



PAGINACIÓN VARIA _____

129

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

TECNOLOGIA INTERNETWORKING

TESIS

QUE PARA OBTENER EL TITULO DE INGENIERO
MECANICO ELECTRICISTA PRESENTAN :

EDGAR ORTIZ BELTRAN
RENE RENDON GALICIA

DIRECTOR DE TESIS :

ING. MARIO A. IBARRA PEREYRA

MEXICO , D.F.

1994



TESIS CON
FALLA DE ORIGEN



UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DERECHOS RESERVADOS © PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

A MIS PADRES JULIETA Y JAVIER :

Que gracias a su apoyo incondicional , a su máxima comprensión , a su valiosa compañía , a su constante preocupación y a su preciado amor he logrado una de mis más grandes metas que es dedicada para ellos

A MIS HERMANOS LETY Y PACO :

Que no se olviden que la vida está llena de objetivos que alcanzar

A PAPA ANGEL :

Que gracias a su orientación en el momento más oportuno , influyo en gran parte a que eligiera ésta profesión

EDGAR

A mis amados padres :

EBELA y ANEL

Gracias a su valioso apoyo , sus continuos consejos y su verdadera comprensión y amor incondicional que me han brindado y aquellas actitudes que de alguna forma han contribuido a culminar una mas de mis valiosas metas , dedicado a ellos.

A mis hermanos :

JULISA y JULIO
(Mis verdaderos amigos)

Por la paciencia y entendimiento , por aquellos momentos de felicidad de exito y fracaso que hemos vivido juntos.

" A todos aquellos personas que han permanecido y estaran junto a mi".

RENE.

TEMA : TECNOLOGIA INTERNETWORKING**CAPITULO UNO
CONCEPTOS BASICOS.****CAPITULO DOS
ESTANDARES Y PRINCIPIOS DE LA TECNOLOGIA INTERNETWORKING.**

- 2.1 Historia de la internetworking.
- 2.2 Principios de la interconexión de sistemas abiertos.
- 2.3 Protocolos OSI para la internetworking.
- 2.4 Aplicación de dispositivos considerando el modelo OSI.
- 2.5 Proyecto de la IEEE 802.
- 2.6 Estructura de la frame LAN.
 - 2.6.1 Ethernet.
 - 2.6.2 IEEE 802.3.
 - 2.6.3 IEEE 802.5.
 - 2.6.4 ARCNET.
 - 2.6.5 FDDI.
- 2.7 Estándares del bridging conforme a la IEEE.
 - 2.7.1 Método Transparent Bridging.
 - 2.7.2 Método Source Routing.
 - 2.7.2.1 Formato del frame.
 - 2.7.3 Método Source Routing Transparent.

**CAPITULO TRES
ESCENARIOS DE LA INTERNETWORKING : LAN-TO-LAN Y LAN-TO-WAN.**

- 3.1 Diseño de la conexión LAN to LAN.
 - 3.1.1 ¿ Qué dispositivo emplear ?
 - 3.1.2 Análisis de la red.
- 3.2 Conexión de redes LAN de arquitecturas distintas.
 - 3.2.1.a Repetidores.
 - 3.2.1.b Bridges.
 - 3.2.1.c Routers.
 - 3.2.1.d Brouters.
 - 3.2.1.e Gateways.
- 3.3 Internetworking LAN to WAN.
 - 3.3.1 Diseño de la conexión LAN to WAN.

CAPITULO CUATRO
BASES DE LA INTERNETWORKING.

- 4.1 Bases del ruteo.
- 4.1.1 Antecedentes.
- 4.1.2 Componentes del ruteo.
- 4.1.3 Conmutación.
- 4.1.4 Algoritmos de ruteo.
- 4.1.4.1 Metas de diseño.
- 4.1.4.1.a Optimización.
- 4.1.4.1.b Simplicidad.
- 4.1.4.1.c Capacidad.
- 4.1.4.1.d Convergencia rápida.
- 4.1.4.1.e Flexibilidad.
- 4.1.5 Tipos de algoritmos de ruteo.
- 4.1.5.a Estáticos ó Dinámicos.
- 4.1.5.b De uno ó varios caminos.
- 4.1.5.c Comun ó jerárquico.
- 4.1.5.d De host inteligente ó ruteador inteligente.
- 4.1.5.e Intradomain ó Interdomain.
- 4.1.5.f Estado de enlace ó Vector de distancia.
- 4.1.6 Parámetros.
- 4.1.6.a Longitud del camino.
- 4.1.6.b Confiabilidad.
- 4.1.6.c Retraso.
- 4.1.6.d Ancho de banda.
- 4.1.6.e Carga.
- 4.1.7 Protocolos Ruteados Vs. Protocolos de Ruteo.
- 4.1.8 Protocolos Internet.
- 4.1.8.1 Direccionamiento IP.
- 4.1.8.2 Ruteo Internet.
- 4.1.8.3 Protocolo IGRP.
- 4.2 Bases del Punteo.
- 4.2.1 Bases Tecnológicas.
- 4.2.2 Tipos de bridges.

CAPITULO CINCO
APLICACION DE LA TECNOLOGIA INTERNETWORKING EN UN AMBIENTE REAL.

- 5.1 Introducción.
- 5.2 Análisis del primer sistema.
- 5.3 Análisis del sistema actual.
- 5.3.1 Descripción de la red.
- 5.4 Hardware del ruteador (Cisco).

CAPITULO SEIS
CONCLUSIONES.

BIBLIOGRAFIA.

C A P I T U L O U N O

C O N C E P T O S B A S I C O S

El creciente avance de las comunicaciones ha orillado al desarrollo de múltiples y muy variados sistemas operativos , protocolos y tecnologías creadas por diferentes marcas. Por lo que la tendencia de hoy en día es integrar toda la variedad mencionada anteriormente por medio de una tecnología llamada INTERNETWORKING , la cual no es una simple estrategia de adelanto de red , sino cuyo objetivo es unificar diferentes marcas sobre una variedad de medios de transmisión y aplicaciones diferentes , las cuales requieren ser centralizadas con un manejo distribuido que permita la separación y el control de configuración , seguridad , contabilidad y funcionamiento.

1.1 Desarrollo.

Se analizará la TECNOLOGIA INTERNETWORKING , ¿Qué es? , ¿Cuáles son los elementos que se emplean para cumplir con sus objetivos? y ¿Qué tan eficaz es trabajar con éste método?.

También se hará una revisión sobre los tres dispositivos de internetworking más empleados en la industria de las comunicaciones , estos elementos son :

- Bridges
- Routers
- Brouters

Se analizará la forma de cómo se emplean para integrar las redes , viéndolos como integradores , la manera en que realizan la interconexión en los diferentes niveles , los protocolos empleados , y cuándo serán puenteados y ruteados , además de distinguir entre un puenteo y un ruteo , qué ventajas y qué desventajas con respecto al modelo de referencia OSI , así como los diferentes escenarios de la INTERNETWORKING , incluyendo el volumen de datos , software y hardware , requerimientos para la aplicación , etc.

A continuación se definen los conceptos empleados en capítulos venideros para tener un entendimiento más claro.

ACK (Acknowledgment) : Es un carácter de control , enviado por el receptor , como una respuesta afirmativa para el transmisor. Esto indica que el bloque transmitido se recibió y que el receptor se encuentra listo para aceptar el siguiente bloque de transmisión.

Algoritmo : Es un conjunto de pasos que siguen determinada lógica para obtener un resultado en específico.

Ancho de Banda : Un rango de frecuencias entre dos límites definidos y expresados en ciclos por segundo o hertz.

Arquitectura : Esta describe básicamente cómo el sistema o programa está constituido y la forma en que sus componentes , protocolos e interfaces trabajan en conjunto para lograr la comunicación.

Backbone : Es el cable principal de una red , el cual enlaza segmentos de red individual.

Block (Bloque) : Es una cantidad de información transmitida , en la que se incluyen caracteres de control indicando el inicio y el final ; usualmente un bloque contiene caracteres de control , de ruteo y chequeo de error.

Bps (Bits por segundo) : La velocidad de transmisión de información binaria.

Bridge : Es un dispositivo que conecta dos redes LAN ; el bridge funciona en el nivel enlace de datos del modelo OSI.

Broadcast : La transmisión hacia dos o más estaciones al mismo tiempo .

Buffer : Un dispositivo que proporciona la facilidad de almacenar temporalmente datos agrupados en bloques.

Bus : El bus es una topología lineal empleada en la arquitectura de las redes de área local (LAN) , en la cual las transmisiones de las estaciones de la red se propagan a lo largo de todo el medio de comunicación y pueden ser recibidas por todas las demás estaciones.

Caracteres de Control : Son los caracteres empleados para facilitar la transmisión de datos , por ejemplo , caracteres asociados con el poleo , sincronización , chequeo de error , arranque y parada , etc.

CTS (Clear To Send) : Es una señal de control enviada desde el modem al DTE , en respuesta al RTS proveniente del DTE , usada para indicarle al DTE que el modem está listo para enviar datos.

DCE (Equipo de comunicación de datos) : Es un dispositivo que mantiene y termina una conexión entre el equipo terminal de datos y un medio de comunicación (por ejemplo un modem).

DSR (Data Set Ready) : Es una señal de control que es enviada desde el modem al DTE , ésta se usa para indicarle al DTE que el modem está listo para transmitir datos.

DTE (Equipo Terminal de Datos) : Es un dispositivo el cual transmite o recibe datos.

DTR (Data Terminal Ready) : Es una señal de control enviada por el DTE al modem , se usa para indicarle al modem que el DTE esta listo para transmitir datos .

RTS (Request To send) : Es una señal de control enviada por el DTE al modem para indicarle , que el DTE enviará datos .

Control de Flujo : Técnica de ajuste de velocidad que se utiliza en las comunicaciones de datos para impedir el bloqueo de dispositivos receptores y pérdida de datos.

CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
: CSMA es el medio por el cual cada estación de trabajo escucha el cable de transmisión , si este no está ocupado , la estación de trabajo envía la información a través del cable. CD permite detectar una colisión en la red y pedir a la estación de trabajo que envió la información que haga una retransmisión de la misma.

Data Base (Base de Datos) : Es toda la información contenida en un sistema de computación , la cual es fundamental en una empresa que opera con su propio sistema . El acceso a la base de datos puede ser restringido para ciertos usuarios o programas de aplicación.

Datagram : Es un paquete de tamaño fijo con suficiente información para que el sistema sepa cual es su destino , sin tener alguna relación con transmisiones previas.

Ethernet : Es una red de área local (LAN) diseñada por Xerox cuya característica es la transmisión en banda base de 10 Mbps sobre cable coaxial blindado , además de emplear CSMA/CD como un mecanismo de control de acceso.

E1 : Es la norma europea de transmisión (voz o datos) en forma digital , que equivale a 2.048 Mbps.

Frame : Es una unidad de transmisión lógica manejada en los niveles de enlace de datos , ésta incluye , su propio control de información para direccionamiento y chequeo de error , además de la dirección de transmisión.

Gateway : Es una estación de red lógica que se emplea para que dos redes incompatibles se comuniquen , ésta ejecuta una función de conversión de protocolo a través de varios niveles de comunicación .

HDLC (High Level Data Link Control) : Conjunto de estándares altamente estructurado que rige el medio a través del cual se pueden comunicar dispositivos diferentes entre sí en grandes redes de comunicación de datos.

Interfase : Es un área definida entre dos componentes de un equipo por la cual todas las señales que pasan a través de ella son manejadas cuidadosamente (todo a nivel físico).

LAN (Local Area Network) : Es una red que cubre una área geográfica relativamente pequeña. Dentro de ésta se incluyen dispositivos y recursos de computación como PC's , impresoras , minicomputadoras y mainframes , enlazados por un medio de transmisión común , como por ejemplo , un cable coaxial ó par trenzado.

MAN (Metropolitan Area Network) : Es una red que se extiende en un rango de 50 Km. , y opera a velocidades de 1 a 200 Mbps proporcionando servicios de datos , voz y transmisión de imágenes en tiempo real.

Network (Red) : Son los caminos de comunicación entre computadoras , terminales y otros dispositivos de tal manera que todos se puedan intercomunicar.

Packet (Paquete) : Es un grupo de dígitos binarios , como por ejemplo , los datos y los caracteres de control contenidos en un formato definido.

Puerto : Es la interface física ó eléctrica , en la cual se presenta el acceso al medio de comunicación o transmisión.

Protocolo : Es una serie de reglas que definen en forma precisa el formato de los procedimientos y mensajes para permitir que se comuniquen los dispositivos que conforman una red.

Repetidor : Es un dispositivo en donde las señales que recibe las amplifica y regenera , para compensar las pérdidas y distorsiones.

Router : Es un dispositivo que interconecta redes locales ó remotas , empleando protocolos específicos tales como el XNS y el TCP/IP. Este proporciona un manejo administrativo por separado para cada segmento de la red. A diferencia del bridge y del gateway , éste opera hasta el nivel de red del modelo OSI.

SDLC (Synchronous Data Link Control) : Es una versión de IBM similar al protocolo de bit orientado HDLC .

Subnet : Es una parte de una red completa interconectada a ella por medio de un ruteador.

TCP/IP (Transmission Control Protocol/Internet Protocol) : Es un software desarrollado por el Departamento de Defensa de U.S.A. El IP trabaja con el nivel tres de OSI y TCP trabaja en los niveles cuatro y cinco de OSI.

Throughput : Es la cantidad de bits transmitidos en un determinado período tiempo. Por lo general , éste término se relaciona con el aprovechamiento del ancho de banda.

Token Bus : Es un mecanismo para acceder a una LAN , y tiene una topología en la cual todas las estaciones conectadas al bus escuchan una señal para transmitir . Las estaciones que desean transmitir deben recibir ésta señal antes de hacerlo , sin embargo , la estación que sigue para recibir la señal no necesariamente es la siguiente estación física en el bus. El acceso al bus es controlado por algoritmos que asignan prioridad.

Token Ring : Es un mecanismo para acceder a una LAN , tiene una topología en la cual una señal de supervisión pasa desde una estación a otra en forma secuencial. Las estaciones que desean obtener el acceso a la red deben esperar la llegada de la señal antes de transmitir datos . En una Token Ring la siguiente estación lógica que recibe la señal es la estación que sigue conectada físicamente en el ring.

T1 : Es la norma americana cuyo formato digital , para transmisión de voz o datos es de 1.544 Mbps.

WAN (Wide Area Network) : Es una red de comunicación de datos diseñada para servir a una área de cientos de miles de kilómetros cuadrados , un ejemplo de éstas es la red pública.

C A P I T U L O D O S

"ESTANDARES Y PRINCIPIOS DE LA INTERNETWORKING"

- 2.1 HISTORIA DE LA INTERNETWORKING.
- 2.2 PRINCIPIOS DE LA INTERCONEXION DE SISTEMAS ABIERTOS.
- 2.3 PROTOCOLOS OSI PARA LA INTERNETWORKING.
- 2.4 APLICACION DE DISPOSITIVOS CONSIDERANDO EL MODELO OSI.
- 2.5 PROYECTO DE LA IEEE 802.
- 2.6 ESTRUCTURA DE LA FRAME LAN.
 - 2.6.1 ETHERNET.
 - 2.6.2 IEEE 802.3.
 - 2.6.3 IEEE 802.5.
 - 2.6.4 ARCNET.
 - 2.6.5 FDDI.
- 2.7 ESTANDARES DEL BRIDGING CONFORME A LA IEEE.
 - 2.7.1 METODO TRANSPARENT BRIDGING.
 - 2.7.2 METODO SOURCE ROUTING.
 - 2.7.2.1 FORMATO DEL FRAME.
 - 2.7.3 METODO SOURCE ROUTING TRANSPARENT.

C A P I T U L O D O S

ESTANDARES Y PRINCIPIOS DE LA INTERNETWORKING

Definir el término INTERNETWORKING no es cualquier cosa ya que el término mismo proviene de una lengua extranjera , y no tiene una traducción específica al español , además de que este término está auxiliado en base a otros conceptos de la misma índole.

Actualmente existen diferentes definiciones acerca de la INTERNETWORKING ; la IBM la define como "Una comunicación entre dos o más redes".

Otra definición de INTERNETWORKING podría ser "comunicación entre dispositivos (procesadores de datos) pertenecientes a una red con otra posible red diferente con sus correspondientes dispositivos".

El término INTERNETWORKING describe los diferentes problemas a los que se han enfrentado diseñadores , administradores , o bien gente relacionada con ésta tecnología ; por ejemplo , en un manejo de red puede surgir la necesidad de comunicar una "DEC minicomputer" con una IBM Mainframe ; otro caso podría ser consultar el "Set up" de una LAN Ethernet, con capacidad de acceso remoto.

Gracias a ésta tecnología un administrador de red puede enlazar sistemas con hardware con software diferente , o bien integrar Macintosh , PC o UNIXworkstations.

2.1 Historia de la Internetworking.

A finales de los 60's y comienzos de los 70's , las redes de computadoras se encontraban sustentadas por el uso de "Mainframes".

Posteriormente muchos centros de información adquirieron minicomputadoras o Mainframes , en donde las marcas que predominaron fueron IBM , Honeywell , DEC o Sperry (actualmente UNISYS).

El usuario fué eligiendo en base a sus necesidades la topología , arquitectura , hardware y software ; con la posibilidad de rediseñar la red instalada , pero en el caso de que el sistema instalado necesitara un cambio o rediseño , la compañía o centro donde se encontrara el sistema de computadoras tenía que recurrir al fabricante quien suministraba y hacía los cambios pertinentes para su realización.

A la mitad de los años 70 hubo un cambio en el concepto de sistemas de computadoras , que trajo como consecuencia la idea de un sistema abierto (una arquitectura de red basada en un estándar) ; de este modo apareció una ruptura en la base de las arquitecturas tradicionales , ya que surgió la necesidad de acceder de una DECminicomputer a una IBM Mainframe llegando a ser más que una posible idea. Posteriormente DEC , en su versión de 1982 FASE IV , realizó la conexión con la arquitectura SNA.

Dos grupos fueron los precursores para desarrollar el estándar para un " sistema abierto ": Por un lado , los usuarios quienes querían soluciones de vendedores independientes y por el otro , los vendedores quienes requerían productos comerciables. La colaboración de estos dos grupos conjuntamente trajo como resultado la evolución de los estándares. Un número de organizaciones emergieron tales como el Comité Consultivo Internacional de Telefonía y Telegrafía (CCITT) ; la Organización Internacional para Estandarización (ISO) y el Instituto Nacional Americano de Estándares (ANSI).

Debido a que ya no fué suficiente tener la comunicación de computadora a computadora , sino comunicar usuarios de varias redes entre sí (objetivo de la INTERNETWORKING) ; se creó el Modelo de Referencia OSI (Interconexión de Sistemas Abiertos) ; publicado primeramente en 1978 por la ISO , en éste se definían las funciones de comunicación en términos de siete niveles distintos.

Actualmente , debido a la aparición de las organizaciones antes mencionadas , la mayoría (sino es que todos) de los productos de interconectividad (modems , multiplexores , convertidores de interface , conmutadores , bridges , ruteadores , compresores , concentradores , gateways , controladores , etc.) existentes en el mercado , están apegados a las normas definidas , de tal manera que la gente involucrada en el medio de la ingeniería en comunicaciones hable un sólo idioma.

2.2 Principios de interconexión de sistemas abiertos.

El Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI) , es diseñado como un estándar que permite la comunicación de sistemas de información , además que el modelo OSI se encuentra referido a los protocolos utilizados en éstos sistemas.

Un sistema abierto se encuentra basado en un estándar , éste sistema puede comunicar y trabajar con otros sistemas utilizando interfaces y protocolos que ambos manejan.

El Modelo OSI fué creado por la Organización de Estándares Internacionales (ISO) el cual establece un modelo de comunicación de redes que se encuentra dividido en 7 niveles (Fig. 2-1).

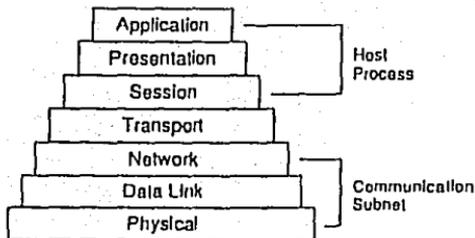


Fig.2-1. "Niveles del Modelo de Referencia OSI".

Nivel Físico.

Primeramente el nivel físico es orientado para la transmisión de bits de un nodo a otro nodo ; los bits pueden ser proporcionados por un Host, una workstation , etc. El objetivo del nivel físico es incluir y definir las interfaces del medio de transmisión , codificación de la señal , definición del rango de los voltajes ó magnitudes de las corrientes , las dimensiones de los conectores , la forma de los pines y otros dispositivos asociados a la transmisión física para el flujo de bits.

Nivel Enlace de Datos.

Este nivel mantiene y asegura las comunicaciones de enlace de ambos nodos , y considera que el nivel físico está libre de errores por ruido. Este nivel proporciona un mecanismo confiable para transmitir frames de datos hacia el nodo destino. El nivel de enlace de datos inserta direcciones en los frames (tanto en origen y destino) y proporciona control de errores en los datos , normalmente implementado por un método estadístico conocido como chequeo de Redundancia Cíclica (CRC).

Nivel de Red.

Este nivel establece un camino para el transporte del paquete de datos junto con la subnet , con dirección origen a destino. Este nivel se encuentra sustentado en dispositivos como son switches , routers , etc. , que controlan el tráfico de esta información de paquetes dentro de la subnet. La subnet es una red que es parte de la extensión de la red , ésta puede ser conectada vía bridges , routers o gateways.

Nivel de Transporte.

El nivel de transporte proporciona una transmisión confiable de mensajes originados en el Host provenientes del nivel 7 (nivel de aplicación) , además asegura que el nivel enlace de datos transmita los frames de ambos nodos ; la diferencia entre el enlace de datos y el nivel de transporte es que el nivel enlace de datos , libera ambos nodos mientras que el dominio del nivel transporte se extiende desde el origen al destino a través de la subnet de comunicación , de esta forma se puede enviar un mensaje desde el origen hasta el destino. Por ejemplo , el nivel de transporte controla los segmentos a lo largo del mensaje dentro de las pequeñas unidades (packets) dando prioridad a la transmisión y asegura el reensamble de estos paquetes dentro del mensaje original en el extremo receptor.

Nivel de Sesión.

Este nivel establece iniciar y terminar procesos , realiza sesiones (conversaciones) entre Hosts , traslada nombres y direcciones en base de datos , así como la sincronización entre 2 Hosts.

Nivel de Presentación.

Este nivel establece la sintaxis (forma) en la cual se intercambian datos entre los 2 Hosts , además éste nivel estrictamente proporciona funciones para la manipulación de datos más no para comunicar , el nivel también comprime y encripta datos.

Nivel de Aplicación.

Este nivel proporciona servicios a los usuarios finales , además transfiere archivos , mensajes electrónicos , emula terminales virtuales y accesa a bases de datos remotas , el usuario final interactúa con los niveles de aplicación.

