, el EGP es más un protocolo de alcance que un protocolo de ruteo. Esta restricción también coloca limitaciones de topología en la estructura de Internet. Específicamente, una porción EGP de Internet debe ser una estructura de árbol en la que un gateway núcleo es la raíz, y no existen loops entre otros ASs en el árbol. Esta restricción es una limitación primaria del EGP, y proporciona una razón para su remplazamiento gradual por otros protocolos de gateway exterior más capaces.

Error

Los mensajes de *error* identifican varias condiciones de error del EGP. Además del encabezado común del EGP, los mensajes de rror del EGP proporcionan un campo de *razón*, seguido por un *encabezado del mensaje de error*. Las razones de error del EGP típicas incluyen *formato de encabezado del EGP en mal estado, formato del campo de datos del EGP en mal estado, tasa de encuesta excesiva,* y *la indisponibilidad de información de alcance*. El encabezado del mensaje de error consiste de las tres primeras palabras de 32 bits del encabezado del EGP.

BIBLIOGRAFIA

Bibliografía

-Dvorak, John C.
Anis, Nick
Telecomunicaciones para PC
Editorial McGraw-Hill.

-Benítez Santana José Luis
Nuñez Rodríguez
Introducción a Redes LAN Conectividad
Editorial Compucosmo.

-Black Ulises
Redes de Computadoras
Editorial Macrobit RAMA 1990.

-Stalling W; Van Slike R; "Bussines Data Communications", Segunda edición
Macmillan College Publishing, 1994

- Stalling W; "Handbook of Computer Communications Standars, Volumen 3: The TCP/IP Protocol Suite", Segunda edición Macmillan College Publishing, 1989

- Cisco Systems Inc, "Internetworking Terms and Acronyms", 1993

- Cisco Systems Inc, "Internetworking Technology Overview" 1993

- Fred Halsall, segunda edición, "Data Communications, Computer Networks and OSI" Adisson-Wesley Publishes, 1990

- James Martin, "Local Area Networks", Prentice Hall, 1989

- Mark A. Miller, P.E., "Trobleshooting Internetworks", MGT Books, 1991

- Tanenbaun, Andrew S.
Redes de Computadoras
Prentice-Hall 1988

- Redes Locales de Cómputadoras: Protocolos de alto nivel y evaluación
McGraw-Hill

- Hopper Andrew
Diseño de Redes Locales
Sistemas Técnicos de Edición 1989

- Teleinformática y Redes de Cómputadoras
Marcombo 1987

- Stallings William
Local Networks
Collier Macmillan 1990

- Keiser Gerd
Local Area Networks
McGraw-Hill 1989

- Marney-Petix Vcki
Networking and Data Communications
Reston 1986

- Weber Doug
Novell Netware a su alcane: Ordenes e Instalación
Osborne McGraw-Hill 1991.