47
2ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS
A R A G O N

" INTERCONEXION DE UNA RED LAN Y UNA RED WAN"

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A

JOSE ALBERTO PEÑA FLORES

ENEP ARAGON

MEXICO, D.F. 1997

INTERCONEXIÓN DE UNA RED LAN Y UNA RED WAN

INDICE.

CAPÍTULO 3. PROTOCOLOS.

CAPíTULO 4. INTERCONECTIVIDAD.

AGRADECIMIENTOS

- **A MIS PADRES**
  ANTONIA FLORES PRADO Y RAUL PEÑA FLORES

Por todo el amor, por haberme dado la vida y fundamentalmente por educarme e inculcarme los valores que ahora poseo.
Porque gracias a su apoyo, comprensión, confianza y cariño siempre brindados, he realizado una de las metas más importantes de mi vida, lo cual constituye la herencia más valiosa que pude recibir de ellos.

- **CON FRATERNAL CARIÑO PARA MIS HERMANOS.**
  ROSA MARÍA, CELIA, ALICIA, RICARDO Y RAUL.

Porque cada uno de ellos de alguna forma me motivaron para lograr este objetivo, por su apoyo incondicional, gracias.

- **A MIS AMIGOS.**
  ALEJANDRA, COLUMBA, LILIANA, MARCELA, ADRIAN, CARLOS, EUSEBIO, FEDERICO, MIGUEL.

Por haberme brindado su amistad desinteresadamente y haber contribuido para mi superación personal y profesional, todos de distinta forma. Gracias por ser mis grandes amigos.

- **UN ESPECIAL AGRADECIMIENTO A:**
  MANUEL MARTINEZ ORTIZ

Por haberme apoyado y dirigido en la realización del presente trabajo.

- **A MIS PROFESORES.**

Que a lo largo de mi vida han contribuido con su sapiensa y sencillez a mi formación profesional.
Gracias por haberme transmitido sus conocimientos.

A TODOS LES DOY LAS GRACIAS.

JOSE ALBERTO.

INTERCONEXIÓN DE UNA RED LAN Y UNA RED WAN.

Objetivo:

Describir las alternativas que se tienen para comunicar redes LAN con redes WAN para el intercambio de información.

INTRODUCCIÓN

Recientemente, para resolver la necesidad de hacer más eficiente el uso de recursos de computación en organizaciones de todo tipo, surgieron las redes de computadoras. En el mundo actual, se han convertido en elementos de fundamental importancia y todo indica que la tendencia seguirá, incorporando tecnologías cada vez más novedosas para obtener mayor velocidad de transferencia y seguridad de los datos, así como la compatibilidad de productos de diversos fabricantes.

Sin embargo, a pesar de que todos utilizamos directa o indirectamente los servicios de las redes de computadoras, al acudir a una institución bancaria, un supermercado, una institución gubernamental o una empresa privada, muchas personas ignoran algunos conceptos básicos al respecto.

En el presente se incluirá una breve historia de las redes de computadoras así como una descripción general de sus elementos más importantes, se describirán las funciones de las capas del Modelo de Referencia OSI (*Open Systems Interconnection*), se tratará acerca el funcionamiento de las Redes de WAN (*Wide Area Network*) enfocado hacia la Conmutación de Circuitos y Conmutación de Paquetes, se describirán algunos de los protocolos utilizados dentro de las redes, se explicará el funcionamiento de los dispositivos utilizados para interconectar redes (Puentes, Ruteadores y *Gateways*).

CAPÍTULO I. MODELO OSI.

Objetivo:

Describir las características principales del modelo de referencia OSI como estándar de comunicaciones de redes de área local.

CAPITULO 1. MODELO OSI.

Como la mayoría de los proyectos de ingeniería, independientemente de la disciplina, las redes cuentan con una serie de estándares o normas que definen su funcionamiento en todos los aspectos. Por ello se establecen los modelos de referencia cuya finalidad se divide en dos puntos básicos:

- Flexibilizar la implementación de una red dividiéndola en capas o niveles de software interactuando jerárquicamente.

- Estandarización de los diversos fabricantes tanto de hardware como de software del modelo de referencia más utilizado en la actualidad y por lo mismo, objeto de éste capítulo es el llamado modelo OSI.

En 1978 la Organización Internacional de Estándares (ISO *International Standards Organization*) propuso un modelo para comunicaciones de redes locales al que titularon Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI *The Reference Model of Open Syetms Interconnection*).

"Interconexión de Sistema Abiertos" significa el intercambio de información entre terminales, microcomputadoras, personas, redes y procesos.

El modelo de referencia no es por sí mismo un estándar, ni una descripción de las comunicaciones entre microcomputadoras. El modelo

define dónde se han de efectuar las tareas, pero no cómo se han de efectuar. No especifica servicios ni protocolos.

El modelo OSI intenta proporcionar una base común para coordinar el desarrollo de estándares dirigidos a la conexión entre sistemas.

1.1. MODELO OSI .

El modelo de referencia OSI fue creado para hacer posible "la definición de procedimientos estandarizados que permitan la interconexión y el intercambio efectivo de información entre usuarios", en donde el término "usuarios" se refiere a sistemas que constan de una o más computadoras, software asociado, periféricos, terminales, operadores humanos, procesos físicos, mecanismos de transferencia de información y elementos relacionados. Estos elementos juntos, deben poder "realizar procesamiento y/o transferencia de información". Los estándares desarrollados a partir del modelo de referencia permitirán a diversas redes del mismo tipo o diferentes comunicarse fácilmente entre sí, como si constituyeran una misma red.

Al principio es importante tener presente que el apego al modelo de referencia no implica ninguna implantación de tecnología en particular. Dicho de otra manera, no especifica un medio (como cable de fibras ópticas, par trenzado o coaxial), ni un conjunto específico de recomendaciones como las redes 802.3, 802.4 u 802.5 del IEEE. El modelo está diseñado para soportar procedimientos de intercambio de

información estandarizados, pero no ofrece detalles o definiciones ni protocolos de interconexión. Por lo tanto el modelo OSI es un marco de referencia para sistemas abiertos y los detalles de la implantación se dejan a otros estándares.

La recomendación OSI identifica las siete capas funcionales mostradas en la figura 1.1. Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física. La meta de una red de comunicación de datos es intercambiar información entre aplicaciones o usuarios. La información a ser transferida debe ser formateada, empaquetada, ruteada y entregada. El receptor debe entonces desempacar y probablemente reformatear la información. Esas son esencialmente las funciones ejecutadas por las siete capas.

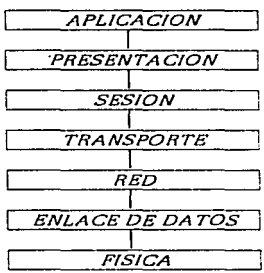


Fig. 1.1. Capas del Modelo OSI

La figura 1.2. describe las capas en dos diferentes procesadores la información de la capa de aplicación en el procesador 1 se mueve hacia

abajo a través de las diversas capas hasta alcanzar la capa física, la cual transmite los datos a la capa física del procesador 2. Los datos entonces trabajan ascendentemente a través de los niveles en el procesador 2 hasta alcanzar el nivel de aplicación.

Cada capa en el procesador transmisor ejecuta su trabajo para ser entendido por su correspondiente nivel en el procesador receptor. Entonces las capas de presentación apoyan a capas de presentación, las capas de sesión apoyan a otras capas de sesión y así sucesivamente. Entre las diferentes capas existen interfaces a través de las cuales pasan los datos. Esas interfaces son flexibles de tal modo que los diseñadores pueden implementar varios protocolos de comunicación y aun seguir el modelo de referencia OSI.

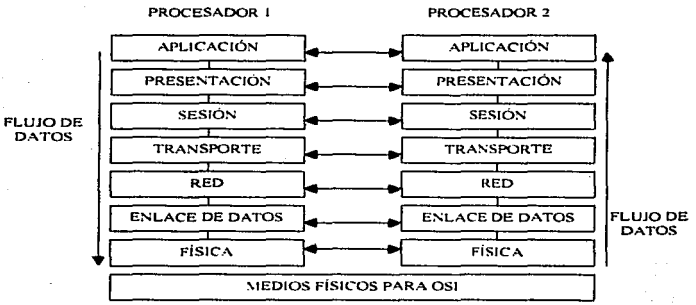


Fig. 1.2 Flujo de Datos en 2 Procesadores de Acuerdo al Esquema del Modelo OSI

1.2. CAPAS DEL MODELO OSI.

El sistema se compone de un conjunto ordenado de capas o niveles. Los niveles del modelo OSI están separados por interfaces. Los niveles adyacentes se comunican entre sí por medio de una interfaz común.