Los 7 niveles están divididos en 2 plataformas. El primer grupo está comprendido por los 3 primeros niveles (físico , enlace de datos y red) que concluyen la comunicación de la subnetwork , plataforma o la parte portadora del sistema. Los 3 niveles superiores (sesión , presentación y aplicación) son normalmente conocidos como los procesos de Host ; el nivel medio (nivel de transporte) actúa como buffer entre las 2 plataformas , agrupando los niveles superiores con la parte del procesador Host.

La arquitectura Internetwork resulta cuando 2 Sistemas Abiertos son conectados físicamente con un cable (Ver fig. 2-2).

En ésta configuración los niveles operan par a par ; dentro del mismo sistema la conexión es vertical (comunicación entre niveles de OSI) , mientras los protocolos se encuentran comunicados horizontalmente entre el par de niveles de ambos sistemas.

En la misma fig.2-2 podemos ver un ejemplo sencillo ; se asume que el sistema abierto A desea enviar información al sistema abierto B , el nivel de aplicación del sistema abierto A crea una entrada al programa de aplicación. El mensaje entonces procede a descender a través de los siete

niveles (desde el siete hasta el uno del sistema A) atravesando el medio físico de transmisión (por ejemplo el cable) , y ascendiendo a los siete niveles (desde el uno hasta el siete) del sistema B ;

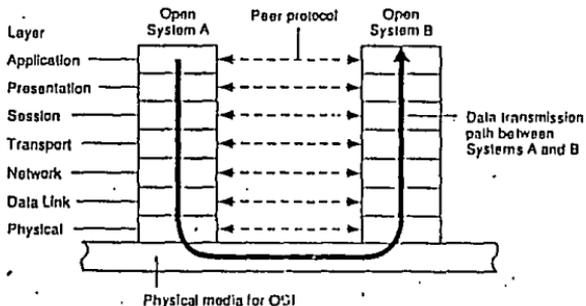


Fig.2-2. "Modelo de Referencia para los 7 Niveles y Protocolos Pares".

un proceso detallado es mostrado en la fig 2-3 ; los datos del proceso de aplicación X pasan al protocolo del nivel de aplicación el cual añade su encabezado de aplicación (AH). El encabezado contiene Control de Información de Protocolo (PCI) necesario para que el proceso par Y interprete los datos ; el encabezado AH más la aplicación de datos (AD) pasa entonces al nivel de presentación , maneja los encabezados AH y AD como sus propios datos , agrega

el encabezado de presentación PH y los envía a los niveles sesion, transporte y red en turno ; cuando el mensaje encapsulado llega a el nivel de enlace de datos , se agregan los encabezados Framing (F) , Address (A) y Control (C) como información del nivel enlace de datos. Una Secuencia de Chequeo de Frame (FCS) más caracteres adicionales Framing (F) se incluyen en el trailer de enlace de datos. El frame pasa al nivel físico , en el cual se codifican los datos para transmisión , accesa al medio de transmisión y monitorea la transmisión serial de bits , en el nodo destino ocurre el inverso de este proceso. El nivel físico manda sus bits al nivel enlace de datos , el cual los decodifica y elimina los encabezados. El frame se envía a los niveles superiores. El proceso finaliza cuando el mensaje (mostrado nuevamente como aplicación de datos) es entregado al proceso de aplicación Y.

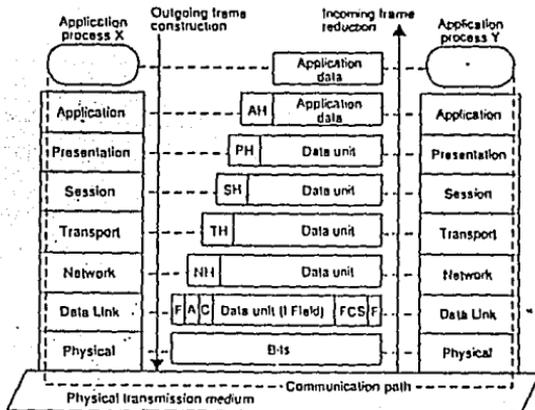


Fig.2-3. "Construyendo un frame para transmisión".

Cuando no es posible enlazar 2 sistemas por el mismo cable físico puede ser usado un sistema abierto relay (fig. 2-4). El relay es también conocido como nodo de conmutación e implementado en los 3 primeros niveles del modelo OSI (plataforma de comunicación). Un ejemplo de un sistema abierto relay es la Red de Telefonía Pública la cual es usada para transmitir señales de voz y datos. Varios de los centros de conmutación conocidos como centrales, rutean y conmutan una determinada llamada telefónica, la cual toma diferentes rutas pasando a veces por gran cantidad de centrales, alcanzándose así el objetivo final de comunicarse. Por lo mismo es necesario identificar los nodos origen y destino, por ejemplo sistemas abiertos A y B. Los datos que se originan en el sistema A pasan a través de la plataforma de comunicación, llegando por éste camino al sistema B. Los datos no sufren ninguna modificación dentro de la subnet, lo cual se considera como una transmisión transparente de datos.

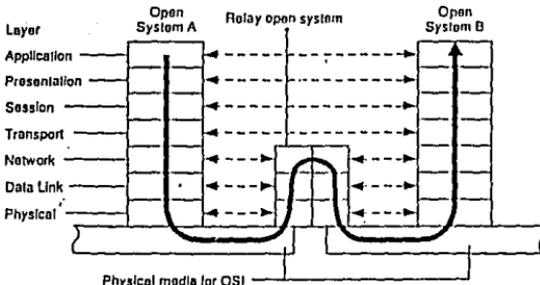


Fig.2-4. "Comunicación involucrando sistemas abiertos relay".

2.3 Protocolos OSI para Internetworking.

El Modelo de Referencia OSI (desarrollado por la ISO) ha traído como consecuencia el desarrollo de protocolos asociados , es decir , protocolos estandarizados cuyo estándar tiene similitud con muchos otros. Estos protocolos describen la utopía de la internetworking : "Si todos los vendedores emplearan protocolos idénticos en todos los niveles , los problemas de internetworking de los usuarios estarían resueltos". Desafortunadamente , el predominio de SNA , DECnet y otras arquitecturas propietarias de conectividad han atrasado la evolución de una industria que cumpla totalmente con la arquitectura de OSI.

A continuación se presenta una relación que existe entre las normas a nivel mundial y la similitud que presentan sus estándares referidos a los 7 niveles del modelo OSI (ver fig. 2-5).

Los protocolos de los niveles físico y enlace de datos ofrecen múltiples opciones para tener acceso a sistemas LAN , WAN y Minimainframes ; por ejemplo , existen muchos estándares , referidos a los niveles mencionados , tales como los de IEEE 802.3 , 802.4 y 802.5 , los cuales tienen su contrapartida en la ISO : ISO 8802/3 , 8802/4 y 8802/5 , respectivamente.

Otros estándares de ISO definen los tipos de conectores (p.e. el ISO 8877 , el cual define el plug de 8 pin conocido también como un RJ-45) o formatos de frame (p.e. el ISO 7809 , el cual se refiere al HDLC (High Level Data Link Control)) similar al SDLC (Synchronous Data Link Control) de la IBM.

Otras asociaciones han creado sus estándares a los niveles físico y enlace de datos , que son ampliamente aceptados , por ejemplo : la Asociación de Industrias Electrónicas (EIA) , el Instituto Nacional de Estándares Americanos (ANSI) ó el Comité Consultivo Internacional de Telegrafía y Telefonía (CCITT) , etc. Un ejemplo de un protocolo del nivel enlace de datos es ISO 7776 el cual es equivalente a LAP/LAPB de X.25 de la CCITT. Este estándar define el protocolo LINK ACCESS PROCEDURE/LINK ACCESS PROCEDURE BALANCED usado dentro del protocolo X.25.

OSI Layer	Example ISO Protocols				
Application	ISO 9040/9041 VT	ISO 8531/8532 JIM	ISO 8571/8572 FTAM	ISO 8595/9598 CMIP	
Presentation	ISO 8823/CCITT X.226 Connection-Oriented Presentation Protocol				
Session	ISO 8327/CCITT X.225 Connection-Oriented Session Protocol				
Transport	ISO 8073/CCITT X.224 Connection-Oriented Transport Protocol				
Network	ISO 8473 Connectionless Network Service			ISO 8206/CCITT X.25 Packet Level Protocol	
Data Link	ISO 8802 2				
	ISO 9314.2 FDDI	ISO 8802.3 CSMA/CD BUS	ISO 8802.4 Token BUS	ISO 8802.5 Token RING	ISO 7776 CCITT X.25 LAP/LAPB
Physical	ISO 7609 HDLC				
	Options from EIA, CCITT, IEEE, etc.				

Fig.2-5. "Ejemplos de protocolos OSI".

Los estándares del nivel de red pueden definir cualquier servicio "Connection-Oriented" definido por ISO 8208 y 8878 (OSI emplea el Protocolo Packet-Level para proporcionar un servicio de movimiento de datos e indicaciones de error por medio de un circuito virtual) o "Connectionless" definido por ISO 8473 (estándar que proporciona 2 tipos de servicios : 1o el que define el tipo de protocolo que está empleando el nivel de red y 2o , el servicio proporcionado al nivel de transporte para transferencia de datos).

El ISO Internet Protocol (ISO IP) es similar al usado por el Departamento de la Defensa de U.S.A. y tiene alguna relación con el TCP/IP. Existiendo algunas diferencias como por ejemplo , el ISO IP permite longitudes de dirección variable donde la mayoría usualmente definen una longitud de dirección fija ; un campo preliminar en el encabezado de ISO IP define la

longitud del campo la cual contiene a su vez las direcciones mismas. Por otro lado, un campo de opciones es también incluido dentro del encabezado de ISO IP para especificación de parámetros opcionales, así como la calidad del servicio o el ruteo de la información.

En el nivel de transporte de la ISO, un número de opciones de protocolo son disponibles dependiendo fundamentalmente del tipo de red que se está empleando. Se tienen 3 clases diferentes de redes: Tipos A, B, y C. La red tipo A representa un servicio óptimo, libre de errores y sin existencia de resets (N-RESETS) en el nivel de red. La red tipo B asegura una perfecta entrega de paquetes, pero es necesario la existencia de resets debido a congestión en la red o fallas en el hardware/software. La red tipo C proporciona un servicio inconfiable, posibilidad de pérdida de paquetes y uso de resets constantemente. Algunos ejemplos típicos de estos tipos de redes son: Redes LAN, Redes de Datos Públicas y Redes de Radio-Paquetes, respectivamente.

Dentro de los 3 tipos de redes, se tienen 5 clases de protocolo del nivel de transporte:

- Clase 0 : Clase común empleada por la red tipo A. No se necesita secuencia o control de flujo.
- Clase 1 : Clase básica para la recuperación de errores, empleada en la red tipo B. Esta clase emplea una secuencia para manejar el reseteo (N-RESETS).
- Clase 2 : Clase de multiplexaje, usada por la red de tipo A. Esta clase amplía la clase cero para permitir la función del multiplexaje.
- Clase 3 : Recuperación de errores y clase de multiplexaje, empleada por la red de tipo B.
- Clase 4 : Detección de error y recuperación de clase usada por la red de tipo C. Asume el tipo de red en el peor de los casos y toma la interpretación de protocolo más compleja.

De los protocolos mencionados anteriormente (conocidos como TP0-TP4) , TP4 es el más parecido a el protocolo del Departamento de Defensa , Transmisión Control Protocol (TCP) , siendo el más discutido frecuentemente. Dos estándares detallan los protocolos del nivel de transporte : ISO 8072 (Connetion-Oriented Transport Service) e ISO 8073 (Connection - Oriented Transport Protocol) ; el equivalente al CCITT con respecto al ISO 8073 es CCITT X.224.

El nivel de sesion proporciona cuatro servicios. El primero es establecer la conexión , hacer cambio de datos y terminar la conexión ; el segundo es emplear señales para manejar el cambio de datos , sincronizar la conexión y determinar el tipo de transmisión requerida : half o full dúplex. El tercer servicio es establecer los puntos de sincronización dentro del flujo de datos así que la comunicación puede ser resumida desde uno de estos puntos si es que se presenta una interrupción. El cuarto servicio interrumpe la transferencia de datos continuando desde un punto de sincronización predeterminado. Los estándares empleados en éste nivel son ISO 8326 (Connection - Oriented Session Service) e ISO 8327 (Connection - Oriented Session Protocol). El equivalente al CCITT con respecto al ISO 8327 es CCITT X.225.

Más que ser una función de comunicación , el nivel de representación distribuye dentro de lo posible la representación de datos. Este nivel conserva el significado de los datos que están siendo transmitidos , independientemente de la sintaxis o la forma empleada. Los estándares usados en el nivel de presentación son ISO 8822 (Connection - Oriented Presentation Service) y la ISO 8823 (Connection - Oriented Presentation Protocol). La estructura de datos titulada ABSTRACT SYNTAX NOTATION 1 (ASN 1) es también definida como la ISO 8824. Estos estándares están relacionados a funciones tales como la encriptación y la compresión de datos.

El nivel de aplicación tiene estándares para distintas funciones específicas. La ISO 9040/9041 define Virtual Terminal Service/Protocol ; el ISO 8831/8832 define Job Transfer y Management Service Protocol , para ejecución de programa remoto.

El ISO 8571/8572 es File Transfer Access y Manipulation Service/Protocol , el cual define los servicios de manipulación de archivos remotos. ISO 9595/9596 define la Common Management Information Service/Protocol usado para el manejo de la red.

2.4 Aplicación de dispositivos considerando el modelo OSI.

En las siguientes líneas se hará una breve explicación de cómo algunos dispositivos de conectividad trabajan de acuerdo al Modelo de Referencia OSI. Recordando el modelo de protocolo "por pares" y considerando que dos sistemas abiertos son conectados por un medio de transmisión físico tales como cables de par trenzado ó fibra óptica. ¿Qué pasa si la longitud del cable es tan grande que la señal se atenúa de forma considerable?. Una primera y simple solución sería colocar un repetidor el cual amplificará o regenerará la señal física (fig. 2-6). Los repetidores funcionan únicamente en el nivel físico y operan solamente entre redes iguales, tales como comunicación de Token Ring a Token Ring o de Ethernet a Ethernet. Un repetidor forma parte de la Internetwork para extender la amplitud de comunicación de las redes a grandes distancias; segmentos conectados se comportan físicamente (y lógicamente) como una sola red.

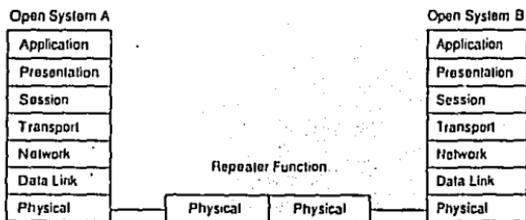


Fig.2-6."Comparando un repetidor al modelo OSI".

Cuando la señal es insuficiente para que la comunicación exista en la red , el repetidor es cambiado por un bridge (fig. 2-7) , el cual ahora trabajará hasta el nivel de enlace de datos. El Bridge "lógicamente" separa dos segmentos de red según la indicación de el direccionamiento dentro del Frame del nivel de enlace de datos (en la norma IEEE ésta función es empleada por el nivel MAC (Control de Acceso al Medio)). La información es almacenada en el bridge y es proporcionada dentro del frame transmitido , indicándole al bridge que tome una simple decisión : Que pase el Frame al siguiente segmento (Forwarding) o que no pase el Frame al siguiente segmento (Filtering). Los bridges operan en redes que son compatibles con esquemas de direccionamiento en el nivel de enlace de datos (comunicaciones de IEEE 802.3 a 802.3 o 802.3 a 802.5) , siendo transparente a los protocolos correspondientes al nivel de red y a los protocolos de los niveles superiores.

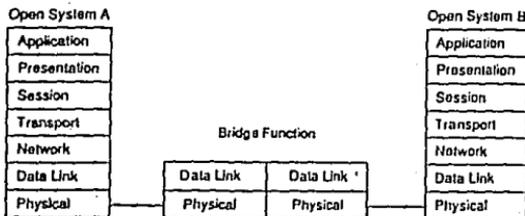


Fig.2-7."Comparando un bridge con el Modelo de OSI".

Los ruteadores operan en el nivel de red del Modelo de Referencia OSI (Fig.2-8) y tienen la capacidad para interpretar ya sea uno o más protocolos en este nivel. Llamar al nivel de red es tomar una opción entre varios caminos disponibles en la subnet de comunicación, eventualmente comunicando los host origen y destino. Un ruteador trabaja de manera semejante leyendo información acerca de la dirección de la red destino y enviando los paquetes a ella misma. (Los bridges, como se observó anteriormente toman una simple decisión binaria para enviar o no un frame después de que examinó la dirección del nivel de enlace de datos). En otras palabras el ruteador es empleado para funciones de conectividad en redes extensas. Los ruteadores pueden manejar protocolos del nivel de red, tales como el Internet Protocol (IP), o cualquier otro como el DECNET y el IPX (Internetwork Packet Exchange) de Novell.

Finalmente, las compuertas (gateways) trabajan a los siete niveles de OSI (Fig.2-9). Las compuertas operan en aplicación-orientada; tienen la capacidad para conectar sistemas de correo electrónico incompatibles, convirtiendo y transfiriendo archivos desde un sistema a otro ó habilitando la interoperabilidad entre sistemas de operación distintos.

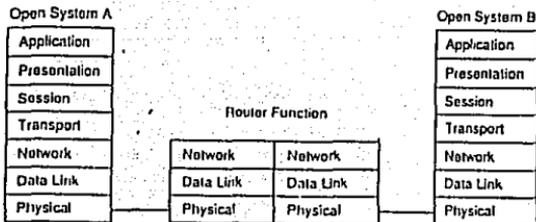


Fig.2-8. "Comparando un Router al Modelo OSI".

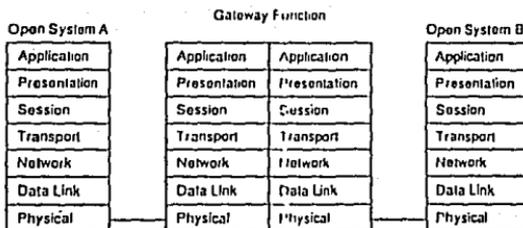


Fig.2-9."Comparando una compuerta al Modelo OSI".

2.5 Proyecto 802 de IEEE.

Al ver la necesidad de estandarizar el mercado de las redes LAN, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) creó el proyecto 802 llamado así por que fué creado en el mes de febrero y año de 1980; éste proyecto direcciona los estándares de LAN a los niveles físico y enlace de datos del Modelo OSI (como se muestra en la fig. 2-10).

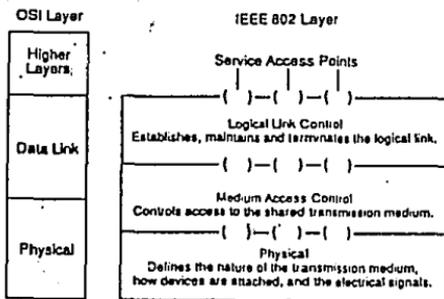


Fig.2-10. "Comparando el proyecto 802 de IEEE con el modelo OSI".

El nivel físico del modelo de LAN de la IEEE es similar a su contrapartida en la OSI , dentro de sus funcionalidades se encuentran codificación y decodificación de la señal , transmisión y recepción serial de bit y proporciona la conexión física al medio de transmisión , ya sea por par trenzado , cable coaxial ó cable de fibra óptica.

El nivel MAC (Control de Acceso al Medio) de la IEEE se encuentra entre los niveles físico y enlace de datos , éste nivel como su nombre lo indica controla el acceso al medio de transmisión y a su vez se subdivide dentro de otros estándares :

- 802.3 : Carrier Sense Multiple Access/ Collision Detection (CSMA/CD).
- 802.4 : Token Passing Bus.
- 802.5 : Token Passing Ring.

Cada uno de estos estándares contenidos en el nivel MAC define un formato único.

El nivel superior del modelo de LAN IEEE es el nivel Logical Link Control (LLC) , definido a su vez por el estándar de IEEE 802.2 , el nivel LLC guarda cierta similitud con el nivel enlace de datos , existiendo siempre algunas diferencias. Primero , ambos niveles deben ser totalmente confiables para transmitir frames de información entre estaciones adyacentes. En el modelo de LAN esto no es necesario para las funciones del nivel de red como pueden ser el ruteo y la conmutación. Teniendo sólo una ruta disponible (el medio de transmisión física , el direccionamiento definido en el frame del nivel MAC es suficiente para entregar el frame). Otras funciones tales como el flujo de control y el control de error son también manejados por el nivel enlace de datos.

La mayor diferencia entre el nivel de enlace de datos de OSI y el nivel LLC de la IEEE 802.2 es que múltiples puntos finales al enlace de datos pueden existir en el modelo de IEEE. Tener la comunicación entre una LAN y múltiples SAPs (Acceso a los Puntos de Servicio) es a menudo requerido. Los SAPs funcionan en cierta forma análoga a los puertos. Por esto una workstation que tiene una dirección en el nivel MAC puede comunicarse con distintos procesos de los niveles superiores. Cada uno de estos procesos debe tener una dirección SAP única. Tanto las direcciones Origen (SSAP) y Destino (DSAP) son especificados en el Protocolo de la Unidad de Datos del nivel LLC de 802.2 (mostrado en la fig. 2-11).

Se definen tres tipos de operaciones del nivel LLC :

- Tipo 1 (Sin reconocimiento , Connectionless Services).
El envío y recepción de frames en un datagram. Transmisiones punto a punto , multipunto y broadcast son soportadas.
- Tipo 2 (Connection - Oriented Service). Una conexión lógica entre SAPs que proporcionan un control de secuencia control de flujo control de error y reconocimientos.

Tipo 3 (Reconocimiento Connectionless). Servicio punto a punto con reconocimientos.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

DSAP Address = destination service access point address field

SSAP Address = source service access point address field

Control = control field (16 bits for formats that include sequence numbering, and 8 bits for formats that do not)

Information = information field

* = multiplication

M = an integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

Fig.2-11. "El protocolo de la unidad de datos Logical Link Control (LLC)".

2.6 Estructura de la frame LAN.

Las 4 redes de área local (LAN) más importantes actualmente son: Ethernet, Token Ring, ARCNET y FDDI (Fiber Data Distribute Interface), las cuales tienen diferentes formatos de transmisión para sus frames en el nivel de enlace de datos.

2.6.1 Ethernet.

El formato de frame Ethernet fué desarrollado por DEC , Intel y Xerox , en este formato (mostrado en la fig. 2-12) existe una ligera diferencia con el de la IEEE 802.3.

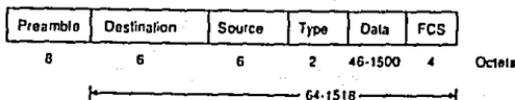


Fig.2-12."Formatos del Frame Ethernet".

El frame de Ethernet comienza con un preámbulo de 8 octetos , que están alternados de la siguiente forma 1010 , el cual finaliza con 10101011 , y proporciona la sincronización. La dirección de destino es un campo de 6 a 8 octetos y cada una define una dirección en el nivel físico ó una multicast de direcciones , la cual está determinada por el LSB (Bit Menos Significativo) del primer bit de este campo.

La dirección de un nivel físico es originada normalmente en una memoria ROM ; cuando se ajusta LSB=0 , ésta dirección es la única que cruza todas las redes Ethernet.

La multicast de direcciones puede ir a un grupo ó dirigirse a todas las estaciones si tenemos LSB=1 , en el caso de un direccionamiento dirigido , el campo se ajusta en 1's , siendo FFFFFFFFH , donde H significa la notación hexadecimal.

Las direcciones de los campos están subdivididas así :

Los 3 primeros octetos están contenidos en la manufactura de block (asignada por la IEEE) , y los 3 últimos octetos son asignados por el fabricante. El chip ROM contiene la dirección original que puede ser removida de la vieja tabla hacia una nueva tabla , ó la dirección puede ser ajustada en un registro usando el diagnostico NIC.

La dirección del origen , es la dirección de la estación que origina el frame.

El campo , conocido como Ethertype , contiene 2 octetos que especifican los protocolos de los niveles superiores usados en el campo de datos , algunos Ethertypes conocidos pueden ser 0800H (TCP/IP) y 0600H (XNS).

El campo de datos es sólo un campo de longitud variable que puede ser mínimo de 46 a un máximo de 1500 octetos.

Los contenidos de estos campos son completamente arbitrarios y también determinados por el protocolo usado en un nivel superior.

El último campo es un FCS , que es un CRC de 32 bits basado en los contenidos de dirección , tipo y campo de datos.

La longitud permitida de los frames no incluye el rango de preambulo (de 64 a 1518 octetos) , aquellos que se encuentren fuera de este rango se consideran inválidos.

2.6.2 IEEE 802.3.

El formato del frame IEEE 802.3 se muestra en la figura 2-13, este frame comienza con el preámbulo (7 octetos) que es un patrón alternado 1010 ; el siguiente es el SFD (Start Frame Delimiter) definido como 10101011. Hay que notar que el preámbulo de 802.3 y SFD están combinados en un patrón idéntico al preámbulo de Ethernet.

Al SFD le sigue la dirección destino, la cual puede ser de 2 a 6 octetos de longitud, siendo más común la de 6 octetos. El campo Individual/Group (I/G) corresponde a la designación de Ethernet Physical/Multicast, el campo Universal/Local (U/L) indica cuando la dirección es universalmente administrada (por la IEEE) ó localmente (por el administrador de red).

A la Dirección Destino le sigue la Dirección Origen (2 octetos para destino y 2 para fuente o bien 6 octetos para destino y 6 para origen, pero no 2 y 6). El campo Longitud es de 2 octetos e indica el número de octetos LLC en el campo de datos y requiere un mínimo de 46 octetos de datos, cuando el LLC es menor a 46, el campo Pad es usado. La máxima longitud de datos y el Pad utiliza 1500 octetos; hay que notar que el LLC PDU de 802.2 está completamente encapsulado dentro de la Unidad de Datos del frame 802.3 MAC.

Finalmente el FCS, esta basado en 32 bits CRC y es procesado de acuerdo a los contenidos de las direcciones Destino, Origen, Longitud, Unidad de Datos y Campo Pad.

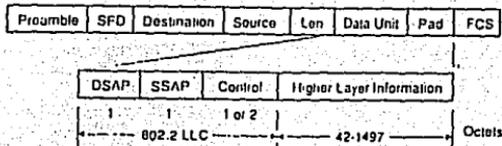


Fig.2-13."El formato Frame IEEE 802.3 MAC".

Considerando nuevamente las figuras 2-12 y 2-13, se nota la diferencia entre los frames de Ethernet y la IEEE 802.3. Primeramente, el 802.3 reemplaza el campo Type con el campo Length; entonces aparecen 2 diferencias, por un lado, los frames son de la misma longitud como en el nivel de enlace de datos pero a su vez son incompatibles con los de los niveles superiores. Por otro lado, si la longitud de los datos se especifica dentro de la frame Ethernet, algunos parámetros definidos por el nivel de red serán enviados. Además, la Ethernet no tiene Pad ya que los datos requieren de un mínimo de 46 octetos. Por esto, en Ethernet, el nivel de red puede considerar éstos parámetros y la longitud del Pad.

2.6.3 IEEE 802.5.

En una red Token Ring se definen dos tipos de Frame : "Tokens y Data/Command", como se muestra en la fig. 2-14.

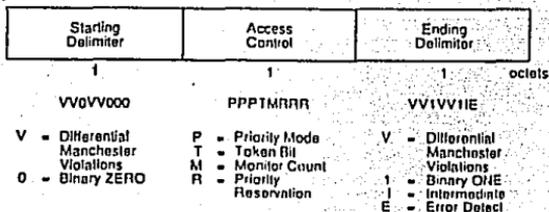


Fig.2-14."Formatos del Frame Token Ring IEEE 802.5".

Tokens

El Token tiene una longitud de tres bytes , los cuales son Start Delimiter , Access Control y End Delimiter. El primero informa a cada estación de la presencia de una señal ; éste campo incluye señales para distinguir su byte de los demás.

El Byte de Access Control contiene los campos de prioridad y reservación , así como un Token Bit , el cual es empleado para diferenciar un Frame Token de un Frame Data/Command , además contiene un monitor-bit el cual indica cuando un Frame está circulando infinitamente dentro de un Ring.

Finalmente el End Delimiter indica el fin de un Frame Token o un Data/Command. Este también contiene bits que indican un Frame dañado y el último Frame de la secuencia lógica.

Data/Command

Este tipo de Frames varía en tamaño , dependiendo de la longitud del campo de información. Los Frames de datos llevan la información a los protocolos de los niveles superiores ; y los Frames de comando contienen el control de la información.

Dentro del Frame Data/Command , se tiene el Byte Access Control (cuya función es similar al mencionado en el Frame Token) , seguido por el Byte Frame Control , que indica cuando el Frame contiene datos o control de información. En los Frames de control , éste Byte indica la forma de controlar la información. En seguida de estos se tienen dos campos de direcciones los cuales identifican a las estaciones origen y destino ; inmediatamente después se tiene el campo de datos , cuya longitud depende del tiempo en que la señal permanezca en la estación. Después del campo de datos , se tiene el campo de Secuencia de Chequeo de Frame (FCS) , a este campo la estación origen le asigna un cierto valor , y la estación destino calcula este valor para determinar si el Frame sufrió algún daño durante la trayectoria , si es así , el Frame es descartado. Finalmente se tiene el End Delimiter.

2.6.4 ARCNET.

ARCNET originalmente fué desarrollado por la Corporación Data Point , y no forma parte de los estándares del proyecto de la IEEE 802 , ésta arquitectura es un sistema sencillo que soporta los tres principales medios de transmisión : par trenzado , cable coaxial y fibra óptica ; y dos topologías bus y estrella.

Básicamente ARCNET tiene cinco formatos de Frame como se observa en la fig. 2-15. Primero se tiene la señal Invitación a Transmitir (ITT) , que es la señal que permite el paso de control de una workstation a otra. Segundo el Free Buffer Enquiry (FBE) , el cual es una señal enviada por la estación que desea transmitir y desea saber si la estación receptora tiene suficiente espacio en su Buffer para que el Frame pueda ser recibido. El Packet (PAC) es el Frame mismo , que puede contener hasta 508 octetos de datos de mensaje. Un Acknowledgment (ACK) que confirma la recepción del paquete o que indica una respuesta positiva al FBE. El Negative Acknowledgment (NAK) , el cual indica el rechazo del paquete o una respuesta negativa al FBE.

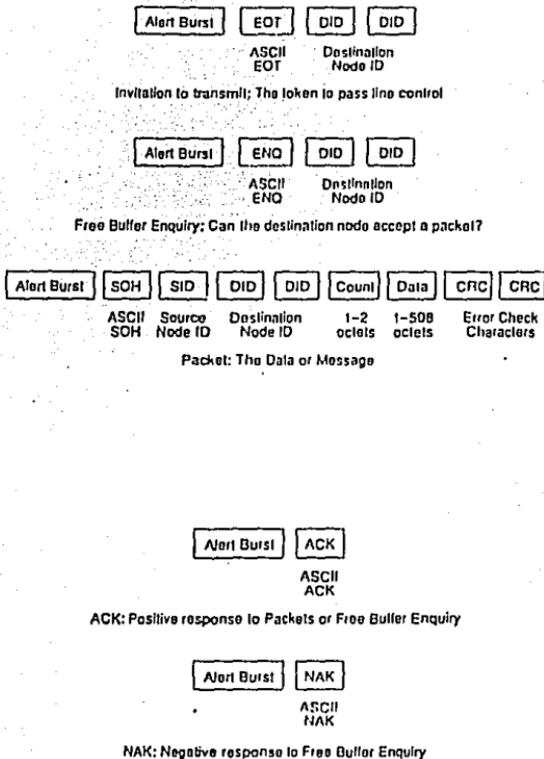


Fig.2-15."El formato del Frame ARCNET".

2.6.5 FDDI (Fiber Data Distributed Interface).

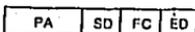
Es una red que maneja velocidades de 100 Mbps desarrollada por la ANSI, y asocia un gran número de estándares en redes LAN y MAN; la red LAN-FDDI está sustentada físicamente por un bus de fibra óptica, semejante a la IEEE 802.5, a su vez los formatos de Frame FDDI guardan una similitud con el definido para 802.5. El esquema de codificación empleado en FDDI define un "Symbol" el cual es equivalente a 4 bits. El primer formato de FDDI se observa en la Fig. 2-16a, el cual consiste de cuatro campos, primeramente por el "Preamble" de 16 símbolos, que es usado para sincronización; el Starting Delimiter (SD) formado por 2 símbolos, el cual indica el comienzo del Frame. El Frame Control (FC), de dos símbolos, el cual define el tipo de Frame y la función; los subcampos son:

C : Clase de Frame (Síncrono y Asíncrono).
 L : Longitud de la Dirección del Frame (16 a 48 bits).
 F : Formato de Frame (define los datos MAC y LLC).
 Z : El control de Bits MAC (El cual indica el tipo de Frame MAC).

El Frame "Ending Delimiter" (ED) de dos símbolos, el cual indica el final del Frame; el segundo formato FDDI de la fig. 2-16b contiene cuatro campos entre el FC y ED.

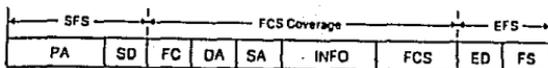
DA : Dirección de destino (de 4 a 12 símbolos del mismo formato IEEE 802).
 SA : Dirección de origen (acompañado por-DA).
 INFO : Información variable.
 FCS : Frame que chequea secuencia, a 32 Bit de redundancia cíclica (8 símbolos).

El Ending Delimiter (de un símbolo) indica el final del Frame; el estado del Frame FS (de 3 símbolos), incluye detección de errores (E), reconocimiento de direcciones (A) y Copia de Frame (C), como en IEEE 802.5.



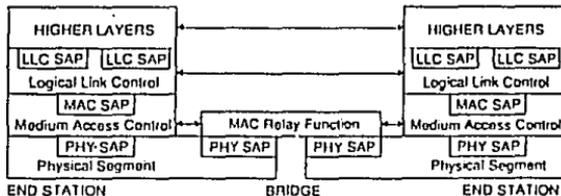
PA = Preamble (16 or more I symbols)
 SD = Starting Delimiter (1 JK symbol pair)
 FC = Frame Control (2 symbols)
 ED = Ending Delimiter (2 T symbols)

Fig.2-16a."Formato del Token FDDI".



SFS = Start of Frame Sequence
 PA = Preamble (16 or more I symbols)
 SD = Starting Delimiter (1 JK symbol pair)
 FC = Frame Control (2 symbols)
 DA = Destination Address (4 or 12 symbols)
 SA = Source Address (4 or 12 symbols)
 INFO = Information (0 or more symbols)
 FCS = Frame Check Sequence (8 symbols)
 EFS = End of Frame Sequence
 ED = Ending Delimiter (1 T symbol)
 FS = Frame Status (3 or more R or S symbols)

Fig.2-16b."Formato del Frame FDDI".



LEGEND:
 PHY = Physical Layer
 MAC = Medium access control sublayer
 LLC = Logical link control sublayer
 SAPI = Service access point

Fig.2-17."Flujos de protocolo para LAN's puenteadas".

2.7 Estándares bridging de la IEEE.

Recordemos que un bridge es un dispositivo , cuya función es relevar frames de datos de un segmento a otro , de tal manera que todos los segmentos aparezcan como una LAN completa. En la figura 2.17 se muestra el modelo de arquitectura de un bridge , en la cual se observa la relación de protocolos pares (indicados por líneas horizontales). Primero cada segmento tiene sus propios niveles físico y Control de Acceso al Medio (MAC). Segundo , tanto los protocolos de los niveles LLC y de los niveles superiores pasan en forma transparente a través del bridge , por otro lado , el bridge es independiente del protocolo del nivel más alto. Tercero los bridges no proporcionan control del flujo de datos ; por lo mismo existe la posibilidad de saturación. Cuando esto ocurre cualquier Frame que fué descartado o que se perdió será recuperado por un proceso de protocolo en los niveles más altos.

Desde que algunos Frames serán enviados (pasan a través del bridge de relevo) y otros serán filtrados (no pasan a través del bridge de relevo) , entonces surge una pregunta : ¿Cómo es que el bridge tomó la decisión de relevo? , para hacer esto existen dos métodos que pueden ser empleados por el bridge :

Transparent Bridging (TB) y Source Routing (SR).

2.7.1 Método Transparent Bridging.

El método toma este nombre porque la decisión de relevo existe en el bridge , siendo totalmente transparente a las workstations que se están comunicando. El método realiza tres funciones distintas :

- 1) Envío de Frame (Frame forwarding).
- 2) Reconocimiento de las workstations (Learning workstation addresses).
- 3) Asegurar que no existan loops en la topología física.

La primera función, Frame Forwarding, es mostrada en la figura 2-18, de la workstation A a la B solo se tiene tráfico en la LAN 1 y no es necesario hacer un relevo a la LAN 2. El tráfico desde la LAN 1 a la LAN 2 (por ejemplo de la workstation B a la C) es relevado por el bridge 1, pero es ignorado por el bridge 2. El tráfico de la LAN 1 a la LAN 3 (de la Workstation A a la E) es relevado tanto por el bridge 1 como el bridge 2.

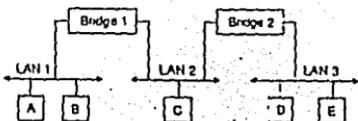


Fig.2-18."Bridge Forwarding".

La segunda función del método TB, Learning Workstation Addresses, es hecha monitoreando tanto los puertos de entrada como los de salida. Una base de datos (en cualquier lado del bridge) es creada para "escuchar" todas las transmisiones (proceso conocido como Learning). El bridge guarda una lista de las estaciones que van a transmitir a cada uno de los puertos, por eso tiene la decisión de enviar (Forwarding) o filtrar (Filtering) basada en la dirección del nivel MAC (ver fig. 2-19).

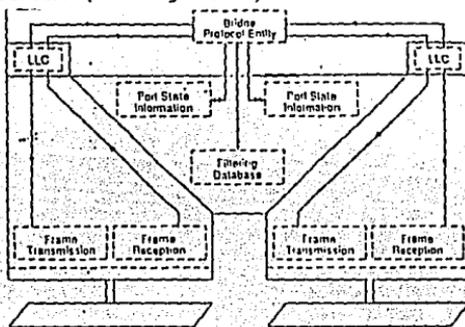


Fig.2-19 "Operación de protocolo Inter-Bridge".

La tercera función proporciona sobre todo el control en la operación de relevo (observada en la figura anterior por el Bridge Protocol Entity). La topología empleada por el TB es una red Spanning Tree, en la cual se tiene sólo un camino (no dos ni más) desde la LAN 1 a la LAN 2 así que no existe la posibilidad de un loop (fig. 2-20), si la workstation A transmite un frame (con dirección destino conocida), tanto el bridge 1 como el 2, deben enviar el frame a su destino. Un loop causara que pasen infinitamente frames de la LAN 1 a la LAN 2, dando un nuevo significado al mensaje original; para eliminar el loop, uno de los bridges debe ser desconectado teniendo entonces sólo un camino de la LAN 1 a la LAN 2.

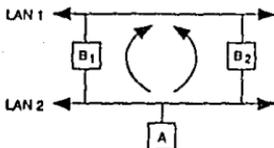


Fig.2-20."Loop de bridges".

El algoritmo que toma la topología de la red física y además crea un Spanning Tree "lógico" es conocido como el Algoritmo Spanning Tree. El bridge se comunica con cada uno de los otros a través de mensajes conocidos como BPDU (Bridge Protocol Data Units). Este algoritmo define a un bridge como Base, por lo mismo los demás Bridges transmiten frames en dirección de éste. El Bridge Base es seleccionado dependiendo de la transmisión de los BPDUs, y de la decisión de la trayectoria más corta. Un ejemplo es la norma IEEE 802.1d, la cual muestra una topología física (fig. 2-21) que al emplear el algoritmo llega a ser una topología lógica mostrada en la fig. 2-22, finalmente el resultado se muestra en la fig 2-23, donde se observa que el bridge 1 se toma como Base, y los bridges 3 y 5 se han desconectado lógicamente. El Algoritmo Spanning Tree, define la topología lógica como sigue:

El Bridge 1 conecta a las LAN 1 y 2, el bridge 2 conecta las LAN 1 y 3, así como también las LAN 1 y 4 y finalmente el bridge 4 conecta las LAN 2 y 5.

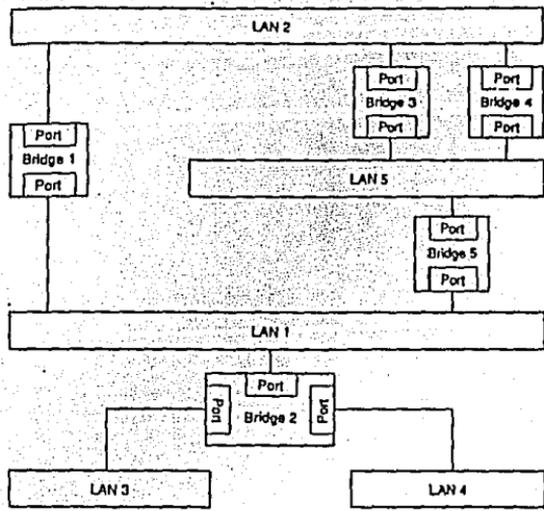


Fig.2-21."LANs PUENTEADAS".

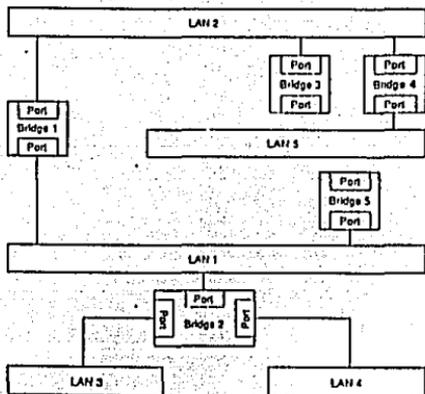


Fig.2-22."Topologia de red puentada".

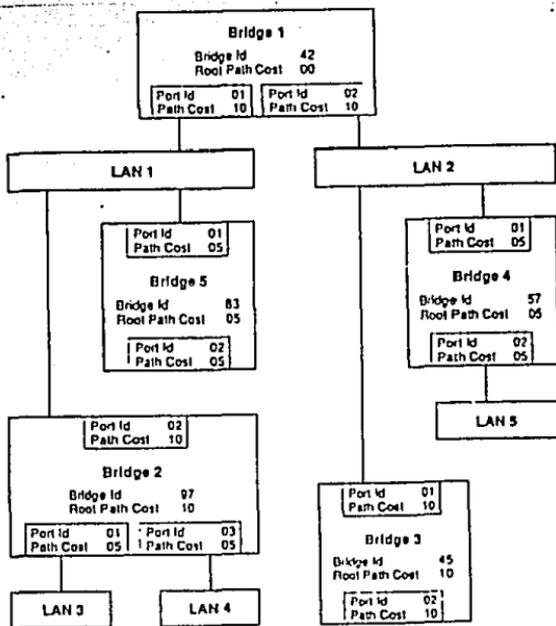


Fig.2-23."Spanning Tree".

2.7.2 Método Source Routing.

El algoritmo Source Route Bridging (SR) fué desarrollado por la IBM , y propuesto por la IEEE 802.1. Este algoritmo es utilizado por muchas LANs.

El algoritmo SR determina la ruta origen-destino , y se localiza en todos los frames Inter-LAN (transmitidos por el origen) ; el SR almacena y envía los frames según se observa en la fig. 2-24. Haciendo referencia a ésta figura y considerando que el Host X desea transmitir frames al Host Y (donde tanto el Host X como el Y pueden o no estar conectados a la misma LAN) para que el Host X determine la localización del Host Y , el primero transmite un frame de prueba el cual regresa nuevamente al Host X , éste frame de respuesta puede ser positivo ó negativo , el cual indicará si se localizó o no el Host Y ; de esta forma el Host X considera que el Host Y se encuentra en un segmento remoto.

Para determinar su ubicación , el Host X transmite un frame explorador el cual es recibido en cada uno de los bridges (en este ejemplo los Bridges 1 y 2) , siendo a su vez copiado por los puertos de destino , posteriormente la información es ruteada y agregada al frame explorador , ya que éstos viajan a través de la internetwork.

El Host Y contesta a cada frame , y almacena la información ruteada , una vez recibidas todas las respuestas de los frames en el Host X , se elige un camino basado en un criterio predeterminado.

En ésta misma figura , éste proceso puede elegir 2 rutas :

LAN 1 - Bridge 1 - LAN 3 - Bridge 3 - LAN 2

LAN 1 - Bridge 2 - LAN 4 - Bridge 4 - LAN 2

donde el Host X debe seleccionar una de éstas 2 rutas.

Las especificaciones de la IEEE 802.5 no siguen un criterio para seleccionar la ruta y toman en cuenta :

- El camino que contiene el primer frame.
- Respuesta con el mínimo número de hops (saltos).
- Respuesta que permite el tamaño del frame.

Posteriormente la ruta es seleccionada y es insertada dentro del frame en forma de un Campo de Información de Ruteo (RIF) , el cual se incluye en éste frame (de origen a destino).

La información de ruteo dentro del frame es indicada por el Bit Más Significativo contenido en el campo de dirección origen (conocido como el Routing Information Indicator (RII)).

2.7.2.1 Formato del Frame.

El RIF de la IEEE 802.5 tiene la estructura que se muestra en la figura 2-25 , en la cual se observa que el subcampo RIF indica cuando el frame debe ser ruteado a un solo nodo , a un grupo de nodos que forman un Spanning Tree , o a todos los nodos.

El primer tipo de frame es llamado "Routed Frame" , el segundo es conocido como Spanning Tree Explorer , el tercero es llamado como All-Paths Explorer. El Spanning Tree Explorer puede ser usado para transportar frames , para reemplazar los caminos explorados y preguntar por las rutas.

Dentro del campo Routing Control se incluyen los siguientes campos :

El subcampo Length indica el total de Bytes del RIF.