Todos los niveles de la estructura disponen de un conjunto de servicios para el nivel superior e inferior. La relación entre los distintos niveles y la información se comunican entre sí por medio de una interfaz común.

Las interfaces se encuentran donde un nivel se comunica con otro, y sirven para separar un nivel del siguiente. Como es fácil esperar que los mecanismos y funciones de los niveles cambien a medida que cambia la tecnología, las funciones de las interfaces están bien definidas, pero el formato utilizado para transferir datos entre niveles no lo está. Esto permite cambiar las características de un nivel sin que afecte al resto del modelo.

1.2.1. CAPA FÍSICA.

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su dueño debe asegurar que cuando un extremo envía un bit con valor 1, éste se reciba exactamente como un bit de ese valor en el otro extremo, y no como un bit de valor 0. Preguntas

comunes aquí son cuántos voltios deberán utilizarse para representar un bit de valor 1 o 0, cuantos microsegundos deberá durar un bit, la posibilidad de realizar transmisiones bidireccionales en forma simultánea, la forma de establecer la conexión inicial y cómo interrumpirla cuando ambos extremos terminan su comunicación, o bien, cuántas puntas terminales tiene el conector de la red y cuál es el uso de cada una de ellas. Los problemas de diseño a considerar aquí son los aspectos mecánico, eléctrico, de procedimiento de interfaz y el medio de transmisión física, que se encuentra bajo la capa física. Se puede considerar que el diseño de la capa física cae dentro del dominio del ingeniero eléctrico.

1.2.2. CAPA DE ENLACE DE DATOS.

La tarea primordial de la capa de enlace de datos consiste en que, a partir de un medio de transmisión común y corriente, transformarlo en una línea sin errores de transmisión para la capa de red. Esta tarea la realiza al hacer que el emisor separe los datos en tramas de datos (típicamente constituidas por algunos cientos de octetos), y las transmita en forma secuencial y procese las tramas devueltas por el receptor. Como la capa física básicamente acepta y transmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace de datos la creación o reconocimiento de los límites de la trama. Esto puede llevarse a cabo mediante la inclusión de un patrón de bits especial al inicio y al término de la trama. Si estos patrones de bits pueden

aparecer entre los datos, deberá tenerse un cuidado especial para evitar cualquier confusión al respecto.

La trama puede destruirse por completo debido a una ráfaga de ruido en la línea, en cuyo caso el software de la capa de enlace de datos perteneciente a la máquina emisora, deberá retransmitir la trama. Sin embargo, múltiples transmisiones de la misma trama introducen la posibilidad de duplicar la misma. Por ejemplo, el duplicado de una trama podría enviarse si el acuse de recibo que regresa al receptor se hubiera destruido. Corresponde a esta capa resolver los problemas causados por daño, pérdida o duplicidad de tramas. La capa de enlace de datos ofrece diferentes clases de servicios a la capa de red.

Otro de los problemas que aparecen en la capa de enlace de datos (y también en la mayoría de las capas superiores) es el referente a cómo evitar que un transmisor muy rápido sature con datos a un receptor lento. Se deberá emplear un mecanismo de regulación de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor. Frecuentemente y por conveniencia, los procedimientos de regulación de flujo y control de errores se tratan en forma conjunta.

Otra dificultad aparece cuando la línea tiene la capacidad de utilizarse para transmitir datos bidireccionalmente. El problema radica en que el tráfico del transmisor A al receptor B compiten por el uso de la línea con las tramas de los datos del tráfico que va desde el receptor B hacia el transmisor A.

1.2.3. CAPA DE RED.

La capa de red se ocupa del control de la operación de la subred. Un punto de suma importancia en su diseño es la determinación sobre cómo encaminar los paquetes del origen al destino. Las rutas podrían basarse en tablas estáticas que se encuentran "cableadas" en la red y que difícilmente podrían cambiarse. También, podrían determinarse al inicio de cada conversación, por ejemplo en una sesión de terminal. Por último, podrían ser de tipo dinámico, esto es en forma diferente para cada paquete, reflejando la carga real de la red.

Si en un momento dado hay demasiados paquetes presenten en la subred, ellos mismos se obstruirán mutuamente y darán lugar a un cuello de botella. El control de tal congestión dependerá también de la capa de red.

Pueden surgir problemas cuando un paquete tenga que desplazarse de una red a otra para llegar a su destino. El direccionamiento utilizado en la segunda red puede ser diferente al empleado en la primera. La segunda podría no aceptar el paquete en su totalidad por ser demasiado grande, los protocolos podrían ser diferentes, etcétera. La responsabilidad, para resolver problemas de interconexión de datos de redes heterogéneas recaerá, en todo caso, en la capa de red.

1.2.4. CAPA DE TRANSPORTE.

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. Además, todo éste trabajo se debe hacer de manera eficiente, de tal forma que aísle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.

Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red, dividiendo los datos entre ellas con objeto de mejorar dicho flujo de datos. Por otra parte, si la creación o mantenimiento de la conexión de una red resulta costosa, la capa de transporte podría multiplexar varias conexiones sobre la misma red para reducir dicho costo. En todos los casos, la capa de transporte se necesita para hacer el trabajo de multiplexión transparente a la capa de sesión.

La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red. El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes en el mismo orden en que fueron enviados. Sin embargo, el transporte de mensaje aislados sin garantizar el orden de distribución y la difusión de mensajes

a destinos múltiples es otra posibilidad de servicio de transporte el tipo de servicio se determina cuando se establece la conexión.

La capa de transporte es una capa de tipo origen-destino o extremo a extremo. Es decir, un programa en la máquina origen lleva una conversación con un programa parecido que se encuentra en la máquina destino, utilizando los encabezados (*headers*) de los mensajes y los mensajes de control.

Además de multiplexar varios flujos de mensajes en un canal, la capa de transporte debe ocuparse del establecimiento y liberación de conexiones a través de la red. Esto requiere algún mecanismo de denominación, de tal forma que un proceso en una máquina tenga una manera de describir con quién desea conversar. También debe haber un procedimiento para regular el flujo de información, de manera que un equipo muy rápido no pueda desbordar a otro más lento.

1.2.5. CAPA DE SESIÓN.

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utiliza en algunas aplicaciones. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido, transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo. Las sesiones permiten que el tráfico vayan en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si el tráfico sólo puede ir en una dirección en un momento dado, la capa de sesión ayudará en el seguimiento de quien tiene el turno.

Otro de los servicios de la capa de sesión es la sincronización. Considérense, por ejemplo, los problemas que podrían ocurrir cuando se trata de hacer una transferencia de un archivo de dos máquinas en una red con un tiempo medio de una hora entre caídas. Después de abordar cada archivo, la transferencia completa tendría que iniciarse de nuevo y, probablemente, se encontraría de nuevo con la siguiente caída de la red. Para eliminar este problema, la capa de sesión proporciona una forma para insertar puntos de verificación en el flujo de datos, con objeto de que, después de cada caída, solamente tengan que repetirse los datos que se encuentran después del último punto de verificación.

1.2.6. CAPA DE PRESENTACIÓN.

La capa de presentación realiza ciertas funciones que se necesitan frecuentemente para buscar una solución general para ellas, más que dejar que cada uno de los usuarios resuelva los problemas. En particular y, a diferencia de las capas inferiores, que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de

presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

Un ejemplo típico de servicio de la capa de presentación es el relacionado con la codificación de datos. La mayor parte de los programas de usuarios no intercambian secuencias de bits binarios aleatorios, sino, más bien, cosas como nombres de personas, datos, cantidades de dinero y facturas. Estos artículos están representados por secuencias de caracteres, Números enteros, números de punto flotante, así como por estructuras de datos constituidas por varios elementos más sencillos. Las computadoras pueden tener diferentes códigos para representar las secuencias de caracteres como el Código Estándar Americano para Intercambio de Información (ASCII *American Standard Code for Information Interchange*), enteros, etc. Para posibilitar la comunicación de las computadoras con diferentes representaciones, la estructura de los datos que se va a intercambiar puede definirse en forma abstracta, junto con una norma de codificación que se utilice en el cable. El trabajo de manejar estas estructuras de datos abstracta y la conversión de la representación utilizada en el interior de la computadora a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

La capa de presentación está relacionada también con otros aspectos de representación de la información. Por ejemplo, la compresión de datos se puede utilizar aquí para reducir el número de bits que tiene que transmitirse y el concepto de criptografía se necesita utilizar frecuentemente por razones de privacidad u autentificación.