El bit D indica la dirección del frame (adelanto u atraso).

El campo Largest indica que tan grande es el frame que puede ser manejado a lo largo de la ruta.

Por otro lado dentro del campo Route Descriptor se tiene un par de números (uno de ring y uno de bridge) , que especifican la parte de una ruta. Las rutas simplemente alternan secuencias de LANS y números de Bridge que comienzan y terminan con las numeradas.

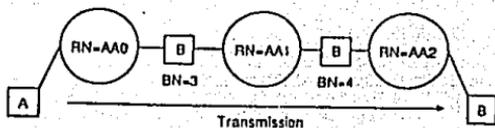


Fig.2-24."Ejemplo de una red empleando el método SR".

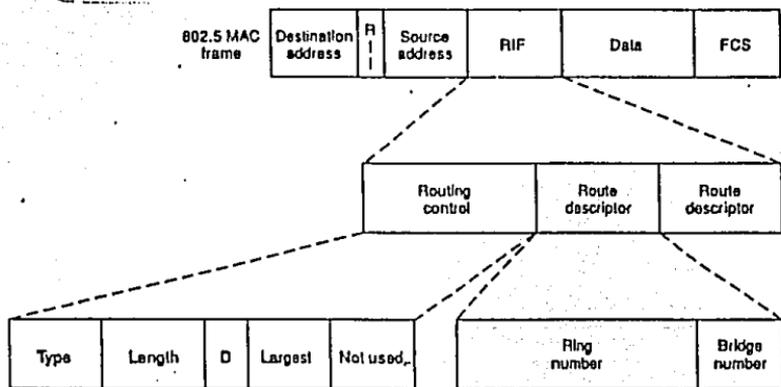


Fig.2-25."Campo RIF de IEEE 802.5".

2.7.3 Método Source Routing Transparent.

Recordando que el método TB (Transparent Bridging) ha sido ampliamente usado en redes IEEE 802.3 y el SR (Source Routing) fué diseñado para IEEE 802.5. Ahora, ¿Qué pasa si se necesita conectar una red basada en el método TB a una red basada en el SR? Se tienen entonces 2 opciones: Lo primero que se piensa es en la combinación de los 2 métodos. Por ejemplo, el Bridge LAN 8209 de la IBM es una configuración, la cual conecta una red Ethernet IEEE 802.3 por un lado y por el otro una red IEEE 802.5. Desafortunadamente, esta realización requiere que la red sea segmentada en 2 dominios.

La segunda opción sería, emplear el Método Source Routing Transparent (SRT). Como su nombre lo implica, el algoritmo SRT combina ambos métodos:

- El Source Routing es ejecutado cuando un frame es recibido con RII=1 (indicando la presencia del campo RI).
- El Transparent Bridging es empleado cuando un frame es recibido con un RII=0 (indicando la ausencia del campo RI).

El estándar del método SRT define la operación de 2 tipos de redes, en donde ambas tienen un campo RI definido:

IEEE 802.5/ISO 8802-5 Token Ring

ANSI X3.139/ISO 9514 FDDI

La operación del algoritmo SRT es ilustrada en la fig. 2-26. Existen 2 secciones lógicas dentro de la entidad de relevo MAC del bridge: SR y TB. Los frames entrando a la entidad MAC con RII=0 (ninguna fuente ruteada) son enviados ó descartados de acuerdo al método TB. Si el frame recibido tiene un RII=1 (fuente ruteada), entonces el SR lógico depende del tipo de frame recibido.

El algoritmo SRT tiene muchas ventajas; la habilidad de mezclar los métodos SR y TB en la misma LAN elimina la previa incompatibilidad entre las 2 técnicas. Por ende, las estaciones SR y las estaciones TB pueden comunicarse, teniendo la conectividad asegurada. Finalmente, desde que el método SRT aplica ambos estándares ANSI FDDI e IEEE 802, se garantiza un camino hacia el backbone de FDDI.

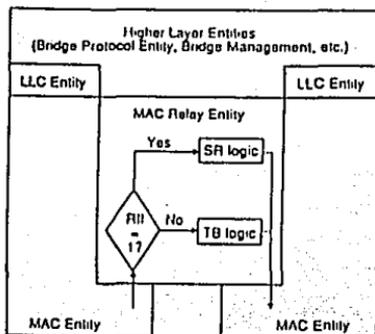


Fig.2-26." Operación Lógica del Bridge empleando el Método SRT".

C A P I T U L O T R E S

"ESCENARIOS DE LA INTERNETWORKING: LAN-TO-LAN Y LAN-TO-WAN"

- 3.1 DISEÑO DE LA CONEXION LAN TO LAN .
- 3.1.1 ¿ QUE DISPOSITIVO EMPLEAR ?
- 3.1.2 ANALISIS DE LA RED.
- 3.2 CONEXION DE REDES LAN DE ARQUITECTURAS
 DISTINTAS.
- 3.2.1.a REPETIDORES.
- 3.2.1.b BRIDGES.
- 3.2.1.c ROUTERS.
- 3.2.1.d BROUTERS
- 3.2.1.e GATEWAYS.
- 3.3 INTERNETWORKING LAN TO WAN.
- 3.3.1 DISEÑO DE LA CONEXION LAN TO WAN.

CAPITULO TRES

ESCENARIOS DE LA INTERNETWORKING: LAN-TO-LAN Y LAN-TO-WAN.

Después de haber analizado y estudiado la variedad de estándares que son empleados tanto en redes LAN como en dispositivos de internetworking (repetidores , bridges , ruteadores y gateways) , es hora de empezar con la revisión de los productos que hacen posible la conexión entre redes de comunicación.

3.1 Diseño de la conexión LAN to LAN.

Básicamente se puede hablar de tres razones principales que han orillado a los manejadores y/o diseñadores de redes de comunicación para buscar un desarrollo con el cual se puedan satisfacer las necesidades de sus clientes.

Primero , la abundancia de PC's ha traído como consecuencia un tremendo crecimiento en el número de estaciones de trabajo que son conectadas a una red LAN. Un crecimiento anual de 100 a 200 por ciento de estaciones de trabajo por red es común.

Segundo , el número cada vez mayor de empresas que se fusionaron , mas aparte todas aquellas que se consolidaron , han forzado el desarrollo de redes de comunicación enormes que a su vez están basadas en infraestructuras considerables.

Tercero , con relación a las dos anteriores , hoy en día se tiene la necesidad de conectar redes en diferentes áreas geográficas ; a éste requisito hay que agregarle otra variable a el diseño : la facilidad de transmisión en una red WAN.

3.1.1 ¿Qué dispositivo emplear?

Aquí se empezará con una información general sobre la selección correcta que debe hacerse del hardware y software más conveniente para el diseño de la internetwork. Las consideraciones que se toman en cuenta para realizar la planeación de la internetworking están dadas según las necesidades que se tengan : múltiples opciones de medios de transmisión , arquitecturas distintas de las redes LAN , manejo de protocolos diferentes , incompatibilidad entre programas de aplicación , etc. También hay que tomar en cuenta que la red de comunicaciones en sus inicios será relativamente pequeña (por ejemplo , menos de 30 nodos) y que en su crecimiento podrá llegar a ser tal vez el doble ó el triple del tamaño (y capacidad) de la red en un principio.

Existen 5 dispositivos de internetworking que pueden ser empleados durante el crecimiento : repetidores , bridges , routers , ruteadores y gateways. En la tabla 3-1 se presentan las características principales de los dispositivos antes mencionados.

Repetidor	Opera en el nivel físico del Modelo OSI. Regenera las señales físicas. Se emplea para extender la longitud de la red LAN.
Bridge	Opera en el nivel enlace de datos del Modelo OSI. Separa lógicamente los segmentos de la red. Es independiente de los protocolos en los niveles superiores. Empleados para manejar el tráfico en la red LAN.
Router	Opera en los niveles enlace de datos y red del Modelo OSI. Combina la transparencia en el manejo del protocolo de un bridge con la habilidad para rutear ciertos protocolos. Empleado en redes que manejan tráfico de protocolo variado.
Router	Opera en el nivel de red del Modelo OSI. Separa lógicamente las subnetworks. Depende del protocolo manejado en el nivel de red. Reconocen la topología de la red en la cual van a trabajar.
Gateway	Opera en los siete niveles del Modelo OSI. Realiza conversiones de protocolo. Se emplea según la aplicación del usuario.

Tabla.3-1. "Comparación de los dispositivos empleados en la internetworking".

3.1.2 Análisis de la Red.

Para realizar el análisis de la red, se considera el siguiente ejemplo. El tráfico en ella se ha incrementado al pasar el tiempo y por consiguiente, los usuarios se quejan por los largos retrasos ó tiempos de respuesta muy grandes. Con ayuda de la figura 3-2, se describe lo que está pasando gráficamente tomando como base una investigación hecha en redes CSMA/CD.

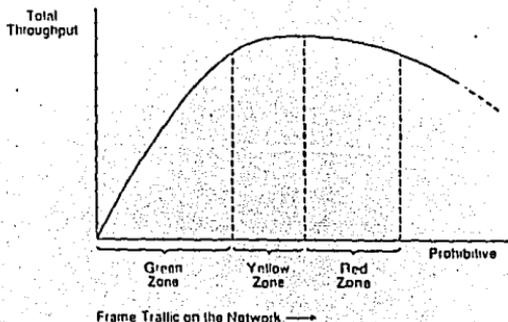


Fig.3-2. "Throughput en la red CSMA/CD como una función del tráfico en ella".

Las redes CSMA/CD operan eficientemente bajo cargas ligeras ó medianas de tráfico. Mientras más estaciones de trabajo intenten el acceso a la red, el throughput empezará a caer, como se ve en la figura 3-2. Si el número de estaciones de trabajo crece, entonces se incrementa el tráfico en la red. En cierto punto (como se muestra en la zona roja de la figura antes mencionada), el throughput total empezará a declinar. La mayor parte de éste decremento es causado por colisiones de frame. En el momento en que dos frames chocan, el algoritmo de la red CSMA/CD requiere que ambas vuelvan a intentar la transmisión en un momento posterior.

Mientras más tráfico exista se crearán mas colisiones , las cuales provocarán que más estaciones tengan que esperar un cierto tiempo para poder transmitir ; debido a que el número de estaciones que esperan transmitir es mayor , se tendrán más colisiones por lo que el throughput se irá para abajo. Las colisiones aumentan el tiempo que la red emplea para efectuar la transmisión de datos.

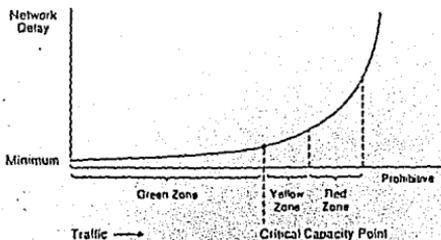


Fig.3-3."Retraso en la red CSMA/CD como una función del tráfico en ella".

Un segundo intento para el análisis de la red , es medir el retraso que hay en ella (el tiempo requerido para acceder a la red y llevar a acabo la transmisión a un nodo distante). En la figura 3-3 , se muestra que éste retraso se mantiene estable y es menor a un 20 por ciento de la capacidad de la red CSMA/CD.

Este parámetro (el retraso) no debe ser confundido con otros dos totalmente distintos : Capacidad de la Red y Utilización de la Red. La Capacidad de la Red es la máxima velocidad de transmisión (en Mbps) que maneja la red. Por ejemplo ,una red

Ethernet tiene una capacidad máxima de 9,922,048 bps cuando se considera un intervalo de 9.6 microsegundos entre frames y no los 10 Mbps de los que se habla por lo general. La Utilización de la Red es una relación del número de bits transmitidos entre el máximo posible de bps en un periodo dado. Una utilización típica de la red se encuentra entre 20 y 30 por ciento.

Para las redes CSMA/CD, el funcionamiento está directamente relacionado con el tipo de dispositivo que está generando éste tráfico.

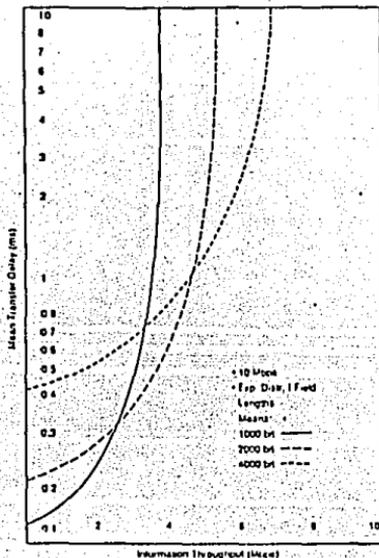


Fig.3-4a. "Relación Retraso-Throughput en una red CSMA/CD cuya velocidad de transmisión es de 10 Mbps".

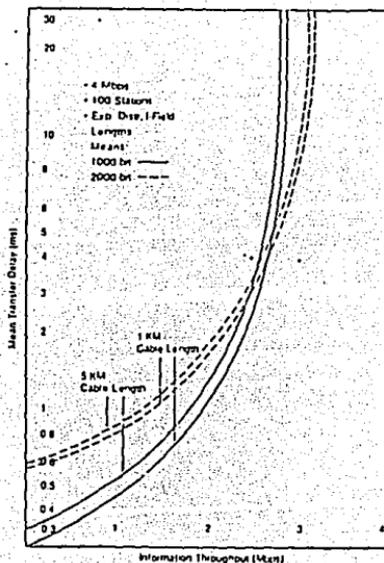


Fig.3-4b."Relación Retraso-Throughput en una red Token Ring a una velocidad de transmisión de 4 Mbps".

Una investigación realizada por IBM ha comparado redes CSMA/CD y Token Ring obteniendo resultados similares. Las redes CSMA/CD muestran alguna variación en el punto de inestabilidad el cual se basa en la longitud media de el Campo de Información. En todos los casos , ésta inestabilidad ocurre entre un throughput de 2 y 4 Mbps (ó entre 20 y 40 por ciento del máximo) de un total de 10 Mbps de la capacidad de la red (fig. 3-4a). Las redes Token Ring presentan características similares cuando la velocidad de transmisión es 4 Mbps (fig. 3-4b) o 16 Mbps (fig. 3-4c).

Para éstos casos , el punto de inestabilidad ha cambiado aproximadamente a un 80 por ciento del throughput máximo. De todo lo anterior se puede concluir que ninguna de las dos redes alcanza un throughput o una utilización de red del 100 por ciento. Por lo que cuando el tráfico crece , los dispositivos de internetworking deben incluirse para ayudar a mantener estable el funcionamiento de la red.

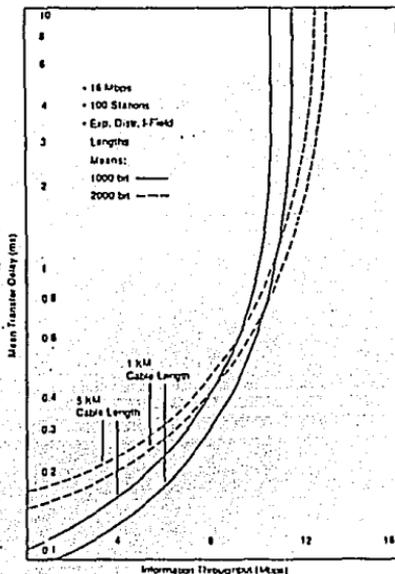


Fig. 3-4c. "Relación Retraso-Throughput en una red Token Ring que maneja una velocidad de transmisión de 16 Mbps".

3.2 Conexión de redes LAN de arquitecturas distintas.

Un punto que es muy importante considerar dentro del diseño de internetworking , es cuando se requiere realizar la conexión de dos (o más) redes LAN cuyas arquitecturas son distintas , por ejemplo una red Ethernet y una red Token Ring. Por lo que surge una pregunta : ¿Cómo es posible conectarlas? Por lo general hay tres métodos usados comúnmente : Emplear un bridge para realizar la conexión LAN a LAN ; Puenteo Interno (Ruteo) en un Server o hacer uso de un protocolo común como el TCP/IP.

El bridge LAN a LAN es la solución más limitada , es la configuración mas común de un bridge para conectar una Ethernet a una Token Ring. Una desventaja al usar éste producto , es que hay que considerar hardware adicional cuyo costo en muchas ocasiones es muy elevado.

En contraste con la solución de hardware , la internetworking en el Server ofrece una solución de software a el problema de conectividad. Básicamente opera en un sistema conocido como Network Operating Systems (NOS) , por ejemplo Novell Netware , el cual tiene una arquitectura que facilita la solución para la internetworking. El NOS se divide en tres componentes generales : Un driver para el hardware NIC (Network Interface Card) - opera en los niveles físico y enlace de datos de OSI - ; protocolos de internetworking - trabaja en los niveles de red y transporte - , mas el soporte de programas de aplicación - niveles de sesión , presentación y aplicación.

En el Server , se instalan dos (o más) NICs distintas. Cada NIC tiene una dirección de hardware única y recibe la información en el nivel superior desde una NOS driver. En otras palabras , un driver Ethernet se comunica a la Ethernet NIC con dirección de hardware A , y un driver Token Ring se comunica con un Token Ring NIC que tiene dirección de hardware B. Si todos los protocolos en los niveles superiores son los mismos , la comunicación entre éstas arquitecturas distintas se realiza de manera automática.

La tercera opción que se presenta , es realizar la conexión por medio de un protocolo común que manejen ambos sistemas de comunicación. El protocolo comúnmente empleado y que de hecho fué realizado con éste propósito es el TCP/IP. Si ambos sistemas distintos presentan la facilidad para emplear el TCP/IP , entonces la conexión llega a ser posible.

A continuación se presenta una serie resumida de las características de los repetidores , los bridges , los routers , los brouters y las gateways.

3.2.1.a Repetidores.

Son dispositivos que operan sólo en el nivel Físico del modelo de referencia OSI. Los repetidores solamente amplifican y regeneran las señales que son recibidas desde un segmento de LAN , así que al hacer la retransmisión hacia otro segmento la señal se recibe con buena calidad.

Los repetidores presentan las siguientes ventajas :

- Son muy simples y es nula la probabilidad de que se encuentren errores dentro de ellos , así que trabajan o no trabajan.
- Son transparentes a los protocolos. Permiten el paso de mensajes formateados en cualquier protocolo.
- Proporcionan la misma eficiencia en el throughput de datos que tiene el segmento de LAN al que se conectan.
- Proporcionan separación de problemas eléctricos en un segmento de LAN los cuales no afectan en lo absoluto a otros segmentos en la red.

Desventajas :

- Debido a que permiten el paso desmedido de paquetes , se crea el tráfico y la congestión en los segmentos de LAN.
- Operan sólo en modo local.

3.2.1.b Bridges.

Los bridges son dispositivos que operan en el Subnivel Control de Acceso al Medio (MAC) del nivel enlace de datos de OSI. Son ideales cuando se tienen dos redes que emplean protocolos distintos en sus niveles superiores, siempre y cuando éstas redes manejen el mismo subnivel MAC. Los bridges son dispositivos que toman la decisión de dejar pasar o no frames a otro segmento de LAN, a ésta toma de decisiones se le conoce como filtering (filtrado o filtración).

Por otra parte, los bridges operan ya sea en el modo local (fig. 3-5) o modo remoto (fig.3-6), en donde se emplean dos bridges manejando transmisión full duplex; independientemente del modo de operación, todos los bridges funcionan bajo los siguientes pasos:

1. El bridge conectado a la LAN transmisora recibe los frames y los filtra.
2. Si la LAN destino está conectada a un bridge remoto, el frame es enviado a éste bridge.
3. Cuando el frame finalmente se encuentra en la memoria del bridge remoto, éste retransmite el frame a la LAN destino.

Los bridges presentan las siguientes ventajas:

- Son bastantes simples en comparación con los ruteadores y las gateways, por lo que su instalación, operación y mantenimiento es más fácil.
- Son transparentes a los protocolos.
- Los bridges de alto funcionamiento proporcionan la misma efectividad en el throughput de datos como la LAN a la que están conectados.
- Implementan condiciones altamente complejas de filtrado. Gracias a esta opción de filtrado, se limita la cantidad de tráfico que fluye entre los segmentos de red, lo que trae como consecuencia un mejor funcionamiento en ella.
- Los bridges pueden trabajar con distintos tipos de cables físicos de LAN; por ejemplo, desde una Ethernet manejando cable coaxial grueso a una Ethernet empleando par trenzado.

Las desventajas que se tienen son :

- Probabilidad grande de que dejen de trabajar repentinamente.

- No tienen la capacidad de convertir protocolos. Así que los protocolos manejados por ambas redes LAN deben de ser compatibles.

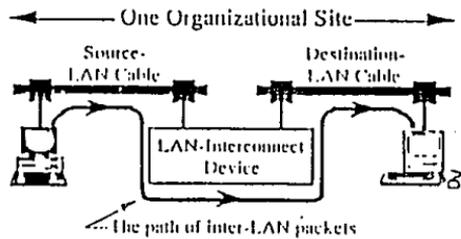


Fig.3-5."Operación de un dispositivo de interconexión local".

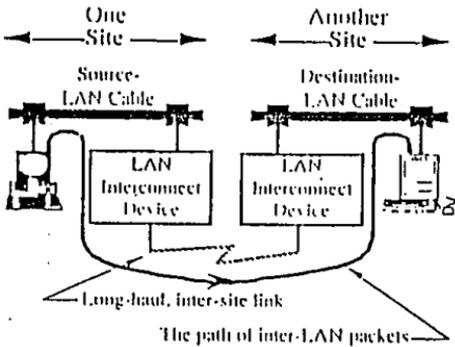


Fig.3-6."Operación de un dispositivo de interconexión remoto".

3.2.1.c Routers.

Un router opera en los tres primeros niveles del Modelo de Referencia OSI. Trabajan en el modo local, remoto ó en ambos modos; a pesar de algunas limitaciones de funcionamiento por lo general son usados en el modo remoto.

En éste modo, se conectan un gran número de routers a través de diferentes medios de transmisión (cubriendo grandes distancias), por los cuales los routers se organizan para emplear técnicas de conmutación de paquetes. De manera que las redes que contienen routers pueden tener todas las características que son asociadas con las redes de conmutación de paquetes: adaptación al ruteo, reruteo automático alrededor de troncales que han fallado, balanceo de la carga a través de troncales paralelas, control en la congestión del tráfico, etc.

Debido al funcionamiento del router en el nivel de red, es indispensable que la mayoría de protocolos de LAN se sujeten a la siguiente condición: que el emisor de un paquete debe proporcionar la información del encabezado del nivel de red, con el cual se identifica tanto la estación destino como la LAN a la cual ésta estación pertenece. Un router usa ésta información para enviar cada paquete a la LAN destino.

La diferencia entre los routers y los bridges son dos:

1.- Los bridges trabajan con los frames de datos transferidos por los niveles de enlace de datos de las dos estaciones. Mientras que los routers trabajan con los paquetes de datos transferidos en los niveles de red de las dos estaciones y determinan, cómo los paquetes van a ser ruteados usando la información contenida dentro de ellos.

2.- Los bridges son transparentes a las estaciones que se están comunicando; mientras que con el uso de los routers se requiere que las estaciones direccionen sus paquetes de datos cuando los servicios de ruteo son requeridos.

Ventajas de los routers:

- Crean muchas subnetworks lógicamente diferentes dentro de las Internetworks.
- Mantienen la información y determinan el camino más eficiente para la transmisión de datos.

- Cada router conoce las direcciones del nivel MAC del siguiente router conectado , así que las direcciones en el nivel MAC no tienen que ser convertidas dentro de un formato diferente antes de transmitir un paquete.

- Los routers se comunican unos con otros en un cierto periodo para determinar en que momento pueden acceder a otras redes. Estos mensajes son usados por los routers para construir y actualizar las tablas de ruteo .

- Manejan esquemas de ruteo dinámico que se ajustan a las condiciones de cambio de la red.

- Así como los bridges , los routers tienen la capacidad de separar las fallas en un segmento del cable de la red LAN.

Desventajas de los routers :

- Dependen de gran medida del protocolo. Deben primero entender el protocolo que maneja la LAN para que pueda ser empleado en su nivel de red.

- Los múltiples caminos proporcionan incremento en la probabilidad de falla.

3.2.1.d Brouters.

Son dispositivos que operan en los tres primeros niveles del modelo de referencia OSI : físico , enlace de datos y red. El brouter también es conocido como un bridge que rutea , ya que es diseñado para proporcionar la velocidad de procesamiento de un bridge con las capacidades de internetworking de un ruteador.

Recordemos que los bridges son dispositivos independientes de los protocolos por su característica de filtración basada en las direcciones de los frames del nivel de enlace de datos ; los ruteadores presentan la otra cara ya que ellos eligen el camino de ruteo basados en la direcciones dentro del nivel de red. Por lo anterior , los ruteadores son dispositivos dependientes del protocolo y por ende , deben antes entender el protocolo en el nivel de red en uso ; tal como IP , IPX , DECnet o algún otro. Se tiene entonces que un brouter es un dispositivo híbrido de un bridge y un ruteador : proporciona la independencia del protocolo de un bridge , mientras añade la capacidad de direccionar el tráfico de una red hacia

otras. Por lo tanto , desde que los ruteadores manejan ciertos protocolos en específico , los brouters tienen la habilidad de rutear los paquetes por medio de los protocolos soportados tales como el TCP/IP y por otra parte , proporcionan una función de bridge para otros protocolos , por ejemplo , el LAT (Local Area Transport) de DEC.

3.2.1.e Gateways.

Operan en los siete niveles del modelo de OSI.

La función principal realizada por una gateway , es la conversión de un paquete formateado en un cierto protocolo a otro. Estos son dispositivos de internetworking empleados para propósitos generales ya que pueden trabajar con cualquier tipo de dispositivo y no sólo para la integración de redes de comunicación.

Las gateways operan cuando reciben un paquete de cierto protocolo y entonces le quitan todos los encabezados de cada nivel del mensaje original. El mensaje original entonces es expresado de otra manera (por ejemplo , conversión de código de carácter) , agregándosele encabezados nuevos y enviándose dentro del frame correspondiente al nuevo protocolo. En general , la mayoría de las gateways opera con un protocolo de LAN manejando en un lado , por ejemplo Novell Netware y por el otro lado empleando un protocolo serial de bit , por ejemplo SNA/SDLC de IBM.

Ventajas de las gateways :

- Implementan un alto grado de filtrado y transformaciones de formatos de paquetes.
- Son bastante seguras.
- Ejecutan conversiones completas de protocolos así como conversiones del medio físico de transmisión.
- Son hábiles para separar las fallas presentadas en un segmento de LAN.

Desventajas de las gateways :

- Se requieren métodos más complejos para conectarlas.

- Operan a menor velocidad que cualquier otro dispositivo de internetworking debido a que necesitan realizar los procesos en los siete niveles , aparte del manejo de conversión de protocolos.

- Son difíciles de instalar , configurar , operar y mantener.

3.3 Internetworking LAN to WAN

Las redes LAN (Local Area Network) se establecen con el fin de conectar entre sí diversas computadoras y dispositivos periféricos que se encuentren próximos unos a otros. Normalmente las redes LAN no rebasan una distancia de un kilómetro. Por el contrario , las redes WAN (Wide Area Network) conectan computadoras a grandes distancias , varios cientos de kilómetros. Pueden existir redes WAN tanto públicas como privadas. Por otra parte , las redes MAN (Metropolitan Area Network) que son el término medio entre las redes LAN y WAN , deberán cubrir en el futuro las necesidades de comunicación regional , especialmente en zonas metropolitanas.

Desde sus comienzos el mercado informático ha desarrollado una actividad creciente como consecuencia del avance en el sector de las computadoras , y son muchos los fabricantes que se han establecido en áreas especializadas. La consecuencia de ello es que ha surgido para el usuario una amplia oferta en el mercado de PC's y redes de comunicación que necesariamente da a lugar a nuevos impulsos en lo relativo a la organización de las redes.

Actualmente , y como resultado de la conexión de computadoras en red , se ha logrado el punto clave para la mejora del sistema : La integración de los servicios. Para poder realizar en el futuro la transmisión de grandes cantidades de información a través de grandes distancias , será necesario ampliar la comunicación de banda ancha tanto a nivel nacional como internacional. En particular , los países con un alto nivel de exportaciones deberán disponer de una rápida comunicación con el exterior.

Así mismo y de acuerdo con los informes y previsiones , los futuros sistemas de oficina mediante redes de comunicación serán más abiertos y flexibles. Sin embargo , como consecuencia de esta mayor apertura de los sistemas cambia de nuevo el alcance ó amplitud en la utilización en los diversos puestos de trabajo.

Por lo tanto , en la introducción de redes WAN y sobre todo de redes MAN deberán establecerse mediante estructuras de tareas claramente definidas los nuevos límites para los empleados , resultará imprescindible en el futuro una planificación organizativa a fondo , de la implantación de redes de alto rendimiento , con el fin de allanar el camino a los posibles cambios en el entorno tecnológico.

El puesto de oficina cambiará de manera decisiva como consecuencia del énfasis creciente en las conexiones de red y el consiguiente aumento de la transmisión de informaciones tanto en la industria como en las instituciones públicas. El cambio será positivo si se detectan y se resuelven oportunamente los problemas.

Con la llegada de las redes , se ha superado la época en que tenía lugar una adaptación a nivel general ante los cambios técnicos. El desarrollo tiende cada vez más , sobre todo en las empresas grandes , hacia conexiones en red a nivel de empresa u organización. Este desarrollo estará apoyado por una parte , por las organizaciones de estandarización y por otra , por los fabricantes haciendo posible la conexión prácticamente con todos los "mundos" ó entornos del proceso.

Al comienzo de ésta década los avances técnicos se están acelerando con múltiples desarrollos que brindan un nuevo panorama en el área de comunicaciones , entre los que cabe mencionar los producidos por la norma 10BaseT y la retransmisión de tramas (Frame Relay) , así como la mayor utilización de servicios conmutados de alta velocidad.

En la gráfica 3.7 se puede observar el vertiginoso crecimiento de las ventas hasta 1996 del mercado internacional internetwork.

Porcentaje de PCs en LAN's 1992 por mercado vertical

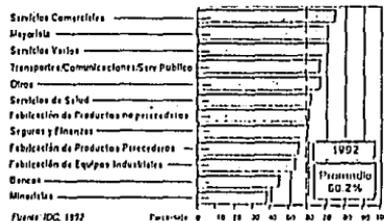


Fig.3-7."Porcentajes de PC's en las LAN's (año 1992) por mercado vertical".

Actualmente existen diferentes recursos de red los cuales se encuentran en diferentes sitios. Desde que las redes fueron instaladas (a mediados de 1980), éstas fueron diseñadas para grupos pequeños en promedio de 10 a 20 estaciones de trabajo por red.

Desde que comenzó la instalación de redes ha sido necesario, modificarlas, desarrollarlas, expandirlas, acceder a nuevos recursos (con diferentes plataformas de conectividad), etc. A finales de la década de los 80's las redes han crecido a una razón de 100 a 200 por ciento, pero actualmente las redes necesitan enlazarse a otras fuentes que probablemente se encuentran en lugares lejanos.

Estas otras fuentes pueden ser una LAN ó una computadora Host, una estación de trabajo remota ó una persona que se encuentra en un lugar distante donde tiene su propia red de acceso. La conectividad puede ser conectando diferentes marcas como son Macintosh con Unix, por ejemplo. Todos estos usuarios pueden utilizar las facilidades de la WAN.

Los tópicos de interconexión LAN to WAN son numerosos y es importante determinar el tipo de transmisión que se requieren para cada conexión.

3.3.1 Diseño de la conexión LAN to WAN.

Actualmente existen Sub-networks en diferentes lugares, de lo cual surge el objetivo de diseñar una conexión LAN to WAN de ésta internetwork. Este diseño se puede dividir en diferentes pasos los cuales son:

- Definir el objetivo : determinar las metas a alcanzar, tanto de una forma general como objetiva, y conocer la tarea de cada parte asociada en la internet. Es importante tomar en cuenta costos, mantenimiento, soporte, funcionamiento y robustez del sistema, etc. Siendo lo anterior importante para la integración LAN to WAN para conocer el comportamiento del sistema en caso de un periodo de trabajo con mucha actividad.

- Identificación de componentes : en ésta parte se identificarán los componentes de hardware/software que existen en cada red, ya que son los integradores de la internetwork.

Se tomarán en cuenta los siguientes puntos : primeramente , el hardware de la LAN para que exista la posibilidad a futuro de cambiarla a otro tipo de arquitectura (por ejemplo , Ethernet a Token Ring) ; segundo , es importante conocer el sistema operativo que maneja la LAN , para que de ésta forma se pueda conectar a diferentes sistemas.

- Aplicación : en ésta parte se tomará en cuenta el nivel de aplicación del modelo de referencia OSI , para así conocer el funcionamiento de los mensajes electrónicos usados por la CCITT (estándar X400) o transferencia de archivos usando el Sun Microsystems NFS (Network File System) , ahora si existe un denominador común en el nivel de aplicación , el diseño del trabajo es más fácil.

- Desarrollo del proyecto : considerando una proyección del desarrollo de la Internet , se toman en cuenta tres áreas de desarrollo :

- Localización individual.
- Número de localizaciones.
- Posibles opciones ó adquisiciones que pueden ocurrir durante el periodo proyectado.

- Análisis del tráfico : en éste punto se considera el tráfico existente en la red de comunicaciones.

Este estudio puede comenzar por mediciones del tráfico en la red sobre cada segmento y hacer un cálculo posterior. De la figura 3-8a a la 3-8e se presentan las hojas de trabajo ; las cuales fueron primeramente diseñadas para redes Ethernet , los principios incluidos en éstas pueden ser utilizados para otros diseños de red. Este análisis es dividido en cinco hojas de trabajo diferentes :

Hoja de Trabajo # 1 ("Recurso del Host").

Es diseñada para obtener un claro entendimiento de los recursos que están disponibles en el lugar remoto. Los parámetros examinados son :

- Tipo de Host (como está manufacturado).
- Protocolos : los protocolos que se encuentran implementados en el Host.
- Corriendo aplicaciones : Categorizar , interactuar , compilar programas , transferir archivos , procesar palabras , bases de datos , etc.

Hoja de Trabajo # 3 ("Tráfico").

En ésta hoja se debe proporcionar información acerca del tráfico para conocer el funcionamiento de la Ethernet la cual se encuentra localizada en un lugar remoto ; para analizar el tráfico de la LAN se pueden utilizar analizadores tanto para hardware como para software , para realizar el análisis deseado es recomendable que el sistema se encuentre en tráfico real , o bien cuando existan ciertas condiciones de tráfico. De ésta forma se tomarán mediciones representativas para el ambiente Ethernet , éstas mediciones serán utilizadas y analizadas en la hoja de trabajo número cuatro.

Traffic Worksheet #3

Site Name _____

Protocol _____

A. Number of Users _____
 B. # of Packets per Sample _____
 C. % of Total Ethernet Traffic _____

MULTICAST TRAFFIC

D. # of Multicast Packets per Sample _____
 E. % of Total Ethernet Traffic _____
 F. % of Protocol Traffic _____
 G. Average Packet Size _____

USER TRAFFIC

H. # of Data Packets per Sample _____
 I. % of Total Ethernet Traffic _____
 J. Average Large Ethernet Packet Size _____
 K. % of Large Packet Traffic _____
 L. Average Medium Packet Size _____
 M. % of Medium Packet Traffic _____
 N. Average Small Packet Traffic _____
 O. % of Small Packet Traffic _____

AVERAGE TRAFFIC PER USER PER PROTOCOL

B/A = Total Number of Packets / Number of Protocol Users
 G/F = Average Multicast Packet Size * % of Protocol Traffic
 J/K = Average Large Data Packet Size * % of Large Packet Traffic
 L/M = Average Medium Data Packet Size * % of Medium Packet Traffic
 N/O = Average Small Data Packet Size * % of Small Packet Traffic

P = Average Number of Bytes per User for this Protocol
 P = [(B/A)((G/F) + (J/K) + (L/M) + (N/O))]

Average Number of Bytes per User for this Protocol _____

Fig.3-8c."Hoja de trabajo #3".

Hoja de Trabajo # 5 ("Desarrollo de la red").

Finalmente considerando la información de las hojas de trabajo anteriores, se permite el diseño de la internetworking. El análisis se basa en el ancho de banda pico por usuario, y el cálculo futuro se hace tomando en cuenta los requerimientos futuros.

El diseñador debe utilizar éstos resultados para determinar la velocidad de transmisión y el enlace entre los dos lugares distantes. El desarrollo de los cálculos es importante para evitar problemas en la transmisión. Sin embargo, se estima que el 80 por ciento del tráfico de la red se encuentra en el segmento local, mientras que el otro 20 por ciento se tiene en el resto de los segmentos.

Con los datos obtenidos del análisis anterior se conocerá la velocidad y el tipo de transmisión necesaria.

Network Growth Worksheet #5

Link Name _____
 Site Name _____ to Site Name _____

A = Peak Bandwidth Utilization of Link _____
 B = # of Current Users _____
 C = Peak Bandwidth per User _____

C = A/B _____

D = Additional Future Users _____
 E = Future Bandwidth Requirements _____

E = C*(B+D) _____

Future Bandwidth Requirements = _____

Fig.3-8e."Hoja de trabajo #5".

- Plan de desarrollo : la internetwork diseñada será una red cuya finalidad sea satisfacer las necesidades actuales y a futuro de los usuarios , siendo compatible con cualquier producto de internetworking (ruteadores , bridges , repetidores , etc.) que cumpla con las necesidades requeridas por la red de comunicaciones.

C A P I T U L O C U A T R O
"BASES DE LA INTERNETWORKING"

- 4.1 BASES DEL RUTEO.
- 4.1.1 ANTECEDENTES.
- 4.1.2 COMPONENTES DEL RUTEO.
- 4.1.3 CONMUTACION.
- 4.1.4 ALGORITMOS DE RUTEO.
- 4.1.4.1 METAS DE DISEÑO.
- 4.1.4.1.a OPTIMIZACION.
- 4.1.4.1.b SIMPLICIDAD.
- 4.1.4.1.c CAPACIDAD.
- 4.1.4.1.d CONVERGENCIA RAPIDA.
- 4.1.4.1.e FLEXIBILIDAD.
- 4.1.5 TIPOS DE ALGORITMOS DE RUTEO.
- 4.1.5.a ESTATICOS O DINAMICOS.
- 4.1.5.b DE UNO O VARIOS CAMINOS.
- 4.1.5.c COMUN O JERARQUICO.
- 4.1.5.d DE HOST INTELIGENTE O RUTEADOR INTELIGENTE.
- 4.1.5.e INTRADOMAIN O INTERDOMAIN.
- 4.1.5.f ESTADO DE ENLACE O VECTOR DE DISTANCIA.
- 4.1.6 PARAMETROS.
- 4.1.6.a LONGITUD DEL CAMINO.
- 4.1.6.b CONFIABILIDAD.
- 4.1.6.c RETRASO.
- 4.1.6.d ANCHO DE BANDA.
- 4.1.6.e CARGA.
- 4.1.7 PROTOCOLOS RUTEADOS VS. PROTOCOLOS DE RUTEO.
- 4.1.8 PROTOCOLOS INTERNET.
- 4.1.8.1 DIRECCIONAMIENTO IP.
- 4.1.8.2 RUTEO INTERNET.
- 4.1.8.3 PROTOCOLO IGRP.
- 4.2 BASES DEL PUENTE.
- 4.2.1 BASES TECNOLOGICAS.
- 4.2.2 TIPOS DE BRIDGES.

C A P I T U L O C U A T R O
B A S E S D E L A I N T E R N E T W O R K I N G

4.1 Bases del ruteo.

4.1.1 Antecedentes.

El ruteo ha sido investigado por dos décadas , pero fué primero necesario el desarrollo de las redes , por lo que últimamente la inclusión de los ruteadores ha traído como consecuencia la conexión de las redes de comunicación que es lo que se conoce como internetworking. Ruteo en una definición general es transportar la información a través de la internetwork desde un nodo origen a un nodo destino. El ruteo es frecuentemente confundido con el puenteo ya que aparentemente realizan la misma función. La diferencia primaria entre estos dos es que el puenteo trabaja en el nivel dos (nivel de enlace de datos) del modelo de referencia OSI , mientras que el ruteo ocurre en el nivel tres (nivel de red) ; debido a ésta distinción , el ruteo y el puenteo procesan de manera diferente la información.

4.1.2 Componentes del ruteo.

Uno de los principales elementos que es considerado dentro del concepto del ruteo es la elección de la mejor ruta ó el mejor camino. La determinación de los caminos es realizada por una variedad de mediciones (resultados de algoritmos , cálculos sobre una determinada variable como puede ser la longitud del camino ó combinaciones métricas) ; la implementación de algoritmos de ruteo conlleva a elegir la ruta óptima.

Al trabajar con los algoritmos de ruteo , es necesario conocer las tablas de ruteo , las cuales contienen la información de ruteo requerida , la cual varía dependiendo del algoritmo utilizado.

Los algoritmos de ruteo llenan las tablas de ruteo con una variedad de información. Cuando un ruteador recibe un paquete entrante , éste verifica la dirección destino del paquete y además asocia ésta dirección con el nodo siguiente. Como se observa en la figura 4-1.

To reach network:	Send to:
27	Node A
57	Node B
17	Node C
24	Node A
52	Node A
16	Node U
26	Node A

Fig.4-1. "Tabla de ruteo Destino/Siguiente Nodo".

Las tablas de ruteo pueden contener más información proporcionada por los parámetros para determinar la mejor ruta. Los ruteadores emplean los parámetros para elegir el camino óptimo. Los parámetros difieren dependiendo del diseño del algoritmo empleado.

Cuando un ruteador se comunica con otro (manteniendo sus tablas de ruteo) utiliza una gran variedad de mensajes, tal como los mensajes de ruteo actualizados. El mensaje de ruteo actualizado consiste de toda ó una porción de la tabla de ruteo. Por el análisis de éstos mensajes de ruteo actualizados que provienen de todos los ruteadores, un ruteador (cualquiera de todos) puede hacer una réplica detallada de la topología actual de la red. El estado del enlace es otro ejemplo de mensajes, el cual informa a todos los ruteadores de las condiciones de los enlaces existentes. Una vez establecida la topología de la red, los ruteadores pueden determinar la ruta más conveniente, según las condiciones que se presenten como por ejemplo de tráfico, de fallas en la red ó de algún equipo, etc.

4.1.3 Conmutación.

Los algoritmos de conmutación son relativamente simples y básicamente son el mismo para la mayoría de los protocolos ; en la mayoría de los casos , un host determina cuando enviar un paquete hacia otro host. Cuando se conoce la dirección de los ruteadores (por algún medio) , el host origen envía un paquete específicamente direccionado a las direcciones físicas del ruteador (nivel MAC) , pero con la dirección del protocolo (a nivel de red) del host destino. Cuando el ruteador recibe un paquete , primero examina su dirección para saber si lo puede enviar o no , en caso de no poderlo enviar , el ruteador lo "olvida" ; en caso de reconocer la dirección , el ruteador lo envía al siguiente nodo para que siga el camino hacia el destino final. El siguiente nodo puede o no ser el último durante la trayectoria hacia el host destino , si no es así , el siguiente nodo es usualmente un ruteador el cual ejecuta el mismo proceso de conmutación realizado por los ruteadores anteriores ; como el paquete viaja a través de la internetwork , su dirección física cambia conforme a la trayectoria , pero no así su dirección de protocolo como se ilustra en la fig. 4-2.

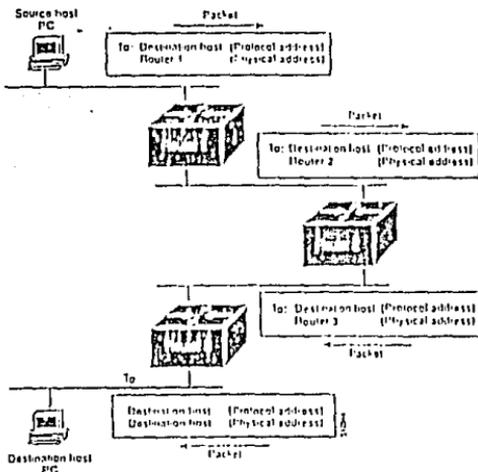


Fig.4-2."Proceso de conmutación".

La explicación mostrada en la figura anterior, describe el proceso de conmutación entre el origen y el destino de un sistema. La ISO ha desarrollado una terminología jerárquica que es útil para describir éste proceso; los dispositivos de red sin la habilidad para enviar paquetes entre subnetworks son llamados "end systems" (ES's), mientras los dispositivos de red con ésta capacidad son conocidos como "intermediate systems" (IS's), éstos se dividen en dos clases, los que se pueden comunicar dentro del dominio de ruteo (intradomain IS's) y los que se comunican tanto dentro como entre uno o mas dominios de ruteo (interdomain IS's).

Un dominio de ruteo es por lo general una parte de una internetwork bajo una autoridad administrativa común, regida por una regla particular de líneas administrativas. Los dominios de ruteo son también conocidos como "sistemas autónomos" (Autonomous Systems AS's) que manejan determinado protocolo. Los dominios de ruteo se pueden dividir dentro de áreas de ruta, pero los protocolos de ruteo "intradomain" son todavía empleados para la conmutación tanto dentro y entre áreas.

4.1.4 Algoritmos de ruteo.

Los algoritmos de ruteo se diferencian porque cada uno tiene sus características propias. Primero, los objetivos particulares de cada diseñador de algoritmos tienen que ver con la operación del protocolo empleado. Segundo, existen varios tipos de algoritmos de ruteo y cada algoritmo tiene un impacto diferente en los recursos tanto de la red como del ruteador. Finalmente, los algoritmos de ruteo emplean una variedad de parámetros que tienen que ver con el cálculo de las rutas óptimas.

4.1.4.1 Metas de diseño.

Los algoritmos de ruteo tienen a menudo una o mas de las siguientes metas de diseño:

- Optimización
- Simplicidad
- Capacidad
- Convergencia rápida
- Flexibilidad

4.1.4.1.a Optimización.