1.2.7. CAPA DE APLICACIÓN.

La capa de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos de terminales incompatibles en el mundo. Considérese la situación de un editor orientado a pantalla que desea trabajar en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de pantalla, de secuencias de escape para insertar y borrar texto, de movimientos de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracta, con el que los editores y otros programas pueden ser escritos para tratar con él.

Con objeto de transferir funciones del terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software deberá emitir la secuencia de comandos apropiados para que la terminal real ubique también su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la capa de aplicación.

Otras funciones de la capa de aplicación es la transferencia de archivos. Distintos sistemas de archivo tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las líneas de texto, etcétera. La transferencia de archivos entre dos sistemas diferentes requiere la resolución de éstas y otras

incompatibilidades. Este trabajo, así como el correo electrónico, el servicio de directorio y otros servicios de propósito general y específico, también corresponden a la capa de aplicación.

1.3. EJEMPLO DEL MODELO OSI.

Utilizando el siguiente ejemplo serán descritas las actividades que podrían ocurrir en cada nivel del modelo de referencia como una aplicación de un nodo de red transmitiendo un mensaje a una aplicación a otro. Considerando una aplicación financiera corriendo en la red, ilustrada en la figura 1.3. Suponga que un cliente bancario utiliza un cajero automático conectado al nodo A las cuentas de los clientes están conectadas en el nodo X. Una aplicación de transacción orientada en el nodo A envía información al nodo X requiriendo que los registros de las cuentas de los clientes sea actualizadas por una aplicación corriendo en el nodo X. Para alcanzar el nodo X, la aplicación debe pasar a través del nodo M.

Capa de aplicación.- La aplicación en el nodo A construye un registro con un identificador de transacción, se debe actualizar el número de la cuenta, la fecha y hora de la transacción, así como el monto a ser deducido o adicionado. El identificador de transacción le dice al mensaje que hacer con el registro: insertarlo, actualizarlo, etc.. El mensaje es ilustrado en la figura 1.4 (a). La aplicación invoca un procedimiento para enviar el mensaje al receptor.

Capa de presentación.- La capa de aplicación formatea cada campo en el registro que está siendo transmitido de acuerdo a sus propias reglas de formato. La aplicación receptora puede tener un formato diferente. Por ejemplo, la aplicación transmisora puede ver una fecha en un formato mientras la aplicación receptora usa un formato de fecha diferente. La capa de presentación es responsable de traducir de un formato a otro. Esto puede hacerlo cambiando a un formato de transmisión estándar, el cual es convertido por la misma capa del nodo receptor, o puede convertirlo directamente al formato esperado por la aplicación receptora. El mensaje después de haber sido traducido aparece tal como se muestra en la figura 1.4 (b). La capa de presentación entonces envía el mensaje hacia la capa de sesión solicitando el establecimiento de una sesión.

Capa de sesión.- Las funciones principales de la capa de sesión son organizar y quizás monitorear un grupo de reglas de diálogo por las cuales las dos aplicaciones se comunican y traer una sesión a una conclusión ordenada. Una sesión de diálogo puede ser en un sentido (*simplex*) o bidireccional (*duplex*). En una transmisión *simplex*, una aplicación envía mensajes a otra pero no recibe mensajes de regreso. La sesión *duplex* puede permitir mensajes en ambas direcciones simultáneamente (*full duplex*) o en ambas direcciones pero solo en una dirección a la vez (*half duplex*). El ambiente de cómo son transmitidos los mensajes es llamado control de flujo. Una vez que la conexión ha sido hecha, la transferencia de datos puede realizarse. La capa de sesión añade un identificador y un indicador de longitud al principio de cada bloque de datos, como se muestra en la figura 1.4 (c). Estos dos campos

son usados para identificar la función del mensaje, por ejemplo, ya sea que ésta contenga datos de usuarios opuestos a las funciones de control como establecimiento de sesión o terminación.

Capa de transporte.- La capa de transporte es la primer capa OSI responsable de la transmisión de datos. Las capas superiores descritas anteriormente están orientadas directamente a los datos e interfaces de aplicación, no hacia la transmisión de datos. La capa de transporte usa una dirección llamada punto de acceso de servicio de transporte (TSAP *Transport Service Access Point*) para únicamente identificar las entidades de sesión. Los TSAP´s de la entidad de sesión fuente y destino, junto con un algoritmo de verificación (*checksum*) para detectar errores, son agregados al mensaje recibido de la capa de sesión. El *checksum* es creado por el emisor de acuerdo a un algoritmo. El receptor también crea uno propio usando el mismo algoritmo. Si el *checksum* del emisor y del receptor coinciden, el dato se asume que es correcto. Este paso es mostrado en la figura 1.4 (d).

Capa de red.- La capa de red realiza funciones de contabilidad, direccionamiento y ruteo. Al recibir un mensaje de la capa de transporte, la capa de red registra el evento en el sistema de contabilidad y entonces prepara el mensaje para transmitirlo al próximo nodo en la ruta de destino (nodo M en nuestro ejemplo). Este busca la dirección destino en su tabla de ruteo de red para encontrar la próxima dirección a lo largo de la ruta. Si el mensaje es demasiado largo, la capa de red lo divide en unidades de transmisión, adicionadas al número de secuencia de cada

unidad y envía las unidades a través del enlace. Esto se ilustra en la figura 1.4 (e).

Capa de enlace de datos.- La capa de enlace de datos es responsable de la delineación de datos, detección de errores y control lógico del enlace. El control lógico del enlace consiste en determinar cómo y cuando una estación puede transmitir, conectando y desconectando nodos en el enlace, y controlando el flujo entre los nodos A y M y entre los nodos M y X. Nótese que el control de flujo del enlace de datos es para un enlace, mientras que el control de flujo de sesión es entre las aplicaciones fuente y destino. Para cumplir está función, la capa de enlace de datos agrega un *header* y una cola (*trailer*) al mensaje. El *header* contiene una bandera que indica el inicio del mensaje, la dirección del receptor, el número de la secuencia del mensaje, y el tipo de mensaje (datos o control). La información de control añadida a los datos en un paquete (*trailer*) contiene un *checksum* para el bloque de enlace de datos y una bandera del fin de la trama. Los *headers* y los *trailers* son mostrados en la figura 1.4 (f).

Capa física.- La capa física no contribuye con nada a la estructura del mensaje. Esta simplemente acepta el mensaje de la capa de enlace de datos y traduce los bits en señales en el medio.

En nuestro ejemplo, el mensaje llega al nodo M y se filtra hasta el nivel de red. La capa de red reconoce que el mensaje está dirigido al nodo X y envía el mensaje hacia debajo de la capa de red para entregarlo al próximo nodo (final). Esto se muestra en la figura 1.3.

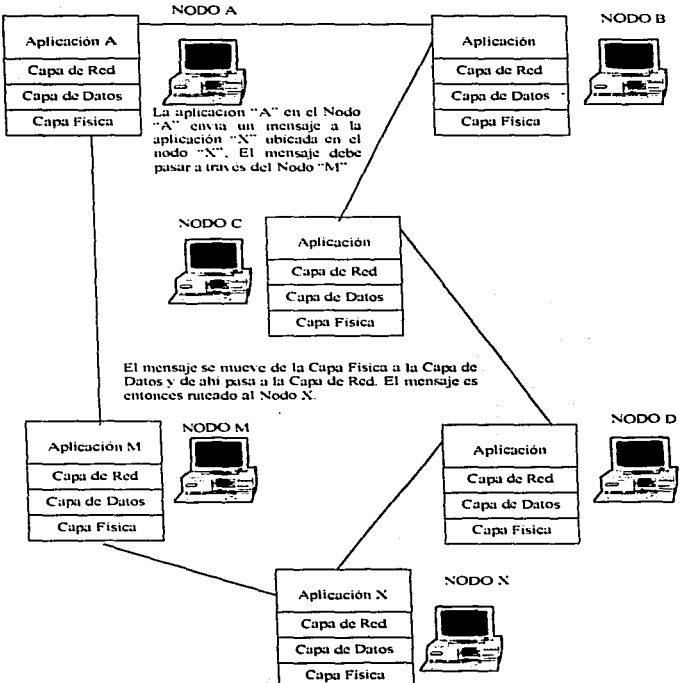


Fig. 1.3. Comunicación en una red a Nivel Aplicación- Aplicación

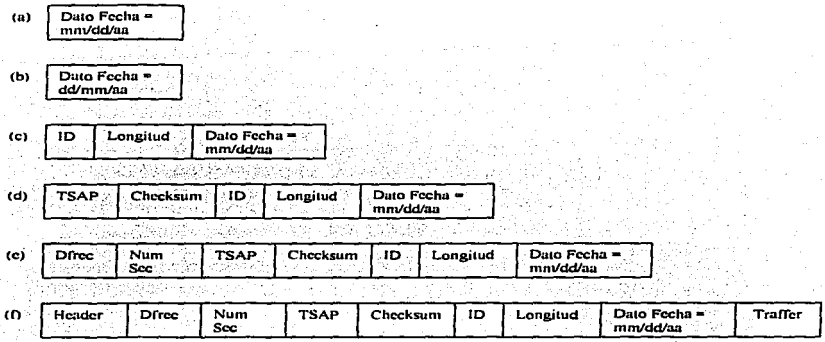


Fig. 1.4.. Formato de los mensajes del Modelo OSI

CAPÍTULO II. REDES.

Objetivo:

Mencionar las ventajas de la utilización de redes LAN, así como los beneficios que se obtienen con la interconexión con redes WAN.

CAPÍTULO 2. REDES.

2.1. ORIGEN DE LAS REDES.

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

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

En los 60´s con la aparición de las terminales se logra una comunicación directa, y por lo tanto más rápida, entre usuarios y computadora central, la desventaja era que entre más usuarios y periféricos se agregaran, decaía la velocidad de comunicación.

A fines de los 60´s y principios de los 70´s la compañía Corporación de Equipos Digitales (DEC *Digital Equipment Corporation*) introduce en el mercado dos elementos primordiales: la fabricación de equipos de menor tamaño y regular capacidad de almacenamiento, a los que se denominó minicomputadoras, y el establecimiento de

comunicación relativamente confiable entre ellos, por esa misma época se inicia en Estados Unidos el proyecto de la Agencia de Proyectos e Investigaciones Avanzados en Redes (ARPANET *Advanced Research Projects Agency Network*),que hizo pasar a primera línea el interés por encontrar soluciones que permitirán en condiciones técnicas y económicas viables, interconectar computadoras situadas a distancia.

En los inicios de la transmisión de datos se pusieron a disposición de los usuarios los circuitos permanentes o líneas telefónicas privadas entre puntos fijos, lo que permitió la transmisión de información en multitud de aplicaciones.

Conforme aumentó la exigencia de los usuarios, las diversas compañías telefónicas se vieron en la necesidad de arrendar también líneas privadas acondicionadas que permitirían la transmisión a mayor velocidad y confiabilidad.

Así a través de la evolución y proliferación de las redes de comunicación de datos aparecieron nuevos servicios como los canales privados compartidos, que trataban de satisfacer las necesidades de los usuarios a costos más reducidos. Nacieron también redes privadas con técnicas introducidas por la industria del procesamiento de datos y que perseguían los mismos propósitos anteriormente mencionados.

La proliferación de éstas redes tenían los inconvenientes de que los procedimientos utilizados en una red eran generalmente incompatibles

con los de otra, por lo que la interconexión de ambas redes tendía a ser imposible.

Para resolver éste grave problema el Comité Consultivo Internacional de Telegrafía y Telefonía (CCITT *Comité Consultatif Internacionale de Teléphonie et de Telegraphie*)1976 pudo elaborar una recomendación nueva, la X.25, la cual define la conexión entre una terminal y una pública de conmutación de paquetes.

Hacia la mitad de la década de los 70´s con el desarrollo de la tecnología del silicio y de la integración en miniatura de circuitos, permitió a los fabricantes de computadoras construir equipos con mayores capacidades. Estas máquinas llamadas microcomputadoras, descongestionaron a las máquinas centrales.

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

A esta época se le podría denominar la era del disco, el cual es un dispositivo de almacenamiento de datos. Sin embargo, de alguna manera se había retrocedido en la forma de procesar la información, porque nuevamente había que llevar la almacenada e los discos flexibles de una microcomputadora a otra y la poca capacidad de estos hacia difícil el manejo de grandes cantidades de datos. Sin embargo ésta explosión trajo

consigo algunos problemas inherentes al crecimiento, como los que a continuación se mencionan.

Problemas en compartir los programas: Cuando un usuario necesitaba la información que se encontraba en el disco duro de otra microcomputadora, la solución más común era tomar un disco flexible y copiar en él los archivos deseados. Sin embargo esto ocasionaba ciertos inconvenientes: el tiempo empleado en tomar los datos y copiarlos de una microcomputadora al disco flexible y posteriormente transferirlos a otro disco duro, o el tener la misma información ocupando espacio en varios equipos simultáneamente así como la dificultad de mantener todos esos archivos repetidos actualizados.

Problemas al compartir ciertos dispositivos: a medida que el número de proveedores de equipos periféricos aumentó, el precio de éstos fue disminuyendo lo cual hacia factible que de la misma manera en que se tenía un elevado número de microcomputadoras también se incrementaba el número de impresoras (una por microcomputadora), sin embargo si esas impresoras eran láser entonces el costo económico se eleva considerablemente. Esto justificaba el querer compartir los recursos más costosos.

Falta de estandarización de los programas y paquetes para computadoras (comúnmente llamado software): El contar con un gran número de microcomputadoras implicaba que el software empleado para realizar una misma tarea era normalmente numeroso, es decir, la posibilidad de que una empresa manejara cuatro o cinco procesadores de

texto era muy alta. Esto ocasionaba problemas para intercambiar archivos, mayor número de horas de entrenamiento e inversión en el software.

Poca seguridad: Inicialmente en las microcomputadoras el aspecto de alta seguridad no fue contemplado como algo prioritario, sin embargo conforme éstas han evolucionado, las aplicaciones y la información que en ellas se maneja es cada vez más confidencial y por lo tanto la importancia que tiene para las empresas es mayor.

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

Hacia 1983, la compañía Novell, In. (Compañía especializada en redes de computadoras), fue la primera en introducir el concepto de servidor de archivos (*File Server*) en el que todos los usuarios pueden tener acceso a la misma información, compartir archivos y contar con niveles de seguridad. En el concepto de servidor de archivos, un usuario no puede accesar indistintamente discos que se encuentren en otras microcomputadoras. El servidor de archivos es una microcomputadora designada como administrador de los recursos comunes. Al hacer esto, se logra una verdadera eficiencia en el uso de éstos, así como una total integridad de los datos. Los archivos y programas pueden acercarse en

modo multiusuario guardando el orden de actualización por el procedimiento, de bloqueo de registros. Es decir, cuando un usuario se encuentra actualizando un registro, se bloquea esté para evitar que otro usuario lo extraiga o intente actualizar.

Durante los años entre 1985 y la actualidad, las redes han luchado por colocarse como una tecnología reconocida contra todo tipo de adversidades. En un principio, la compañía IBM (*International Bussines Machine*), dedicada a la fabricación y venta de equipo de cómputo, no consideraba las redes basadas en microcomputadoras como equipo confiable. Había inclusive personas que llegaban a declarar que las microcomputadoras habían sido concebidas como islas de información en las que un usuario debería tener al alcance de su escritorio todos los elementos para construir un pequeño centro de cómputo autosuficiente.

No es sino hasta 1987, cuando IBM acepta ésta tecnología como el reto del futuro y acuña el término "conectividad", con lo cual se desata un crecimiento acelerado en la industria de las redes locales. Todos los fabricantes se lanzan a adaptar sus equipos y a proponer nuevas posibilidades en ésta área.

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

En la actualidad existe un gran interés en las redes locales. El reto importante para los desarrolladores de ésta tecnología es ofrecer productos confiables de alto rendimiento que hagan uso de la base instalada en el usuario final.

A éste último concepto se le denomina "tecnología de protocolo abierto". Es decir, ofrecer a los usuarios soluciones de conectividad que sean compatibles con los componentes físicos y electrónicos de un sistema de cómputo (generalmente denominado hardware) y el software ya adoptado por el usuario sin importar la marca, sistema operativo o protocolo de comunicación que se use. Novell, por ejemplo, ofrece desde hace algún tiempo el concepto de "conectividad universal" bajo *Netware*, según el cual es posible integrar sistemas operativos anteriormente incompatibles como: VMS, UNIX, DOS, MACINTOSH, los cuales se comunican por medio de una gran variedad de protocolos como son TCP/IPX, X.25, NETBIOS, etc.