Es la meta más común del diseño. Esta se refiere a la habilidad que tiene el algoritmo de ruteo para seleccionar la mejor ruta. La mejor ruta depende de los parámetros más importantes empleados para hacer los cálculos. Por ejemplo, un algoritmo de ruteo debe considerar un cierto tiempo de envío de paquetes a los nodos y cierto tiempo perdido (retrasos), manejando de una forma cuidadosa los retrasos en el cálculo. Naturalmente, los protocolos de ruteo deben definir estrictamente sus parámetros para el cálculo de los algoritmos.

4.1.4.1.b Simplicidad.

Los algoritmos de ruteo deben ser diseñados para ser lo más simples posible. En otras palabras, el algoritmo de ruteo debe ofrecer una funcionalidad muy eficaz, manejando un mínimo de software con una utilización muy grande. La eficacia es particularmente importante cuando la implementación de software de un algoritmo debe correr en una computadora con recursos físicos limitados.

4.1.4.1.c Capacidad.

El algoritmo debe ser capaz. En otras palabras debe trabajar correctamente en casos anormales o bien en circunstancias imprevistas tales como fallas en el hardware, condiciones de carga pesada, implementaciones incorrectas, etc. Debido a que los ruteadores están localizados en el punto de unión de las redes, pueden causar problemas considerables cuando llegan a fallar. Los mejores algoritmos de ruteo son los que se han mantenido cierto tiempo trabajando y han demostrado estabilidad bajo una variedad de condiciones de la red.

4.1.4.1.d Convergencia rápida.

Los algoritmos de ruteo deben converger rápidamente. La convergencia es el proceso en el que todos los ruteadores que conforman la red están de acuerdo en todas las rutas óptimas existentes actuales. Cuando un evento en la red provoca que la ruta se venga abajo ó que se habilite una nueva ruta, los

ruteadores distribuyen mensajes de ruteo actualizados. Estos mensajes permiten que la red indique a los ruteadores que hagan un nuevo cálculo de las rutas óptimas y eventualmente hacer saber a los ruteadores que estén de acuerdo con éstas nuevas rutas. Por otro lado, los algoritmos de ruteo que convergen muy lentamente, pueden causar loops en el ruteo ó caída de la red. La fig. 4-3 describe un loop de ruteo. En éste caso el paquete arriba al ruteador en el tiempo t_1 . El

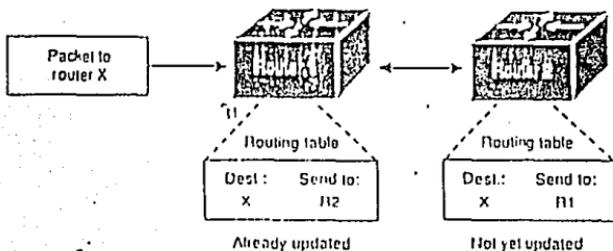


Fig.4-3."Ejemplo de una convergencia lenta que provoca un loop de ruteo".

ruteador 1 está ya actualizado así que sabe que la ruta óptima hacia el destino es pasar por el ruteador 2 que es el siguiente en el camino. Por lo tanto, el ruteador 1 envía el paquete al ruteador 2. El ruteador 2 no está actualizado todavía así que cree que la ruta óptima es hacia el ruteador 1. Por lo tanto, el ruteador 2 envía el paquete al ruteador 1. Por lo que el paquete continuará en un ir y venir entre los dos ruteadores hasta que el ruteador 2 es actualizado ó hasta que el paquete ha sido conmutado mas de el máximo del tiempo permitido.

4.1.4.1.e Flexibilidad.

Los algoritmos de ruteo deben también ser flexibles , es decir , deben adaptarse rápida y exactamente a una variedad de circunstancias de la red. Por ejemplo , se asume que un segmento en la red se ha caído. Muchos algoritmos de ruteo , empiezan por notificar de éste problema así que rápidamente seleccionarán el mejor camino siguiente para todas las rutas que normalmente estaban usando éste segmento. Los algoritmos de ruteo pueden ser programados para adaptarse a cambios en la red como por ejemplo , cambio de ancho de banda , tiempo de espera del ruteador , retrasos en la red y otras variables.

4.1.5 Tipos de algoritmos de ruteo.

Los algoritmos de ruteo se pueden clasificar por tipos. Por ejemplo :

- Estáticos ó Dinámicos
- De uno ó varios caminos
- Común ó Jerárquico
- De host inteligente ó ruteador inteligente
- Intradomain ó Interdomain
- Estado de enlace ó Vector de distancia

4.1.5.a Estáticos ó Dinámicos.

Los algoritmos de ruteo estáticos son difíciles en todos los sentidos. Los mapas de las tablas de ruteo estáticas son establecidas por el administrador de la red , así que éstos mapas no podrán cambiar a menos que el administrador cambie también. Los algoritmos que usan rutas estáticas son simples en el diseño y trabajan muy bien en ambientes donde el tráfico es relativamente predecible y el diseño de la red es simple.

Debido a que los sistemas estáticos de ruteo no pueden reaccionar a los cambios de la red , son por lo general inconvenientes en las redes de hoy en día por los constantes cambios que se presentan en la red. La mayoría de los algoritmos de ruteo en los 90's son dinámicos.

Los algoritmos de ruteo dinámico se ajustan , en el tiempo real , a las circunstancias de cambio en la red. Ellos realizan ésto por el análisis de ruteo actualizado. Si el mensaje indica que un cambio en la red ha ocurrido , el software de ruteo vuelve a calcular las rutas y envía posteriormente nuevos mensajes de ruteo actualizados , los que permiten a la red indicarle a los ruteadores que reactiven sus algoritmos y cambien las tablas de ruteo en un acuerdo común. Los algoritmos de ruteo dinámico pueden ser contemplados con rutas estáticas en donde se requiera. Por ejemplo , un ruteador "de último recurso" (es un ruteador el cual procesa de alguna manera los paquetes no ruteables). Este ruteador actúa como un procesador para todos los paquetes no ruteables , y asegura que todos los mensajes sean manejados de alguna manera.

4.1.5.b De uno ó varios caminos.

Algunos protocolos de ruteo sofisticados soportan múltiples caminos hacia una misma dirección. Estos algoritmos multicamino permiten multiplexar el tráfico sobre muchas líneas ; mientras que los algoritmos de un sólo camino no lo hacen. Una de las ventajas de los algoritmos multicamino es que proporcionan un mejor throughput y una muy buena confiabilidad.

4.1.5.c Común ó Jerárquico.

Algunos algoritmos de ruteo operan en un espacio común , mientras otros son empleados en sistemas de ruteo jerárquicos. En un sistema de ruteo común , todos los ruteadores cuentan con su pareja respectiva en el nodo destino (punto a punto). En un sistema de ruteo jerárquico , se tienen ruteadores que conforman el backbone del sistema , conociéndose entonces como los ruteadores del backbone. Los paquetes que provienen de los ruteadores "extremos" viajan a través de los ruteadores del backbone , así que ellos son enviados a través del backbone hasta que alcanzan las áreas de destino. En éste punto , ellos viajan a través desde el último ruteador del backbone pasando por uno o más ruteadores "extremos" hasta que llegan a su destino final.

Los sistemas de ruteo a menudo designan grupos lógicos de nodos conocidos como dominios ó áreas. En sistemas jerárquicos , los ruteadores pertenecientes a un dominio se pueden comunicar con ruteadores que pertenecen a otro

dominio , mientras otros sólo pueden comunicarse con ruteadores del mismo dominio. En redes muy grandes , se puede hablar de niveles jerárquicos. Los ruteadores en el nivel jerárquico mas alto forman el backbone de ruteo.

La ventaja principal del ruteo jerárquico , es que imita la organización de la mayoría de las compañías y por esto soporta sus patrones de tráfico perfectamente. La mayoría de la comunicación entre redes ocurre dentro de pequeños grupos en la compañía (dominios). Los ruteadores "intradomain" sólo necesitan conocer acerca de otros ruteadores dentro de su dominio , así que sus algoritmos de ruteo pueden ser simples. Dependiendo del algoritmo de ruteo que se está empleando , el tráfico de ruteo actualizado puede ser reducido en un acuerdo común.

4.1.5.d De host inteligente ó ruteador inteligente.

Algunos algoritmos de ruteo asumen que el nodo final de la fuente determinará la ruta a seguir. Esto es usualmente conocido como "ruteo desde la fuente". En sistemas de ruteo desde la fuente , los ruteadores simplemente actúan como dispositivos de almacenar y enviar , con el objetivo de enviar el paquete al siguiente ruteador del sistema. Otros algoritmos asumen que los hosts no conocen nada acerca de las rutas. En éstos algoritmos , los ruteadores determinan el camino a través de la internetwork basado en cálculos hechos. En el primer sistema , los hosts tienen la inteligencia para hacer el ruteo. En el último sistema , los ruteadores tienen la inteligencia para hacer el ruteo.

El tener ruteo por medio de host inteligente ó ruteador inteligente es una opción de dos : un camino de optimización contra la sobrecarga del tráfico de datos. Los sistemas de host inteligente por lo general eligen la mejor ruta , porque típicamente descubren todas las rutas posibles al destino antes de que el paquete se envíe , por lo que eligen el mejor camino basado en las definiciones de optimización del sistema en particular. El hecho de determinar todas las rutas , a menudo requiere un conocimiento constante del comportamiento del tráfico.

4.1.5.e Intradomain ó Interdomain.

Algunos algoritmos de ruteo trabajan sólo dentro del dominio , mientras que otros trabajan dentro y entre dominios. La naturaleza de éstos dos tipos de algoritmo es diferente.

4.1.5.f Estado de Enlace ó Vector de Distancia.

Los algoritmos de "estado de enlace" (también conocidos como algoritmos que escogen el primer camino más rápido) , envían la información de ruteo a todos los nodos en la internetwork. Sin embargo , cada ruteador envía sólo la porción de la tabla de ruteo que describe el estado de sus propios enlaces. Los algoritmos "vector de distancia" (también conocidos como algoritmos Bellman-Ford) llaman a cada ruteador vecino para enviarle toda o alguna parte de su tabla de ruteo. En pocas palabras , los algoritmos de estado de enlace envían mensajes actualizados cada vez que es posible , mientras que los algoritmos vector de distancia envían también mensajes actualizados constantemente a sus ruteadores vecinos. Debido a que convergen más rápido , los algoritmos de estado de enlace están menos expuestos a los loops de ruteo , que los algoritmos vector de distancia. De otra forma los algoritmos estado de enlace son más especiales que los algoritmos vector de distancia , ya que requieren un CPU más poderoso y una gran capacidad de memoria.

4.1.6 Parámetros.

Las tablas de ruteo contienen información usada por el software de conmutación para seleccionar la mejor ruta. Pero , ¿Cómo se construyen las tablas de ruteo? , ¿Cuál es la naturaleza específica de la información que ellos contienen?

Muchos parámetros han sido empleados en diferentes algoritmos. Algoritmos de ruteo sofisticados seleccionan la mejor ruta en base a múltiples parámetros , combinándolos de manera que se obtenga sólo un parámetro (híbrido). Por lo general se emplean los siguientes parámetros :

- Longitud del camino
- Confiabilidad
- Retraso
- Ancho de Banda
- Carga

4.1.6.a Longitud del camino.

Este es el parámetro de ruteo más común. Algunos protocolos de ruteo permiten a los administradores de red asignar costos arbitrarios a cada enlace de la red. En este caso, la longitud del camino es la suma de los costos asociados con cada enlace considerado. Otros protocolos de ruteo definen un parámetro conocido como hop count, el cual especifica el número de saltos a través de los productos de internetworking (por ejemplo, los ruteadores) por los que pasan los paquetes desde el origen al destino.

4.1.6.b Confiabilidad.

La confiabilidad, en el contexto de los algoritmos de ruteo, se refiere a la confiabilidad (usualmente descrita en términos de "promedio de error en los bits") de cada enlace de la red. Algunos enlaces de la red se pueden caer más a menudo que otros. Una vez caídos, algunos de ellos se pueden reparar más rápidamente o más fácilmente que otros. Cualquier factor de confiabilidad puede ser evaluado dentro de una cuenta en la asignación de rangos de confiabilidad. Las evaluaciones de confiabilidad son usualmente asignadas a los enlaces de la red por los administradores de la red. Por lo general estas evaluaciones son valores numéricos arbitrarios.

4.1.6.c Retraso.

El retraso en el ruteo se refiere al tiempo extra que se ha requerido para mover un paquete desde el origen hacia el destino a través de la internetwork. El retraso depende de muchos factores incluyendo, el ancho de banda de los enlaces intermedios, el tiempo en que el puerto espera la respuesta de cada ruteador a lo largo del camino, la congestión en la red en todos los enlaces intermedios y la distancia típica por la que los paquetes viajarán.

Debido a que se tiene una conglomeración de las distintas variables importantes, es necesario considerar el retraso como un parámetro útil.

4.1.6.d Ancho de Banda.

Este se refiere a la capacidad de tráfico disponible en el enlace. Por lo general un enlace en Ethernet de 10 Mbps es más común que uno de 64 Kbps. Aunque el ancho de banda es una evaluación del máximo throughput alcanzable en un enlace, las rutas a través de los enlaces con un ancho de banda enorme no necesariamente proporcionan las mejores rutas que las que cuentan con una velocidad muy baja. Por ejemplo, si un enlace a una velocidad grande esta demasiado ocupado el tiempo requerido para enviar un paquete hacia el destino puede ser mayor que a través de un enlace no muy rápido.

4.1.6.e Carga.

La carga se refiere al grado en el cual el recurso de la red (el ruteador) está ocupado. La carga se puede calcular de muchas formas, incluyendo la utilización del CPU y paquetes procesados por segundo.

4.1.7 Protocolos Ruteados Vs. Protocolos de Ruteo.

Los protocolos ruteados son aquellos que son ruteados sobre una internetwork. Ejemplos de tales protocolos son el IP, Decnet, Apple Talk, etc. Los protocolos de ruteo son aquellos que implementan algoritmos de ruteo. Estos simplemente enrutan los protocolos ruteados a través de una internetwork. Ejemplos de estos protocolos son el: Interior Gateway Routing Protocol (IGRP), el Open Shortest Path First (OSPF), el Routing Information Protocol (RIP), etc.

4.1.8 Protocolos Internet.

A mediados de 1970 , la Agencia de Proyectos de Investigación Avanzados de la Defensa (DARPA) , se interesó en la necesidad de desarrollar una red de conmutación de paquetes para poder realizar la comunicación entre varios centros de investigación en los Estados Unidos. DARPA y otras entidades gubernamentales entendieron el potencial de ésta tecnología de conmutación de paquetes , y precisamente fueron ellos los que enfrentaron por primera vez el problema que tienen todas las compañías que desean enlazar sus redes : tener la comunicación con cualquier tipo de sistema.

Con la meta de lograr la conectividad heterogénea , se tuvo como resultado la creación de una serie de protocolos de comunicación , los cuales son los protocolos Internet y entre los más conocidos y los más empleados se encuentran el TCP (Transmission Control Protocol) y el IP (Internet Protocol) , cabe señalar que comúnmente éstos dos protocolos son más conocidos como TCP/IP debido a que trabajan en conjunto , TCP a nivel de transporte e IP a nivel de red.

Los protocolos Internet pueden ser empleados para comunicar cualquier conjunto de redes conectadas. Por lo tanto , son convenientes tanto para redes LAN como para redes WAN. En la fig. 4-4 , se muestra la relación entre el modelo de referencia OSI y los protocolos Internet.

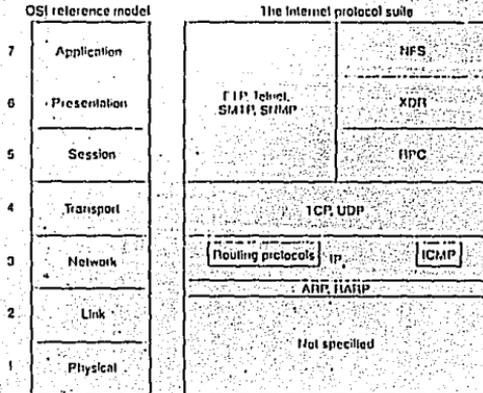


Fig.4-4. "Relación entre el modelo de referencia OSI y los protocolos Internet".

4.1.8.1 Direccionamiento IP.

Así como en todos los protocolos en el nivel de red , el esquema de direccionamiento en IP es de gran importancia para el proceso de enrutamiento a través de una red. Una dirección IP tiene un campo cuya longitud es de 32 bits , divididos ya sea en dos ó tres partes (octetos). La primera parte comprende la dirección de la red , la segunda parte (si es que existe) designa la dirección de la subnet y la tercera parte indica la dirección del host. La dirección de la subnet existe , siempre que el administrador de la red haya decidido dividir la red en partes. Las longitudes de los campos de la red , la subnet y del host son siempre variables.

El direccionamiento en IP soporta cinco clases de redes. El bit más a la izquierda indica la clase de red. Las direcciones IP son escritas en formato decimal y separadas por puntos decimales , por ejemplo , 34.0.0.1 . Las clases se indican a continuación :

- Red Clase A. Asignan 7 bits para el campo de dirección de la red y 24 para la dirección del host. Para identificar a éste tipo de redes , el valor decimal puede ser cualquiera entre 1 y 127 en el primer octeto.
- Red Clase B. Asignan 14 bits para la dirección de red y 16 para la dirección del host. El valor decimal en el primer octeto puede ser cualquiera entre 128 y 191.
- Red Clase C. Asignan 22 bits para la dirección de la red y 8 para la dirección de host. El valor decimal en el primer octeto puede ser cualquiera entre 192 y 223.
- Red Clase D. Estas direcciones son reservadas para grupos multicast.
- Red Clase E. Estas direcciones son reservadas para uso futuro.

En la figura 4-5 se muestra el formato de direcciones para las redes Clase A , B y C.

Si el administrador de la red ha elegido asignar 8 bits , el tercer octeto de la dirección IP de la Clase B proporciona el número de la subnet. En el ejemplo , suponiendo que el campo se modificó de la siguiente manera 182.10.1.0 , esto nos indica red 182.10 , subnet 1 y host 0.

4.1.8.2 Ruteo Internet.

Los ruteadores dentro de Internet , están organizados jerárquicamente. Algunos de ellos son empleados para llevar información a través de un grupo particular de redes que están regidas bajo una misma autoridad administrativa , a este grupo particular se le conoce como Sistema Autónomo. Los ruteadores empleados para llevar éste intercambio de información dentro de los sistemas autónomos son más conocidos como ruteadores internos (interior routers), los cuales emplean una variedad de protocolos de comunicación internos (interior gateways protocol [IGP]) para poder realizar su propósito. Los ruteadores que mueven información entre los sistemas autónomos son llamados ruteadores externos (exterior routers), los cuales emplean un protocolo externo de comunicaciones (exterior gateway protocol). La fig. 4-7 muestra la arquitectura Internet.

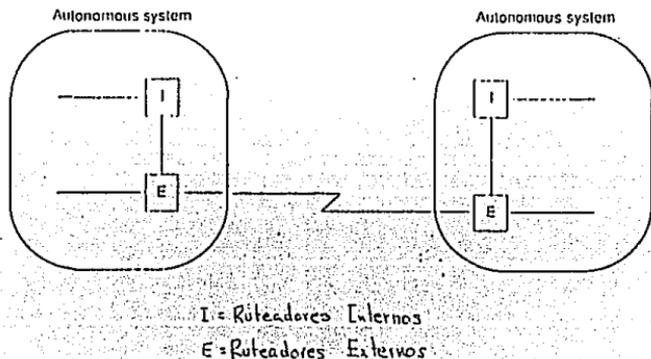


Fig.4-7."Arquitectura Internet".

Los protocolos de ruteo IP son dinámicos. Una tabla de ruteo en IP consiste de una asociación par como se muestra en la fig. 4-8. En ésta figura se muestra un ejemplo que es interpretado de la manera siguiente : para alcanzar la red 34.1.0.0 (subnet 1 en red 34) será por medio del nodo con dirección 54.34.23.12

Destination address	Next hop
34.1.0.0	54.34.23.12
78.2.0.0	54.34.23.12
147.9.5.0	
17.12.0.0	
.	54.32.12.10
.	54.32.12.10

Fig.4-8."Tabla de ruteo IP".

El ruteo en IP especifica los paquetes que viajarán a través de la red por determinado nodo en un cierto tiempo. La ruta de la red completa no es conocida en el momento de comenzar la transmisión, si no que al llegar al siguiente nodo, éste analiza la dirección destino del paquete y busca en la tabla de ruteo la ruta óptima por donde enviarlo. La participación de cada nodo en el proceso de ruteo consiste sólo de enviar los paquetes al siguiente nodo por donde exista la mejor ruta, sin importar que los paquetes contengan errores o no. En otras palabras, IP no proporciona corrección de errores ni los reporta al emisor para que haga retransmisiones. Para hacer ésta y otras tareas existen otros protocolos. El protocolo de ruteo en IP, es activado (en los ruteadores Cisco) en el protocolo IGRP (Interior Gateway Routing Protocol).

El nivel de transporte en Internet es implementado por los protocolos TCP y UDP. (Se considera el TCP por ser más importante que el UDP). TCP proporciona servicios full-dúplex, reconocimiento y control de flujo para los protocolos manejados en los niveles superiores, el transporte de datos es a conexión orientada. Este maneja los datos en una forma continua y con un flujo de bytes sin estructura, sólo identificados por una secuencia de números. El formato del paquete en TCP se muestra en la fig. 4-9.

Source port		Destination port	
Sequence number			
Acknowledgment number			
Data offset	Reserved	Flags	Window
Checksum		Urgent pointer	
Options (+ padding)			
Data (variable)			

Fig.4-9."Formato del paquete TCP".

4.1.8.3 Protocolo IGRP.

El protocolo de ruteo IGRP , fué desarrollado por Cisco Systems , con el objetivo de manejar un protocolo poderoso y confiable dentro de sistemas autónomos que cuenten con una topología compleja y que manejan diversas características. Un sistema autónomo es una colección de redes controladas bajo una administración comun que comparten una misma estrategia de ruteo.

IGRP es un protocolo "vector de distancia". Este tipo de protocolo se comunica con cada ruteador para enviarle toda ó parte de la información contenida en su tabla de ruteo en forma de mensajes de ruteo actualizados. Como la información se va proliferando a través de toda la red , los ruteadores pueden calcular la distancia que hay entre ellos.

IGRP maneja una serie de parámetros que son importantes al momento de tomar las decisiones para hacer el ruteo y para seleccionar la ruta óptima. Dentro de estos parámetros se consideran por ejemplo la confiabilidad , el tráfico , el retraso , el ancho de banda , etc. Si todos los parámetros mencionados anteriormente se encuentran en un rango de valores que se consideran como adecuados , entonces se puede decir que la ruta es óptima.

Debido a la flexibilidad que ofrece este protocolo , existe la posibilidad de rutear por múltiples caminos. La opción de múltiples caminos depende totalmente de las mediciones (metrics). Por ejemplo , si los metrics nos indican que un camino tiene una buena velocidad de transmisión , poca carga , muy confiable y menor retraso , es lógico esperar que este camino sea utilizado más veces que otros.