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

2.2. COMPONENTES BÁSICOS DE UNA RED.

Una red de computadoras está compuesta tanto de hardware como de software, además los avances que se producen en estos aspectos

permiten trabajar conjuntamente con sistemas sin relación entre sí. Los componentes básicos necesarios en una red son los siguientes:

Servidor de archivos (*File Server*): El servidor de archivos, figura 2.1, es la computadora donde se reside el sistema operativo de la red, debe tener al menos un disco duro ya sea interno o externo, 4 MB de RAM para aplicaciones básicas y pocos usuarios (en promedio 5 a 10), 16 a 32 MB para aplicaciones complejas y un mayor número de usuarios y 64 a 128 MB más para aplicaciones complejas, empleo de gráficos, gran número de usuarios y varias redes, así también debe contener al menos una tarjeta de red.

Un servidor de archivos puede contener programas y datos que todos los usuarios de la red puedan compartir. Puede funcionar en diferentes modalidades, si se usa como estación de trabajo es un servidor no dedicado. Si no puede usarse como estación de trabajo se denomina servidor dedicado.

Fig. 2.1. Servidor de Archivos

Estación de trabajo (*Work Station*): Son todas aquellas microcomputadoras, figura 2.2, mediante las cuales se accesa a la información localizada en el servidor de archivos y que ayudan al

procesamiento de la misma, se encuentra interconectada por medio de una tarjeta de interfaz (límite compartido, definido por características físicas de interconexión en común).

En la red tanto servidores como estaciones de trabajo pueden ser PS´s AT, PC´s, RISC´s., equipo 386 o 486 con características especiales y diseñadas para cada aplicación.

Figura 2.2.

Tarjeta de interfaz de red (NIC *Network Interface CardK):* Cada nodo de la red, llámese estación de trabajo o servidor de archivos debe contar al menos con una tarjeta de red, la cual estará en función del tipo de red que se esté empleando. Existen tres tipos de tarjetas que dominan el mercado internacional: Arcnet, Ethernet y Token-Ring. En la mayoría de los casos, la tarjeta se adapta la ranura de expansión de la computadora.

La tarjeta de interfaz obtiene información de la computadora personal (PC P*ersonal Computer*), la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información para que la PC la pueda entender y la envía la PC.

Sistema de cableado: El cableado, el cual es la columna vertebral de cualquier sistema de red, ya que conecta todas las tarjetas de interfaz. Este proporciona el enlace de comunicación entre todas las computadoras del sistema (servidores de trabajo) y periféricos. Existe una gran variedad de tipos de cables, entre los más utilizados podemos mencionar el cable coaxial, el par trenzado y la fibra óptica.

El cable coaxial, se conforma por un alambre conductor básico cubierto por una capa metálica que actúa como tierra. El alambre conductor y la tierra se encuentran separados por un aislante plástico y, finalmente todo el conjunto está protegido por una cubierta exterior también aislante.

Su principal característica es que puede transformar una señal eléctrica a mayor distancia mientras más grueso sea el conductor, los tipos más comunes de cables coaxiales empleados en las redes son:

Cable coaxial grueso RG-8 y RG-11 usados en Ethernet (50 Ohms), 0.4 pulgadas de diámetro, permite manejar señales de hasta 500 mts. Sin presentar ningún tipo de atenuación que produzca errores en la comunicación.

Cable coaxial delgado RG-58 utilizado en Ethernet (50 Ohms), 0.2 pulgadas de diámetro y permite transportar una señal hasta 300 mts. sin el uso de repetidores.

Ventajas:

- Soporta anchos de banda mayores que el cable de par trenzado (arriba de 10 Mbps). Resiste la interferencia electromagnética mejor que el cable par trenzado.
- Transmisión de voz, y datos.
- Fácil instalación.

El cable telefónico se forma principalmente por dos alambres de cobre que se encuentran aislados por una cubierta plástica y torcidos una contra el otro, es por esta característica que se le conoce como cable de par trenzado (*twisted pair*). El par trenzado a su vez se encuentra envuelto por una cubierta aislante y protectora en la capa exterior.

Los cables con los conductores de cobre más delgados y menos protegidos están dentro de la clasificación de cables tipo par trenzado sin blindar (UTP *Unshielded Twisted Pair*). Son sumamente baratos y permiten manipular una señal a una distancia máxima de 110 mts. sin el uso de amplificadores.

Los cables de conductores más gruesos y bien protegidos por una cubierta aislante son denominados cable par trenzado blindado (STP *Shieldes Twiested Pair*). Estos últimos son más caros y menos flexibles que los UTP, pero permiten un rango de hasta 500 mts.

Ventajas:

- Tecnología ampliamente empleada.
- Facilidad y rapidez de instalación.
- Compatibilidad con Ethernet y Token –Ring.
- Relativamente barato.

El cable de fibra óptica, se compone de una fibra muy delgada elaborada de dos tipos de vidrio con diferentes índices de refracción, uno para la parte interior y otro para la parte exterior. Esta diferencia en la refracción evita que la luz penetre en una parte de la fibra óptica hasta la parte exterior evitando así la pérdida de la información. La fibra a su vez se encuentra cubierta por una cubierta aislante y protectora en la parte más exterior para darle mayor fuerza al cable. Es extremadamente flexible ya que se pueden realizar giros de hasta 360 grados sin afectar el cable.

El diámetro de la fibra interior es generalmente de 62.5 micras y el diámetro exterior de 125 micras. Para la transmisión de información en redes se utiliza una fibra como transmisor y otra como receptor. Las distancias máximas obtenidas para redes locales son de 2000 mts. de nodo a nodo sin el uso de amplificadores.

Ventajas:

- Transmisión de voz, vídeo y datos por el mismo canal.
- No genera señales eléctricas o magnéticas.

- Inmune a interferencias y relámpagos.
- Es compatible con Ethernet, Token-Ring e Interfaz de Datos Distribuidos por Fibra (FDDI *Fiber Data Distribuited Interface*).

Sistema operativo de red: Adicionalmente al sistema operativo normal de los equipos (regularmente MS-DOS, OS, UNIX), es necesario que se cuente con un sistema operativo para red, que lo auxilie o sustituya en el trabajo de compartir recursos (archivos, periféricos, usuarios, etc.) y lleva el control y seguridad de estos.

El sistema operativo de la red se engloba en dos componentes básicos. El sistema operativo de red de servidor, se ejecuta dentro de la misma máquina y procesa todos los servicios. La parte residente del sistema en la estación de trabajo se ejecuta en ésta, establece la conexión con la red y el servidor y controla el flujo de las comunicaciones.

Software de aplicación: Este puede ser tan diverso, como las necesidades de la empresa o usuario lo requieran, y puede incluir desde procesadores de texto, sistemas administrativos, paquetes integrados, sistemas de contabilidad, sistemas especializados (por ejemplo: control de producción, correos electrónicos, etc.) sin embargo, al momento de elegirlo, se debe considerar el que mejor se adapte a las características de la red. Hay software que necesita una red rápida para funcionar eficientemente. Existe otro que requiere mucho espacio de almacenamiento. Otro más, tiene límite de usuarios.

Puentes (Bridges): Proporcionar un servicio de conexión más inteligente. Tienen una función específica que es interconectar segmentos de red. Mantienen una sola red lógica aunque exista separación física.

Ruteadores (Routers): Al igual que los puentes aumentar el tamaño de una red, pueden tomar decisiones de enrutamiento que determinen la trayectoria de datos entre dos segmentos de red, o entre redes lógicamente distintas. El ruteador, tiene la inteligencia para decidir el enrutamiento de datos dinámicamente mientras éstos circulan por la red.

Gateway: Ofrecen el servidor de conexión más inteligente pero también más lento. Hace traducciones de diferentes protocolos de computadoras y también permiten que los dispositivos de una red LAN se comuniquen con los dos de otro ambiente de red diferente. Típicamente se usan para adaptar redes a aplicativas IBM Arquitectura de Sistemas de Red (SNA *System Network Architecture*).

2.3. ORGANISMOS DE NORMALIZACIÓN.

Para crear una red, todos los elementos que la componen (el equipo, la topología, los enlaces de comunicación, el protocolo, etc.) han de formar un sistema compacto y unitario. Los distintos elementos del sistema pueden variar bastante entre si, pero no hay ningún componente del sistema que se pueda seleccionar o diseñar aisladamente.

Las partes del sistema han de estar compensadas en su totalidad para que pueda tener lugar la comunicación. Si un solo componente del sistema no se comunica correctamente con el resto, la comunicación no puede ser eficaz.

El número de posibles combinaciones para formar una red es casi infinito. Debido a que los equipos y las tecnologías cambian rápidamente, es necesario disponer de algún sistema para coordinar todos los elementos. En el campo de las comunicaciones hay una fuerte tradición de eficacia y autoridad en los organismos de normalización. El tema de las redes se haya inmerso en el de las arquitecturas telemáticas jerarquizadas, aunque presenta particularidades específicas. A continuación haremos mención de los distintos organismos competentes en esta materia.

2.3.1. ISO.

Es una de las organizaciones de estándares más importantes del mundo, fue fundada en 1946 y hoy en día incluye a más de 2000 comités, subcomités técnicos y grupos de trabajo envueltos en un gran campo de actividades. Entre sus miembros se incluyen asociaciones de estándares de más de 90 países.

2.3.2. CCITT.

Este es un organismo de gran influencia en el entorno de las comunicaciones. Sus recomendaciones para la conexión y el cableado de interfaces (V.24, X.21, etc.) son de aplicación común. Además de la recomendación X.25 para la normalización de redes de conmutación de paquetes, cabe resaltar su aceptación del modelo de referencia OSI bajo la denominación X.200 y sus recomendaciones para el nivel de aplicación (X.400 y X.500). En lo que concierne a redes locales, sus normas afectan a todo lo relativo para su conexión con los servicios ofrecidos con las redes públicas de área extendida.

2.3.3. IEEE.

Este organismo ha tenido una especial participación en el tema de las redes locales. Las recomendaciones de la serie 802.6 son una norma estable para los niveles inferiores de las redes locales y han sido adaptadas por ANSI (Instituto Nacional Americano de Estándares) con la misma denominación y por ISO bajo la deniminaciñon 802.2.

2.4. REDES LAN.

A través de los años, millones de redes Ethernet y Token-Ring han sido instaladas. Las Redes de Area Local (LAN´s *Local Area Network*) son un conjunto de dispositivos interconectados (computadoras, terminales e

impresoras) dentro de una misma habitación, edificio, complejo u otra área geográfica limitada.

En términos simples, una LAN es un medio de distribución de recursos – espacio, ancho de banda, o tiempo – para las personas o los equipos que estén utilizados dichos recursos para comunicarse. Las LAN´s facilitan el intercambio de información entre usuarios, sin considerar el tipo de equipo, protocolos, o medios de transmisión.

Además existen estándares en los cuales se basan los diferentes proveedores de equipos y materiales de comunicaciones, dicho estándares son definidos por el IEEE, de estos, la serie IEEE 802 define las características de los tipos de LAN existentes (ejemplo: Ethernet, Token-Ring).

2.4.1. TOPOLOGÍAS.

Las topologías pueden ser descritas física y lógicamente. Una topología física es la apariencia actual o distribución de la red. La topología lógica describe el flujo de datos a través de una red. Existen muchas topologías de redes, algunas de las más populares son:

- Malla
- Estrella
- Bus
- Anillo
- Híbrida

Las primeras redes a menudo consistían de enlaces "punto a punto" o "multipunto". Estas permanecen como los elementos fundamentales de las arquitecturas de comunicación actuales.

Un enlace "punto a punto" es una conexión directa entre dos dispositivos (nodos). Un ejemplo es la conexión de una computadora personal a una impresora directa. Una ejemplo común fue un enlace entre una terminal y un mainframe. Otro ejemplo es el enlace entre dos antenas de microondas.

Un enlace "multipunto" es la conexión entre tres o más dispositivos en un mismo enlace. Los enlaces "multipunto" fueron muy usados para conectar un sitio central con una serie de nodos, como cuando múltiples terminales estaban conectadas a un procesador frontal (FEP *Front End Processor*) de comunicaciones. En el actual ambiente de las LAN´s enlaces "multipunto" conectan multiples dispositivos en topologías de bus o de árbol.

Los enlaces "punto a punto" difieren de los "multipunto" en que los primeros implican ancho de banda dedicado, por lo tanto no se requiere direccionamiento. Con "multipunto" el canal es compartido.

2.4.1.1. MALLA.

Una red de malla tiene conexiones punto a punto entre cada nodo de la red, sin embargo usualmente no son consideradas prácticas, ya que

uno de los problemas que presentan es que se requiere múltiples enlaces en cada dispositivo para proporcionarle a la red enlaces redundantes, otro problema es que la cantidad de cable para una red grande (en términos del número de nodos conectados) es muy elevada. Finalmente, a menos que cada estación envíe frecuentemente información a las otras estaciones, una excesiva cantidad de ancho de banda de la red es desperdiciada.

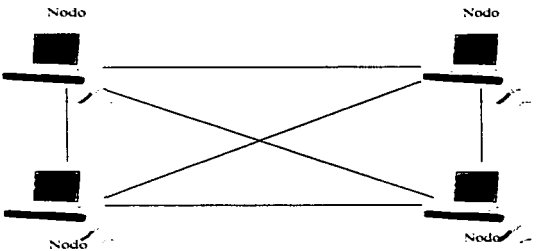


Fig. 2.3. Topología de Malla.

2.4.1.2. ESTRELLA.

Una red estrella, es aquella en donde cada dispositivo está conectado vía un enlace "punto a punto" a un punto central. Esos puntos centrales son comúnmente llamados repetidores multipuerto o concentradores o (hub´s), figura 2.4. ese punto central puede ser "pasivo", "activo" o "inteligente". Un hub pasivo simplemente conecta los brazos de la estrella. Todo el tráfico se obtiene de los otros nodos, no

se realiza ninguna regeneración de señal, por lo tanto esos dispositivos no son repetidores. Cada nodo debe separar los datos que sean para otros nodos. Un hub activo a diferencia de un pasivo es que sí regenera la señal. Los hubs activos son por lo tanto participantes activos en el enlace de protocolo. Los llamados "hubs inteligentes" además de regenerar la señal, ejecutan actividades como selección de trayectoria inteligente (como activar el enlace de desvío en él caso de que el enlace primario falle) y manejo de red.

Dado que toda la información en una red estrella va a un punto central la detección de problemas es relativamente sencilla. Las estrellas pueden también ser organizadas jerárquicamente, proporcionando flexibilidad arquitectural y aislando el flujo de tráfico.

Dependiendo la localización de los hubs, la cantidad de cableado puede ser màyor que en otras topologías.

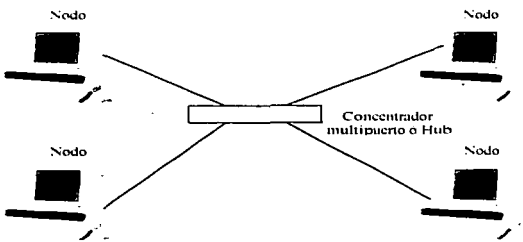


Fig. 2.4. Topología de Estrella.

2.4.1.3. LINEAL O DE BUS.

Una topología de bus es un medio de transmisión lineal al cual todos los nodos se conectan directamente. El bus utiliza una cantidad mínima de cable puesto que el medio esencialmente dirigido a cada nodo. El bus no tiene puntos de distribución central, lo cual dificulta la detección de problemas. Las redes Token Bus y Ethernet utilizan topología de bus.

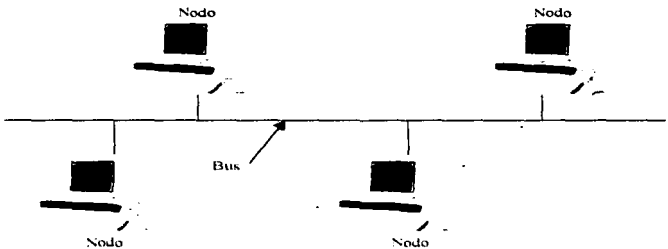


Fig. 2.5. Topología de Bus.

2.4.1.4. ANILLO.

Una topología de anillo, figura 2.6, es aquella que lógicamente forma un bucle cerrado ó anillo, en la cual todos los nodos de la red se conectan punto a punto. Los mensajes se mueven en un dirección a través de la red. Cuando un mensaje llega a un nodo, éste examina la

dirección contenida en este. Si la dirección coincide con la dirección del nodo, el mensaje es aceptado; de otro modo el nodo regenera la señal y regresa el mensaje a la red para que lo tome el próximo nodo en el sistema.