4.2 Bases del Punteo.

Antecedentes :

El bridge comenzó a utilizarse a principios de los 80's para conectar y habilitar el envío de paquetes entre redes homogéneas , en la actualidad se ha podido puntear redes con arquitecturas diferentes.

El método Transparent Bridging comenzó a utilizarse en ambientes Ethernet ; el método Source-Route Bridging fué instalado en ambientes de Token Ring ; el método Traslational Bridging proporciona una traslación entre los formatos de los diferentes tipos de arquitecturas (como de Ethernet y Token Ring). El método Source-Route Transparent Bridging , combina los algoritmos Transparent Bridging y Source-Route Bridging haciendo una mezcla de ambientes Ethernet y Token Ring.

Los ruteadores han acaparado parte del mercado debido a que tienen también la capacidad de punteo. Los bridges contienen filtros , selección de caminos (pseudo-inteligentes) y soportan altas demandas de tráfico. En los últimos años ha habido un gran debate entre los ruteadores y los bridges , ahora en los esquemas de internetworking los dos son importantes.

4.2.1 Bases Tecnológicas.

El nivel dos del modelo OSI en el cual ocurre el punteo (conocido como nivel de enlace) tiene que ver con el flujo de datos , transmisión de errores permisible , direccionamiento físico y control de algoritmos de acceso al medio. El punteo proporciona éstas funciones para soportar varios protocolos en el nivel enlace ; por ejemplo el protocolo del nivel enlace de datos que es incluido en el Ethernet , Token Ring y FFDI.

Los bridges no son dispositivos complicados , ya que éstos analizan los frames entrantes , toman decisiones de envío basadas en información contenida dentro de los frames y los envían hacia el destino final. En algunos casos (por ejemplo el source-route bridging) , el camino entero hacia el destino

está contenido dentro de cada frame. En otro caso (por ejemplo , transparent bridging) los frames son enviados al siguiente nodo en un determinado tiempo.

Los protocolos de nivel superior son transparentes en este proceso , lo cual es una ventaja del puenteo , ya que los bridges operan únicamente en el nivel de enlace de datos , por lo que no necesitan examinar la información correspondiente a los niveles de red en adelante. Debido a éste manejo transparente , no es raro que en los bridges se manejen protocolos tales como Apple Talk , Decnet , TCP/IP , XNS , etc.

Los bridges son capaces de filtrar frames basados en un campo del nivel dos , por ejemplo , un bridge puede ser programado para rechazar (no enviar) todos los frames originados en una determinada red. Debido a que la información en el nivel de enlace de datos frecuentemente incluye una referencia de los protocolos de los niveles superiores , los bridges normalmente se basan en ésta referencia para realizar el filtrado.

Para dividir una gran red en varias unidades (segmentos) , los bridges proporcionan ventajas ; primeramente porque sólo algún porcentaje del tráfico es enviado , el puenteo disminuye el tráfico visto en todos los segmentos ; segundo , el bridge permite la comunicación entre un gran número de dispositivos que permitan soportar una LAN conectada al bridge ; tercero , el bridge permite una extensión efectiva de la LAN , permitiendo así conectarse a estaciones distantes remotas no consideradas anteriormente.

4.2.2 Tipos de Bridges.

Los bridges pueden ser agrupados en varias categorías con diferentes características cada uno. Usando una clasificación común esquemática , los bridges pueden ser locales ó remotos. Un bridge local proporciona una conexión directa con los múltiples segmentos de la LAN dentro de la misma área. Un bridge remoto conecta múltiples segmentos de LAN en diferentes áreas , normalmente en líneas de telecomunicaciones. Estas dos configuraciones se muestran en la figura 4-10.

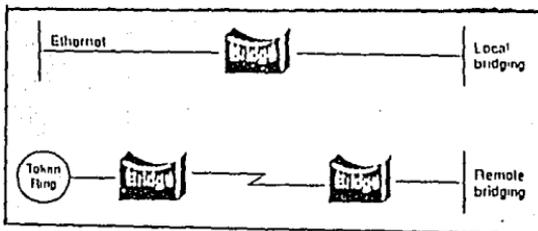


Fig.4-10."Puenteo local y remoto".

El puente remoto presenta una desventaja en el desarrollo de la internetworking. Esta es la diferencia de velocidades que manejan la LAN y la WAN. Día a día se están estableciendo WAN's de alta velocidad con respecto a las actuales y también LAN's de mucho más alta velocidad. Los bridges remotos no pueden conectarse a una WAN de alta velocidad, pero pueden compensar las discrepancias de velocidad a través de un buffer de capacidad suficiente; por ejemplo, si un dispositivo con capacidad de 3 Mbps desea una comunicación con un dispositivo de LAN remoto, el bridge local debe regular los 3 Mbps para no sobrepasar los 64 Kbps (por ejemplo) del enlace. Para poder realizar esto, una serie de buffers almacenan la entrada del flujo de datos y los envía a una velocidad que pueda acomodarse a la que maneja el enlace. Esto puede ser realizado sólo por el envío de ráfagas cortas de datos de manera que no saturan la capacidad del buffer del bridge.

El instituto de ingenieros eléctricos y electrónicos (IEEE), han dividido el nivel de enlace de datos en dos subniveles que son el control de acceso al medio (MAC) y el control de enlace lógico (LLC). El subnivel MAC permite y organiza el control de acceso al medio, mientras que el subnivel LLC se concentra en frames, control de flujo, control de error y direccionamiento del subnivel MAC.

Algunos bridges son para nivel MAC, los cuales trabajan en redes homogéneas (por ejemplo la IEEE 802.3), otros bridges pueden comunicarse entre diferentes protocolos del nivel de enlace de datos, por ejemplo, el IEEE 802.3 y el IEEE 802.5, la mecánica básica de la traslación es mostrada en la figura 4-11.

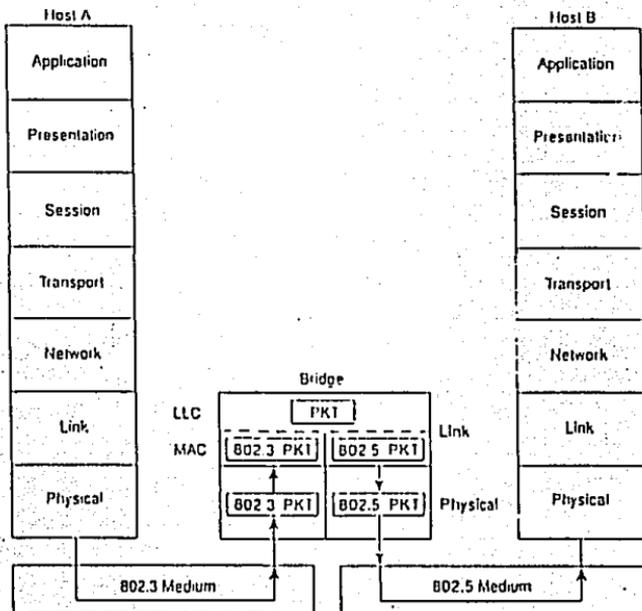


Fig. 4-11. "Puenteo IEEE 802.3/IEEE 802.5".

El IEEE 802.3 en el host A, formula un paquete que contiene aplicaciones de información y encapsula los paquetes en un frame para enviarse sobre un medio IEEE 802.3. En el bridge, al frame se le quita el encabezado de IEEE 802.3 en el subnivel MAC del enlace de datos y es enviado al nivel LLC para un proceso adicional. Después de este proceso el paquete es llevado al IEEE 802.5 el cual encapsula los

paquetes en un encabezado IEEE 802.5 para transmitir en un IEEE 802.5 hasta el host B.

C A P I T U L O C I N C O

"APLICACION DE LA TECNOLOGIA INTERNETWORKING EN UN AMBIENTE REAL"

- 5.1 INTRODUCCION.
- 5.2 ANALISIS DEL PRIMER SISTEMA.
- 5.3 ANALISIS DEL SISTEMA ACTUAL.
- 5.3.1 DESCRIPCION DE LA RED.
- 5.4 HARDWARE DEL RUTEADOR (CISCO).

C A P I T U L O C I N C O

APLICACION DE LA TECNOLOGIA INTERNETWORKING EN UN AMBIENTE REAL

5.1 Introducción.

En este capítulo se analizará , el papel que desempeñan los ruteadores en la integración de los sistemas de comunicación de datos y es aquí donde se emplean los conceptos de la Tecnología Internetworking para llevar a cabo la conexión de redes dispersas en diferentes áreas geográficas ; dicha conexión es realizada por los ruteadores , los cuales son dispositivos con gran versatilidad , alta eficiencia , confiabilidad , flexibilidad , etc.

Dentro de éste capítulo se tiene el objetivo de analizar un sistema antes y después de instalar los ruteadores . Comenzando por analizar la configuración de la red inicial y contemplando las siguientes características :

- La cantidad de servicios conectados a la red.
- ¿Qué dispositivos conformaban la red?.
- ¿Qué limitaciones tenían?.
- ¿Qué función desempeñaban los equipos?.
- La efectividad de los sistemas.

Posteriormente se analizará la red que actualmente existe , tomando en cuenta las siguientes características:

- ¿Porqué se consideraron los ruteadores?.
- ¿Qué ventajas presentan con respecto a los dispositivos anteriores?.
- La cantidad de servicios conectados a la red actual.

5.2 Análisis del primer sistema.

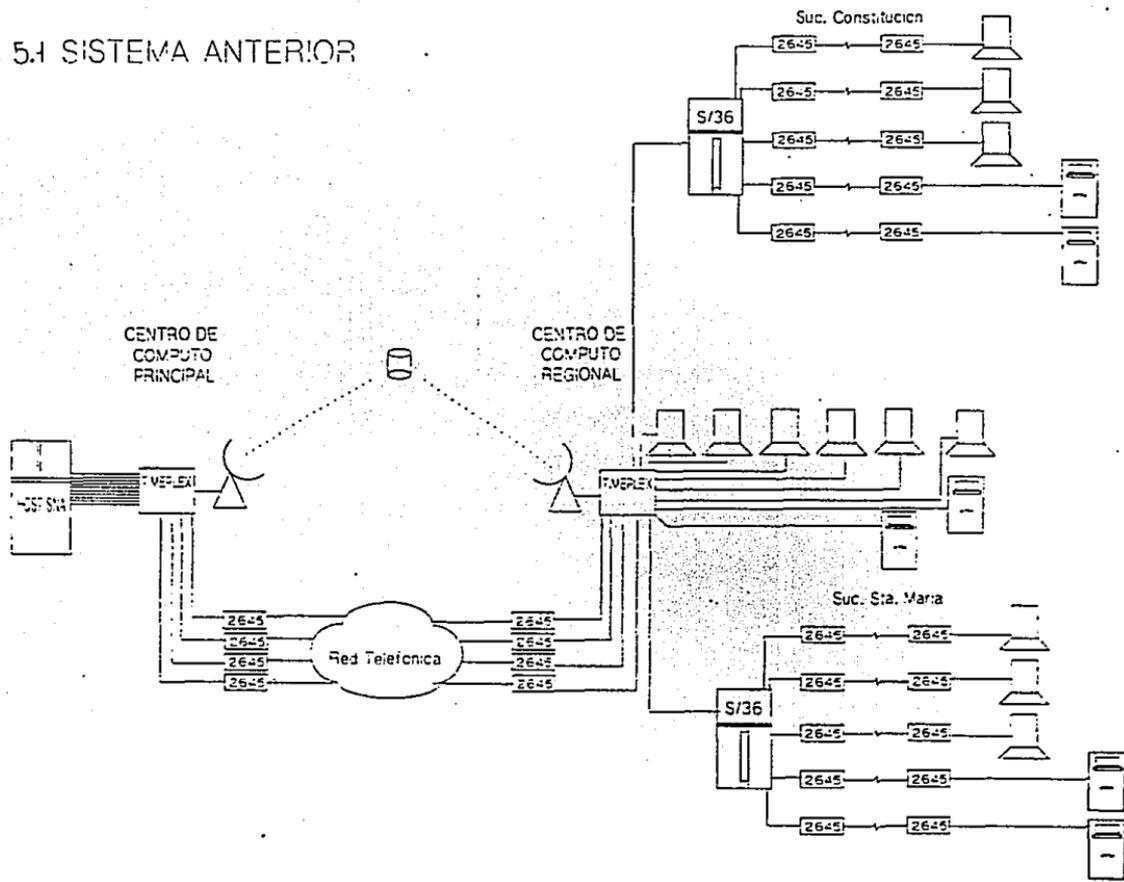
El sistema al que se hace referencia , pertenece a una institución bancaria ; para éste caso , el análisis hecho es en base a sólo dos nodos que forman parte de un sistema a nivel nacional.

El sistema fué creado para proporcionar múltiples servicios a los usuarios (tanto de sucursales locales como de sucursales regionales) de gran importancia para un banco , como pueden ser sistemas de captura de datos , altas y bajas , actualizaciones y consultas de saldos , atención a cajeros automáticos las 24 horas , revisión y canjes de cheques y todas las demás operaciones que se puedan realizar. Esta red de datos , comunica al Centro de Cómputo Principal (CCP) con el Centro de Cómputo Regional (CCR) , a su vez éste está comunicado con las sucursales regionales para tener la comunicación de datos (en formato síncrono) , de tal forma que se pueda atender a los usuarios y a su vez satisfacer todas las necesidades mencionadas anteriormente. En un inicio , el sistema estaba conformado como se muestra en el diagrama de la página 5 y los centros de cómputo estaban comunicados mediante dos enlaces :

- Enlace Satelital.
- Enlace de línea privada.

En ésta configuración (mostrada en la fig. 5.1) , los servicios de los usuarios regionales estaban dedicados punto a punto hacia el host de arquitectura SNA de IBM que se encuentra en el CCP ; en donde el protocolo de comunicaciones que se manejaba era el SDLC (Synchronous Data Link Control) que es empleado en ambientes SNA. La comunicación fué hecha por medio de un enlace satelital a través de los multiplexores Timeplex que empleaban la técnica TDM (Multiplexaje por División de Tiempo) ; desde la creación de ésta red , se pensó en emplear los multiplexores debido a que éstos equipos permiten que varios puertos compartan una misma línea de comunicaciones (como podría ser una línea telefónica , un enlace de línea privada , un enlace por microondas , vía satélite , etc.). La gran limitante que tenían éstos dispositivos era la técnica TDM , ya que al emplearla , a cada una de las estaciones de los usuarios regionales se les asignaba un cierto periodo de tiempo fijo en la línea de comunicaciones , del cual cada usuario tenía el control total , y por lo tanto ese tiempo no podía ser empleado por algún otro servicio en caso de estar desocupado. Otra de las desventajas que se tenían , era que cada puerto de datos estaba dedicado (tanto virtual como

FIG. 5.1 SISTEMA ANTERIOR



físicamente) a sólo un puerto del host , por lo que cuando el puerto estaba sin ocuparse , quedaba sin tráfico (sucedió esto debido a que el multiplexor no tenía la posibilidad de hacer la "conmutación" para sacar beneficio de las conexiones físicas y virtuales).

Con respecto al lado remoto (se considerará como lado remoto a todos aquellos lugares fuera del CCP) , en un inicio los dispositivos que básicamente controlaban la comunicación de las sucursales hacia el CCP eran los Sistemas 36 (S/36) de IBM los cuales eran minmainframes que contenían toda la información acerca de las transacciones básicas que se realizan en el banco y que son necesarias para atender a los usuarios ; otra característica de estos equipos era que hacían también las funciones de un controlador y coordinaban a los usuarios remotos para regular la forma en que los recursos de la red eran utilizados. En otras palabras , en un S/36 de IBM se centralizaba y se contenía parte de la información que estaba contenida en un host. Cabe hacer notar que a cada S/36 se le asignaba una conexión hacia el CCP (por medio de los mux) debido a que tenían la habilidad para distribuir el servicio a los demás usuarios de forma simultánea. Cuando el S/36 no contaba con la información debida para satisfacer la solicitud hecha por el usuario , se comunicaba con el host que se encontraba en el CCP para conseguir la información faltante. Una vez que las horas pico habían pasado y que toda la información se había recabado , renovado y procesado , el S/36 enviaba una copia de la información actualizada hacia el host principal.

Recordando que el CCP y el CCR estaban enlazados principalmente por medio de un enlace satelital , se tenía además un enlace de respaldo , el cual funcionaba de la siguiente manera : el multiplexor constantemente estaba analizando la calidad de la línea troncal , cuando detectaba cierto nivel de degradación , verificaba que si éste era igual o rebasaba cierto umbral establecido por el equipo , automáticamente conmutaba la información hacia los modems (referidos en la fig. 5.1 como los 2645) enlazados por medio de las líneas privadas analógicas. Una de las grandes desventajas que se tenían era que debido a que las líneas privadas trabajaban a una velocidad máxima de 2400 bps , para poder soportar y distribuir toda la cantidad de tráfico que en el satélite se manejaba (hasta 64 Kbps) se necesitaba de bastante equipo (modems) para que los tiempos de respuesta fueran lo más cortos posible y no se saturaran las líneas. Otra de las desventajas que se tenían era la presencia de las líneas privadas cuando el enlace satelital trabajaba siempre , ya que éstas nunca se usaban y había que pagar la renta se usaran o no.

Debido a que se tuvo la necesidad de abrir más sucursales para atender la demanda de los usuarios , la capacidad del enlace satelital empezó a ser insuficiente , por lo que surgió la necesidad de pagar por más ancho de banda ó por contar con una infraestructura. Por lo que el banco optó por ésta última , ya que al ir surgiendo la competencia , se vieron en la necesidad de tener una infraestructura basada en una tecnología , que no solo fuera la más avanzada , sino que también se apegara a los estándares para ser compatible y que estuviera a la altura para proporcionar un servicio mejor y más eficaz no solo a nivel regional sino a nivel nacional.

5.3 Análisis del sistema actual.

Como puede observarse en el diagrama de la fig. 5.2 , el sistema está conformado por dos redes de clase B , las cuales están conectadas y direccionadas para así lograr una red conjunta cuyo objetivo sea comunicar el centro de cómputo regional (y sus sucursales , como se muestra en la fig. 5.3) con el centro de cómputo principal , separados por una distancia de cientos de kilómetros y enlazados por dos medios de transmisión los cuales son:

- Enlace Satelital.
- Enlace de Superficie.

5.3.1 Descripción de la red.

Haciendo referencia al centro regional , existe una red local de topología en anillo (Token Ring) que maneja velocidades de 16 Mbps y está conectada a dos ruteadores que a su vez están enlazados al centro principal por medio de un enlace satelital y un enlace de superficie. Cabe hacer notar que el Token Ring tiene como objetivo ser el medio de comunicación y transmisión entre los dos ruteadores , donde a su vez entre ellos existe el intercambio de tablas de ruteo ; en caso de que el enlace principal (el satelital) se venga abajo , todo el tráfico y la información se conmutan hacia el ruteador "de superficie". Por lo general el ruteador "satelital" genera el token en la red (señal de inspección) para saber en que estado se encuentra el ruteador "de superficie" , a su vez éste sabe el estado que guarda aquel. Ahora bien , de todo lo anterior se consideran dos casos importantes , los cuales son :

FIG. 5.2 SISTEMA ACTUAL

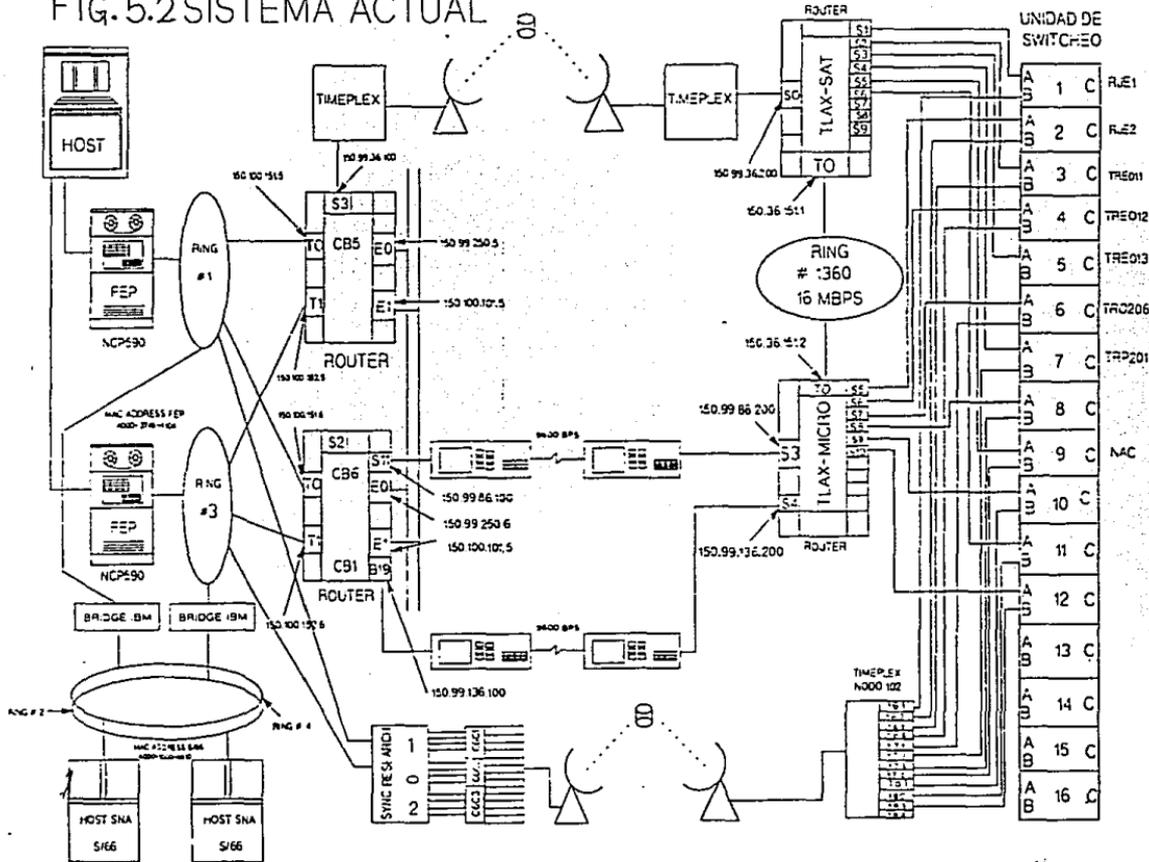
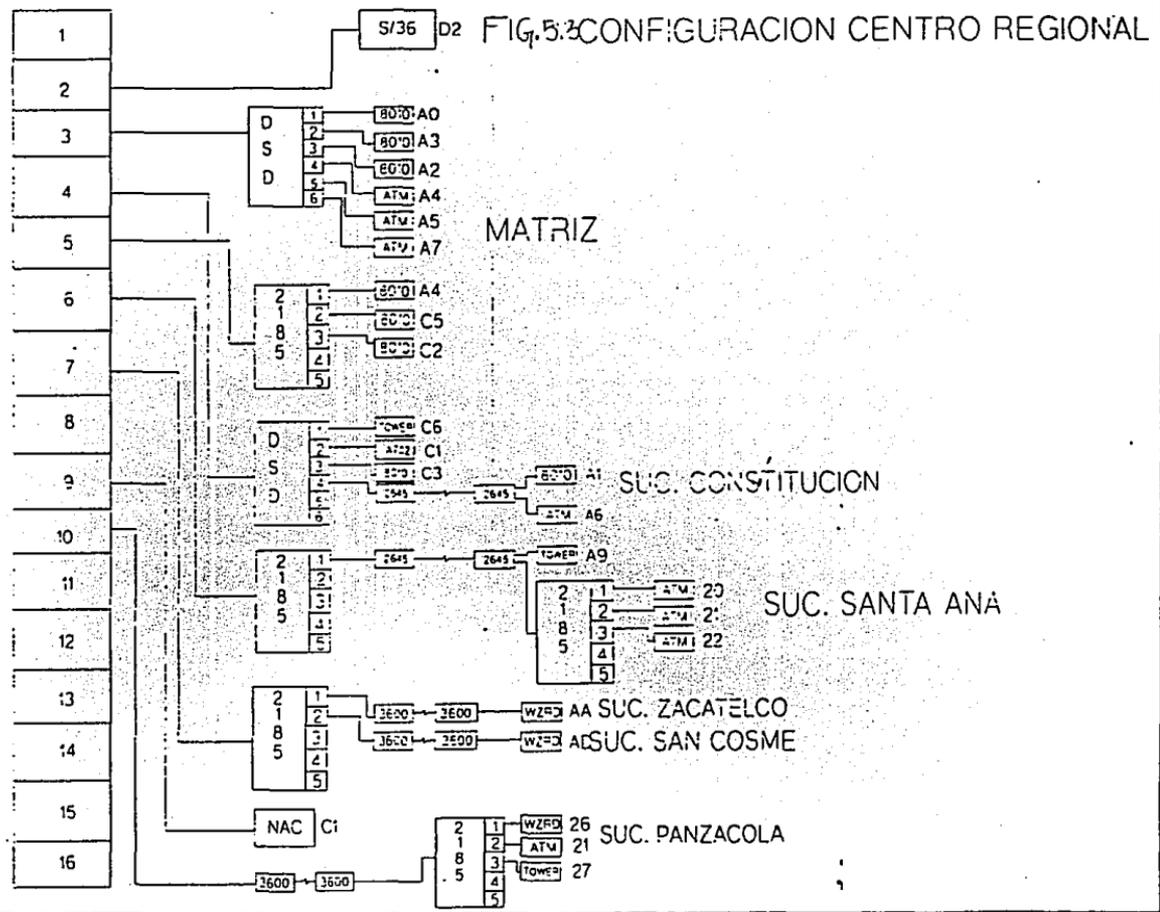


FIG. 5.3 CONFIGURACION CENTRO REGIONAL



- Cuando ambos ruteadores están trabajando (cabe hacer notar que los dos ruteadores siempre trabajan debido a que los servicios están repartidos) ; pero sólo por un enlace se mantiene la comunicación con el centro de cómputo principal y es mediante el satélite , esto es , que el ruteador "de superficie" envía la información de los servicios que atiende hacia el ruteador "satelital" por medio de la token ring , de manera que éste ruteador direcciona y comunica todos los servicios (tanto los atendidos por él como los del ruteador "de superficie") hacia el destino final.