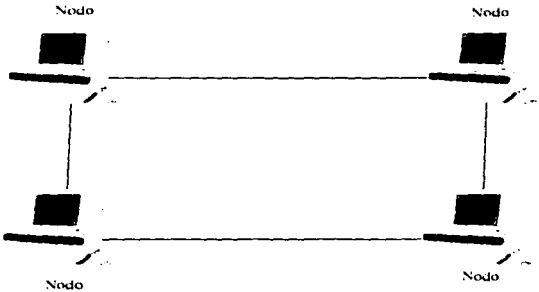


Fig. 2.6. Topología de Anillo.

2.4.1.5. HÍBRIDA.

Las redes híbridas son una mezcla de topologías, figuras 3.6. la topología híbrida ha incrementado su popularidad tanto en empresas como en redes globales que están formadas por la conexión de LAN´s y MAN´s (Redes de Area Metropolitana). Algunos de los ejemplos más importantes son:

- Internet, Usenet, NSFnet y muchas otras redes privadas.

2.4.2. MÉTODOS DE ACCESO AL CANAL.

En un canal punto a punto el transmisor tiene la libertad de transmitir en cualquier momento, sin embargo por lo general son varios los dispositivos conectados en un solo canal generando lo que conocemos como una conexión multipunto. Esta situación ocasionó la aparición de algunos métodos que permitieran a cada uno de los dispositivos transmitir sin que sus mensajes interfieran con los de otros. Los métodos de acceso al canal describen las reglas que rigen la forma en que los equipos conectados al medio lo van a accesar, transmitir y liberarlo. Los métodos de acceso más populares son los siguientes.

- Contensión.
- Token –Passing.

Cada canal posee una velocidad máxima de datos, pero cuando dos o más dispositivos pueden transmitir en el mismo canal, el ancho de banda teórico debe necesariamente ser limitado por el *overhead* del control de acceso al canal. Los diferentes métodos de acceso tienen a su vez diversos efectos de *overhead* en el tráfico de la red.

2.4.2.1. CONTENCIÓN

Con los sistemas de contención las estaciones de trabajo pueden transmitir cada que lo deseen, no hay nadie que "ordene" cuando un equipo pueden o no usar el canal. Este esquema es simple de diseñar y

proporciona igual derecho de acceso a todas las estaciones, las cuales simplemente transmiten cuando están listas para hacerlo sin importar que otras puedan estar enviando información.

Desafortunadamente la estrategia de "transmitir" siempre que esté listo "tiene un importante defecto, el cual surge cuando varias estaciones tratan de transmitir simultáneamente. Cuando esto ocurre, el resultado de la mezcla de señales generalmente ocasiona que la información se pierda. Este evento es conocido como una colisión.

Protocolos de contensión más recientes fueron desarrollados de tal forma que las estaciones "escucharan" el canal antes de transmitir. Si la estación que "está escuchando" detecta una señal se abstiene de transmitir en ese momento y lo intenta posteriormente. Esos protocolos son llamados de Acceso Múltiple con Detección de Portadora (CSMA *Carrier Sense Multiple Access*). La introducción de estos métodos redujo las colisiones, sin embargo continuaba el problema cuando dos estaciones censaban el cable y al no detectar nada transmitían simultáneamente.

Con los protocolos CSMA, la detección de colisiones y la subsecuente retransmisión es iniciada por una capa arriba de la capa de enlace de datos. Cuando la capa superior no recibe una respuesta a su mensaje inicia la retransmisión. Este periodo de espera para recibir la respuesta redujo la efectividad de los protocolos CSMA.

Ejemplos de estos son Acceso Múltiple con Detección de Portadora/Detección de Colisiones (CSMA/CD *Carrier Sense, Multiple*

Access/Collision Detection) y Acceso Múltiple con Detección de Portadora/Prevención de Colisiones (CSMA/CA *Carrier Sense, Multiple Access/Collision Avoidance*). Los protocolos CSMA/CD no sólo sensan el cable antes de transmitir, además detectan colisiones (e inician retransmisiones) en o arriba de la capa de enlace de datos. Si la línea esta libre, la estación transmisora envía su mensaje en ambas direcciones por toda la red. Cada mensaje incluye una identificación del nodo transmisor hacia el receptor y solamente el nodo receptor puede leer el mensaje completo.

Cuando dos estaciones transmiten sus mensajes simultáneamente una colisión ocurre y es necesaria una transmisión debido a que los paquetes de datos colisionados se corrompen. Si una colisión es detectada durante la transmisión la estación detiene el envío de sus datos y comienza a transmitir una secuencia de bits la cual se conoce como patrón de choque (*jam pattern*), él cual consiste de una cadena de 32 a 48 bits para cualquier patrón excepto el valor CRC de 32 bits correspondiente a la trama parcial transmitido antes del patrón de choque. El patrón de choque garantiza que la colisión sea lo suficientemente larga para ser detectada por todos los nodos de la red que están transmitiendo y la refuerza transmitiendo un mensaje de indicación de colisión. La estación detecta la colisión y espera un tiempo aleatorio antes de intentar transmitir nuevamente.

Las ventajas de emplear métodos de contención son las siguientes:

- El control del software es relativamente simple y ocasiona poco tráfico excesivo de tal forma que con bajos niveles de tráfico de datos la cantidad total de datos generados o transmitidos durante un cierto lapso de tiempo (*throughput*) es bastante alto. Sin embargo al incrementarse el tráfico, el tiempo de acceso al canal se eleva de una forma no lineal, con frecuencia obteniéndose niveles inaceptables son valores de transferencia real de datos por debajo de la capacidad actual del canal.

Las desventajas de la contención son las siguientes:

- Los tiempos de acceso al canal no son predecibles excepto de modo estadístico.

- Las prioridades no pueden ser usadas para darle acceso más rápido a ciertos dispositivos.

2.4.2.2. TOKEN-PASSING

En sistemas *token-passing,* una pequeña trama (llamada estafeta o *token*) es pasada de una manera ordenada de un dispositivo a otro. El *token* es un mensaje de autorización especial que temporalmente da el control del canal al dispositivo que en un momento dado lo posee. Pasar el *token* por todas las estaciones distribuye el control del acceso entre los dispositivos del canal.

Cada dispositivo conoce de qué estación proviene el *token* que está recibiendo y a que dispositivo lo va a pasar posteriormente. Cada dispositivo toma el control del *token*, ejecuta sus labores y entonces lo retransmite para que otro dispositivo lo pueda emplear. Las reglas del sistema limitan cuanto tiempo cada estación puede controlar el *token* y solo puede circular uno a la vez en el anillo.

Existen diferentes estándares de protocolos *token-passing*, dos de los más empleados en ambientes LAN son IEEE 802.5 *token-bus*. La diferencia entre ambas redes consiste en que mientras la segunda utiliza topología de bus, *token- ring* hace uso de la topología de anillo. Otro estándar *token.passing* (para LAN´s de fibra óptica) es llamado Interfaz de Datos Distribuidos por Fibra (FDDI *Fiber Distributed Data Interface*).

Cuando una estación recibe un *token*, ésta puede transmitir una trama (*frame*) a la próxima estación. Después de que la trama transmitida viaja a través del anillo y regresa a la estación transmisora, éste es retirado del anillo. Para verificar errores, la estación transmisora compara la trama que recibe con la que transmitió. Tan pronto como la estación transmisora terminó de recibir su trama ésta genera un nuevo *token* y lo transmite a la próxima estación. Si el anillo soporta liberación temprana de *token (early token release)*, uno nuevo puede ser liberado después que el transmisor termina de enviar el último bit de la trama.

Una estación del anillo actúa como monitor activo. Este dispositivo proporciona un tiempo de sincronización para los dispositivos del anillo, remueve tramas que circulan continuamente y realiza otras funciones de

mantenimiento. Todas las estaciones tienen el potencial para ser monitores activos. Cuando no hay monitor activo presente rápidamente y mediante procedimientos automáticos se obliga a una estación convertirse en monitor activo.

Las ventajas de *token-passing* son las siguientes:

- Este método es llamado determinístico y se considera adecuado para canales que controlan algún tipo de equipo automatizado.

- Algunos sistemas ofrecen flexibilidad y una variedad de opciones incluyendo prioridad. Las reglas de acceso al canal pueden ser fijadas inicialmente o en algunos casos permitir cambios durante la operación para mejorar la operación para mejorar el manejo de condiciones variables. La flexibilidad puede mejorar el uso del ancho de banda del canal e incrementar el *throughput*. Se pueden asignar prioridades para asegurar que ciertos dispositivos tengan un acceso más rápido.