- El segundo caso es cuando se viene abajo (o se pierde) el enlace satelital y todos los servicios que eran direccionados al enlace principal a través del ruteador "satelital" , son conmutados hacia el ruteador conectado al enlace de superficie para que lleguen a su destino final ; aquí ocurre exactamente lo mismo que en el primer caso , nada más que aquí la diferencia estriba en que los servicios del ruteador "satelital" son enviados hacia el ruteador "de superficie" a través del token ring para que toda la comunicación se realice por el enlace superficial. Por otro lado , se cuenta con una unidad de switcheo la cual es un dispositivo que está conectada tanto a los ruteadores como a todos los servicios que provienen de las sucursales ; lo que significa que todos éstos servicios pasan por la unidad de switcheo y viajan hasta el centro de cómputo principal por medio de los ruteadores. En caso de que se vengán abajo los dos enlaces (el satelital y el de superficie) , la unidad de switcheo está conectada hacia un multiplexor digital de respaldo y por este medio los datos requeridos por los usuarios regionales llegarán hasta su destino. El "switcheo" es hecho de forma manual.

Por el otro lado , haciendo referencia al centro de cómputo principal , también se cuenta con dos ruteadores el "satelital" y el de "superficie" , los cuales se encuentran conectados a tres redes token ring que a su vez están conectadas entre sí , ya sea por medio de los bridges o bien por los ruteadores. Como se observa en el diagrama (fig. 5.2) , se cuenta con una red Ethernet que tiene conectada una estación de trabajo cuyo objetivo es monitorear el estado de los cuatro ruteadores que integran la red. Por otro lado , entre los Hosts y las redes token ring (Rings 1 y 3 , redes principales) se encuentran los FEPs , cuya función es disminuir la carga y ahorrar el tiempo de procesamiento que se realiza en los hosts , de esta forma el sistema se vuelve más eficaz y reduce de manera significativa el tiempo de respuesta para los diferentes servicios.

En la red token ring (rings 2 y 4) de respaldo , se tienen conectados los hosts de respaldo , para auxiliar a los host y a las redes principales en caso de que por algún motivo queden fuera de servicio.

En conclusión , la integración de los ruteadores ha traído como consecuencia que el número de servicios aumente considerablemente , ya que los equipos proporcionan un funcionamiento de alta calidad en el manejo de velocidades de transmisión realmente altas y con la capacidad de soportar la diversidad de los protocolos empleados por cada arquitectura y en cualquier sistema de comunicaciones ; además , pueden concentrar diferentes funcionalidades como son : facilidades de soportar un gran número de conexiones hacia distintos tipos de redes de área local como Token Ring , Ethernet , FDDI , etc. ; así como una gran variedad en el manejo de distintos tipos de interfaces y medios de comunicación ; por otra parte , estos equipos están pensados para resolver necesidades a corto , mediano y largo plazo como por ejemplo , el ruteador puede modificarse dependiendo del crecimiento de la red , así como la facilidad de adaptarse a las nuevas tecnologías y ser totalmente compatible con estándares y otras recomendaciones.

A continuación se presenta una tabla en la que se explica detalladamente la función de los dos ruteadores que existen en el centro regional , estas tablas recopilan las características técnicas más importantes de los ruteadores. Primeramente se observa que existen diferentes tipos de direcciones , ya que cada protocolo utiliza sus propias direcciones , aquí podemos observar direcciones MAC (para el nivel dos) y las direcciones IP (para el nivel tres).

La tabla V-I está dividida en dos partes , cisco satellite y cisco terrestre (microondas) , en la primer columna se observan los puertos que existen en el ruteador tales como :

- TO : Este puerto indica que existe una conexión con una red Token Ring .
- EO : Este puerto indica que existe una conexión con una red Ethernet.
- SX : Este puerto indica que existe una conexión con otro ruteador (en el cual puede involucrar diferentes tipos de transmisión) , la X puede tomar cualquier valor , solamente es utilizado para identificar el número del enlace.

En la segunda columna se muestra qué tarjetas contienen los ruteadores y a su vez la tarjeta proporciona los puertos de conexión explicados anteriormente. Es importante señalar que también existe una relación por renglones.

La tercera columna indica el tipo de interface que debe tener cada puerto ; en la cuarta columna se muestra que solamente los puertos seriales pueden ser configurados como DTEs ó DCEs , pero no así los puertos correspondientes dedicados a la conexión hacia los puertos de la red ; el N/A indica no aplicable.

En la quinta columna podemos observar el código de línea que maneja cada puerto serial , como puede ser el código NRZ , NRZI u otro ; en la sexta columna se puede observar la velocidad que maneja cada puerto.

En la séptima columna se indica la dirección IP de cada red , es importante señalar que cada puerto de la red debe tener una determinada dirección , de esta misma forma , existe una dirección MAC address.

En la octava columna se indica la dirección "MAC address" la cual es utilizada en el nivel dos , posteriormente se encuentra la columna "ring" o anillo en la que se indica el número de anillo al que pertenece , y en la novena columna se indica a que bridge está relacionado este puerto , en las siguientes columnas se presentan las direcciones SDLC (del nivel dos).

En la tabla dos se observa la posición de las tarjetas (dentro del ruteador) y la posición de las interfaces (parte posterior).

NOTA:

Todo está referido al modelo de referencia OSI.

**ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA**

5.4 Hardware del Ruteador (Cisco).

Las conexiones externas hacia la red son mediante las interfaces y apliques que se encuentran en la parte posterior del "Router AGS+", hay varios tipos de interfaces como apliques ; existen 9 compartimientos (slots) para poder instalar hasta 9 tarjetas por "Router AGS+", las tarjetas están divididas en cuatro tipos de tarjetas:

- Tarjetas procesadoras.
- Tarjetas controladoras del cBus (Contenedor).
- Tarjetas de interface a red.
- Tarjetas de memoria.

A continuación se describen las tarjetas mencionadas anteriormente.

Tarjetas Procesadoras : son las supervisoras que contienen y ejecutan los programas que controlan el sistema , lo anterior es mostrado en la tabla (5-2).

TABLA 5-2

Descripción de la tarjeta procesadora.

TARJETA PROCESADORA	DESCRIPCION
Tarjeta Procesadora CSC/4	MC68ECO40 microprocesador (CPU) con 16 MB de RAM y reloj de 25 MHz.
Tarjeta Procesadora CSC/3	MC68020 Microprocesador (CPU) con 4MB en RAM y un reloj 30 MHz.

Tarjetas de Memoria: Las tarjetas de memoria son representadas por un término largo (NVRAM) nonvolatile random-access memory , son utilizadas para configuración y almacenamiento de datos.

En la tabla 5-4 se lista la memoria disponible para el equipo AGS+ .

Tabla 5-4.

TARJETA	DE	MEMORIA	DESCRIPCION
CSC-MC+			Combinación opcional de memoria FLASH y aplique NVRAM que permite conectarse y almacenar diferentes software. La conexión puede realizarse a las siguientes tarjetas CSC-MCI, CSC-2R Y CSC 1R.
CSC-ENVM			Esta tarjeta monitorea el ambiente del interior del equipo NVRAM y 64Kbytes de almacenamiento en el buffer.

Tarjeta de Interface a Red : Estas tarjetas conectan el AGS+ a una o más redes , en la tabla 5-5 , se describen estas tarjetas.

Tabla 5-5.

TARJETA	DESCRIPCION
CSC-C2MEC	2, 4 ó 6 puertos Ethernet de alta velocidad .
CSC-C2FCI	Interface de comunicación FDDI a una razón de 100 Mbps.
CSC-C2FCIT	Interface de comunicación con la capacidad de traslación de puenteo.
CSC-C2HSCI	Un puerto con interface serial síncrona de alta velocidad , con velocidades de transmisión de hasta 52 Mbps dúplex con interface HSSI ó con velocidades de hasta 125 Mbps dúplex con interface Ultra Net.
CSC-MCI	Dos puertos Ethernet y dos puertos seriales síncronos , con velocidades transmisión de 4 Mbps para los puertos seriales y 10 Mbps para los de Ethernet.
CSC-SCI	Cuatro puertos seriales síncronos con velocidades de transmisión de 4 Mbps cada uno .
CSC-R1GM	Tarjeta con interface para Token Ring manejando el software MADGE , con velocidades de transmisión de 4 ó 16 Mbps seleccionables por medio de un jumper.
CSC-1R	Tarjeta con un solo puerto para Token Ring , con velocidades de 4 ó 16 Mbps, seleccionable por medio del software.
CSC-2R	Versión dual de la tarjeta anterior con las mismas características.

CSC-C2CTR

Tarjeta de Token Ring para 4 puertos
cBus , con velocidades de transmisión
de 4 ó 16 Mbps seleccionables por
medio del software. También se cuenta
con una versión de dos puertos.

Como se mencionó anteriormente todos los servicios se encuentran conectados al Router (cada conexión cumple con un determinado tipo de interfaz dependiendo del servicio que esté atendiendo , cada router contiene diferentes slots , en los cuales se instalan diferentes tarjetas dependiendo de las necesidades que se requieran , las tarjetas que existen en este router son :

CSC ENVM : Cisco enviromental monitor card , la cual es una tarjeta de monitoreo ambiental , que detecta las condiciones de voltaje y temperatura para garantizar una adecuada suspensión forzada de las operaciones , en el caso de condiciones anómalas en el sistema.

CSC /R : Tarjeta de Token Ring , es una tarjeta para puerto de una red Token Ring , la cual utiliza un determinado tipo de conector (en este caso DB9).

En general existen diferentes tipos de tarjetas que se utilizan en diferentes aplicaciones, las cuales contienen un determinado tipo de interfaz, y si es posible configurarlo como DTE o como DCE, también maneja un código de línea, cada una de estas tarjetas es probable que contenga una dirección.

TABLA 5-6 Límite de Puertos para el AGS+.

No. de Tarjetas	Tipo de Tarjetas	Tipo de Interface	No. máx. De puertos
1	CSC-ENVM	Conexión pBus para Flash memory	1
1	Procesador CSC/3 ó CSC/4 (uno u otro)	Consola Auxiliar	1 1
1	CSC-CCTL ó CCTL2 (uno u otro si se desea la tarjeta cBus)	n/a	n/a
6	CSC-SCI-4S ó 4T	RS232 (y RS232 NRZI) ó HDV35	24
6	CSC-SCI-4S ó 4T	RS449	14
6	CSC-MCI-2E2T ó 2E2S	Ethernet y serial	12 12
6	CSC-MCI-2E	Ethernet	12
6	CSC-1R	Token Ring 4/16Mbps velocidades seleccionables	6
6	CSC-2R	Token Ring 4/16Mbps velocidades seleccionables	12
6	CSC-R16M	Token Ring 4/16Mbps velocidades seleccionables, con código MADGE	6

4	CSC-MEC 6 (mÁn una CSC-MCI2E)	Ethernet	26
2	CSC-FCI	Modo simple/multimodo FDDI	2
4	CSC-C2FCIT (con capa cidad de traslaci3n de puenteo)	Modo simple/multimodo FDDI	4
4	CSC-HSCI	HSSI	4
2	Ultra Net (CSC-HSCI)	Ultra Net (HSSI)	2

CAPITULO SEIS

CONCLUSIONES

Como se ha visto , la evolución de los sistemas de comunicación de datos se ha dado de una forma muy rápida debido al desarrollo acelerado de las industrias y sus necesidades de comunicación que así lo han requerido. Por lo mismo , el mercado empezó a saturarse de comerciantes con una gran cantidad de productos que eran ofrecidos para presentar soluciones inmediatas , el gran problema que surgió fue que cada uno de ellos empleaba tecnología propia , lo que trajo como consecuencia la incompatibilidad de interconectar los sistemas instalados. De ahí que surgieron varias organizaciones (a nivel regional) para manejar una norma a la que se apegaran sus productos. Como prevalecía la incompatibilidad (ahora entre organizaciones) surgió la ISO con el Modelo de Referencia OSI que proponía trabajar por niveles , los cuales se manejan en forma independiente , pero existiendo relación entre todos y cada uno de ellos ; de ésta forma , gracias al empleo de éste modelo , se ha logrado que tanto las organizaciones como las compañías (en la elaboración de sus productos) se apeguen a las recomendaciones de la ISO para que todos proporcionen soluciones satisfactorias y totalmente compatibles.

Por otra parte , se ha visto cómo la evolución de las comunicaciones ha tenido sus etapas : primero , se hablaba de usuarios que empleaban terminales en las que recababan la información en un disco por separado ; en segunda instancia , la aparición de las computadoras cuya capacidad de memoria permitía almacenar grandes cantidades de información en un disco interno ; tercero , la creación de las redes de computadoras , en las que se interconectaban todas ellas de tal forma que pudieran compartir recursos de software y periféricos , además de tener intercambio de información (por ejemplo transferencia de archivos , manejo del correo electrónico , abrir sesiones remotas , tener cierto control de la información , etc.) ; como cuarto punto , se hace mención de la llegada de las redes de área local (LAN) cuya estructura se basa en las recomendaciones de la OSI y en el manejo de protocolos estándar que actualmente son aceptados totalmente por la industria de la ingeniería en comunicaciones y quinto , la necesidad de hoy en día :

comunicar las redes locales existentes no sólo a nivel regional si no también a niveles de expansión más grandes , lo que en otras palabras , se le conoce como las redes WAN y MAN.

Para lograr ésto , las organizaciones a nivel estándar mundial junto con las empresas que desarrollan los productos de integración , se han dado a la tarea de crear el concepto internetworking , el cual (a través del trabajo desarrollado) se puede definir como la conexión de dos ó más redes independientes ubicadas en distintas zonas geográficas , por medio de dispositivos que manejen toda una serie de recomendaciones y estándares (basándose en el modelo de referencia OSI) para cumplir con el objetivo de que sean lo suficientemente poderosos , capaces , confiables y sobre todo compatibles.

Dentro de los capítulos incluidos se hizo referencia a los dispositivos de internetworking más utilizados como son las gateways , los bridges y los ruteadores ; en donde éstos dos últimos , serán la mejor solución (a futuro) para las compañías , ya que atenderán las principales necesidades de los sistemas LAN. Dentro de éstas necesidades se incluyen el soporte para los principales ambientes LAN (Ethernet , Token Ring y FDDI) , independencia de los protocolos (DECnet , TCP/IP , IPX) manejados en redes paralelas para asegurar la interconectividad entre los productos ofrecidos por cualquier vendedor , soporte para servicios WAN de alta velocidad (E1/T1) , etc. Estas nuevas redes WAN integradas con bridges/ruteadores ofrecerán a los usuarios una arquitectura WAN que consolide equipo , instalación y administración ; todo esto será una base sólida para nuevas aplicaciones de alto funcionamiento tales como imágenes , bases de datos distribuidas y otras aplicaciones cliente/servidor.

El movimiento hacia la integración de la internetworking , tendrá un gran impacto en un futuro cercano , facilitando la transferencia de grandes volúmenes de información , abriendo un panorama relevante y proyección futura dentro de las estrategias de las corporaciones y grandes usuarios.

Por lo que toca a los ruteadores , éstos son dispositivos que actualmente están teniendo un tremendo crecimiento en importancia debido a que son muy versátiles , capaces , flexibles y sobre todo están hechos para adaptarse a crecimientos futuros.

Con respecto al desarrollo del presente trabajo , se puede hacer mención de que se ha cumplido gran parte del objetivo que se tenía planeado al principio : el de aprovechar los fundamentos y los conceptos teóricos adquiridos durante la elaboración de éste. Todo lo aprendido , ha venido a complementarse con la práctica debido a que de alguna manera los equipos manejados (como modems , multiplexores , concentradores , compresores , convertidores de interface , equipos de radio y microondas , equipos para videoconferencia , equipos para redes de paquetes y los ya analizados como las gateways , los bridges y los ruteadores) y las empresas que los producen , se apegan tanto a la estructura del modelo de referencia OSI así como a los protocolos y a las normas recomendadas.

Otro aspecto importante que hay que hacer notar , es la rápida evolución que se presenta en la rama de las comunicaciones , ya que constantemente las empresas liberan nuevas versiones de sus equipos (nuevas características y capacidades tanto a nivel de software como de hardware) los cuales presentan novedades con respecto a las versiones anteriores , de manera que uno debe estar estudiando frecuentemente para estar al tanto de la nueva información. Una cosa que sí es interesante , es que la ingeniería de redes es muy extensa y muy variada en lo que a conceptos se refiere , por lo que nunca se deja de aprender y de estudiar.

Algo más que vale la pena comentar , es que a través de la investigación , el consultar a ingenieros con bastante experiencia dentro del campo y la elaboración de éste trabajo , de alguna manera todo se ha complementado y ha sido de gran ayuda al momento de estar en la práctica para analizar y buscar la solución de un problema real , aparte de que ya estando ahí es cuando también se ha aprovechado la ocasión para platicar con gente experimentada de la cual se le puede aprender tanto los conocimientos así como la astucia que tienen para dar solución a los problemas.

Dentro de los problemas que se tuvieron durante el desarrollo del trabajo principalmente son la estandarización de los diferentes sistemas de comunicación , como por ejemplo el sistema OSI que no se encuentra instalado y funcionando en su totalidad sino que existen arquitecturas muy similares que de alguna manera tienden a cumplir con las recomendaciones de OSI en un futuro , sin querer decir que no exista la internetworking como tal , ya que en la práctica real se realiza ésta comunicación tomando como partida las características principales de ésta recomendación. Otro

problema que se encontró fue el de los protocolos (debido a que cada protocolo requiere de un extenso conocimiento) sólo se habló de lo esencial de cada uno de ellos para poder comprender ésta tesis , ya que no está dentro de los objetivos del trabajo. Por otra parte , debido a que la mayor parte de la bibliografía consultada está en idioma inglés y que todos éstos conceptos son empleados a nivel mundial y que cada uno de los países los traduce en su idioma y a su forma de ver las cosas , nosotros nos apegamos al idioma inglés y a la forma como se maneja en el país.

Por último , esperamos que la otra parte del objetivo se cumpla : que ésta tesis sirva como una base de referencia teórica y una ayuda para las materias del área de comunicaciones.

BIBLIOGRAFIA

1. **Internetworking**
A Guide to Network Communications
LAN to LAN ; LAN to WAN
Mark A. Miller
M&T Books
USA 1992
2. **LAN Primer**
An Introduction to Local Area Networks
Greg Nunemacher
M&T Books
USA 1992
3. **LAN Protocol Handbook**
Mark A. Miller
M&T Books
USA 1992
4. **Internetworking**
Technology Overview
CiscoSystems
USA 1993
5. **Internetworking**
Concepts Seminar
CiscoSystems
USA 1991
6. **LAN Internetworking:**
The next evolutionary step
Racal Data Communications (Folleto)
USA 1990
7. **Networking**
Dictionary
Racal-Datacom
USA 1992
8. **LAN Hub**
Applications Guide
ADC Fibermux Co.
USA 1992
9. **3+Open Client-Server System:**
3Station and 3Server
3Com (Folleto)
USA 1989-1990

10. **DataPro**
CD-ROM Communications Equipment
Bureau Van Dijk
Mc. Graw Hill Inc.
USA 1992
11. **Teleinformática y Redes de Computadoras**
Antonio Alabau Muñoz
Marcombo
ESPAÑA 1982
12. **Interconexión de Redes:**
Términos y Acrónimos
CiscoSystems (Manual)
USA 1992
13. **IDC White Paper**
Informe Especial Sobre Integración de Redes
LAN-WAN
RAD (Folleto)
USA 1992
14. **Redes de Area Local:**
La Siguiete Generación.
Thomas W. Madron
Megabyte Gpo. Noriega Editores
MEXICO 1992
15. **Redes de Computadoras**
Protocolos , Normas e Interfaces
Uyless Black
Macrobit Ra-Ma
MEXICO 1990