- La carga de tráfico ofrecida por los dispositivos al canal es incrementada, el *throughput* del canal también se eleva hasta llegar a cierto nivel. Un incremento adicional en el tráfico ofrecido más allá de éste nivel no incrementa no decrece el *throughput*. *Token-passing* a menudo ofrece el *throughput* más alto para redes bajo condiciones de carga elevada.

Las desventajas de *token-passing* son las siguientes:

- *Token-passing* requiere de software relativamente complicado en todos las estaciones de trabajo, las cuales además necesitan ser razonablemente inteligentes. Los parámetros de software de cada dispositivo necesitan ser ajustados cada que un nuevo equipo se suma o abandona el canal. Un monitoreo interno y la compartición de responsabilidades, incluyendo detección y recuperación de fallas se requiere en todos los equipos. Algunas redes requieren un control central adicional. Estas complicaciones crean tráfico excesivo y reducen un poco la taza de *throughput*.

Las ventajas, desventajas y la comparación del rendimiento (*performance*) de los sistemas *token-passing* y contensión son tópicos que aún generan discusión en el ambiente de las LAN´s. Se debe hacer hincapié en que ninguna es intrínsecamente superior a la otra desde el punto de vista del rendimiento. Sin embargo bajo condiciones específicas uno u otro pueden mostrar un rendimiento superior.

En general, cuando la carga del canal es alta, el método de acceso *token-passing* proporciona un *throughput* más alto a la red, y el método de contensión tiene un rendimiento mucho menor. Por otro lado, debido a su limitado tráfico excesivo el método de contensión puede superar a *token-passing* en condiciones de carga ligera.

2.4.3. ESTÁNDARES.

En 1980, el Instituto de Ingenieros Eléctricos y Electrónicos (mejor conocido como IEEE) realizó la tarea de definir los estándares LAN. Ellos buscan asegurar un bajo costo, interoperabilidad de interfaces de red para LAN, etc.

Después de iniciado el trabajo, el IEEE determino que ninguno de los estándares satisfacía todas las partes, por lo que decidieron que deberían producir varios. Finalmente en 1985 el IEEE publicó cuatro estándares separados para el proyecto 802. El IEEE 802.2 provee enlace lógico, el IEEE 802.3 define una red CSMA/CD, el 802.4 define una red de bus usando el acceso de *token-passing*, el IEEE 802.5 define una red de anillo utilizando el acceso de *token-passing*.

2.4.3.1. ETHERNET Y IEEE 802.3

Ethernet fue inventada a mediados de los setenta por la compañía Xerox. La especificación para la versión 1.0 fue desarrollada conjuntamente por Digital Equipment Corporation, Intel Corporation y Xerox en 1980. Ethernet versión 2.0 (desarrollada por las mismas compañías) apareció cerca de dos años después. Aproximadamente a los tres años la IEEE liberó sus especificaciones iniciales para 802.3.

Tanto Ethernet como el estándar IEEE 802.3 utilizan el método de acceso CSMA/CD. El estándar IEEE 802.3 ofrece una variedad de

opciones en la capa física del modelo OSI, incluyendo diferentes modos de señalización en banda base y banda ancha (*baseband y broadband*), tipos de medios, topologías y velocidades de transmisión. Esto lo podemos observar en la tabla 2.1.

		Estándares			
Parámetros	Ethernet	IEEE 10 BASES	10 BASE2	1BASE5	10BASET
Velocidad	10	10	10	1	10
Tipo de Señal	Banda Base Manchester	Banda Base Manchester	Banda Base Manchester	Banda Base Manchester	Banda Base Manchester
Segmento Máximo Long.-mts.	500	500	185	250	100 (UTP)
Medio	50-OHM Coaxial (grueso)	50-OHM Coaxial (grueso)	50-OHM Coaxial (delgado)	Par trenzado no blindado	Par trenzado no blindado
Topología	Bus	Bus	Bus	Estrella	Estrella

Tabla 2.1. Tabla de Especificaciones para Ethernet y 802.3

Las siguientes subsecciones explican las diferencias entre los estándares físicos del 802.3. Los estándares han recibido sus nombres generalmente de la siguiente forma:

10 BASE 5

10 . Velocidad en Mbps

BASE Banda base ó Banda ancha

5 Longitud del segmento en múltiplos de 100 mts

10 BASE5: El estándar 10 BASE5 se asemeja estrechamente a Ethernet. Además de las diferencias universales entre Ethernet y todas las especificaciones de IEEE 802.3, la principal diferencia entre ambas es la terminología.

La estación IEEE 802/10BASE 5 se conecta a un medio físico una Unidad de Acceso al Medio (MAU). Este dispositivo es llamado transmisor-receptor (*transceiver*) en la especificación de Ethernet, pero ambos son funcionalmente lo mismo. Los dispositivos de IEEE incluyen componentes digitales para señalización y circuitería análoga para la detección de colisiones. Ellos detectan las colisiones, transmiten y reciben señales en el medio. El cable de la interfaz es llamado cable del transceiver en la documentación de Ethernet y unidad de interfaz de acceso (AUI) en la documentación de IEEE 802.3.

El cable coaxial para IEEE 802/10 BASE5 es moderadamente susceptible a la interferencia electromagnética (EMI) y al ruido eléctrico. Esto permite una velocidad máxima de transmisión de 10 Mbps sobre un segmento con una longitud máxima de 500 metros.

10 BASE2: Esta red es llamada *thinnet*, por *thin* (delgado), y utiliza cable coaxial RG-58. Este cable puede llevar una señal por aproximadamente 185 metros. Más halla de eso, la señal debe ser regenerada por un repetidor.

La razón por lo que esta red es llamada 10BASE2 por IEEE es porque transmite a 10 Mbps sobre un alambre banda base y puede portar

una señal aproximadamente de 2x100 mts. (la real es de 185 mts.). Una red *thinnet* fue diseñada para ser una opción económica para soportar un pequeño departamento o grupo de trabajo.

10 BASET: 10BASET es una LAN Ethernet de banda base que utiliza cable par trenzado sin blindaje (UTP) para conectar las estaciones de trabajo. Muchas redes de este tipo configuradas en un patrón estrella, pero internamente usan un sistema de bus de señalización parecido a otras configuraciones Ethernet.

Típicamente, el *hub* o concentrador de una red 10BASET sirve como un repetidor y a menudo se localiza en un closet de la instalación. Cada estación de trabajo ó servidor está localizado en el punto final de un cable conectado al *hub*. Cada computadora tiene dos pares de cables, un par es utilizado para recibir datos y otro par para enviar los datos. La longitud del cable desde el repetidor a la computadora puede ser de 100 mts. La longitud mínima entre computadoras es de 2.5 mts.

1BASE5: El estándar 1BASE5 (a menudo llamado StarLAN) utiliza el cable UTP en topología estrella con todas las estaciones conectadas a un *hub* de un modo punto a punto. El *hub* repite las señales y detecta las colisiones. La distancia máxima desde una estación es de 250 mts. hasta 5 *hubs* pueden estar en cascada en un modo jerárquico, rindiendo al máximo en un espacio de 250 mts. El *hub* del nivel superior es llamado el *"hub de cabecera"*, los otros son *hubs* intermedios. Las colisiones son reportadas al primero a través de los restantes. Entonces el *hub* de

cabecera emite mensajes de la colisión descendentemente al resto de los *hubs*.

2.4.3.2. ESTRUCTURA DE LAS TRAMAS IEEE 802.3 Y ETHERNET

PREAMBULO	DELIMITADOR DE COMIENZO DEL FRAME	DIRECCION DESTINO	DIRECCION FUENTE	LONGITUD	HEADER 802.2 Y DATOS	CRC
7 BYTES	1 BYTES	6 BYTES	6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

PREAMBULO	DIRECCION DESTINO	DIRECCION FUENTE	TIPO DE SERVICIO	DATOS	CRC
8 BYTES	6 BYTES	6 BYTES	2 BYTES	46-1500 BYTES	4 BYTES

Tabla 2.2. Estructura de las Tramas de IEEE 802.3 y Ethernet

Preámbulo y Delimitador de Inicio de Trama (SFD Start of Delimiter):Para comenzar una trama, el MAU *transceiver* transmite un preámbulo de siete bytes de 1 y 0 alternados. El siguiente byte corresponde al delimitador de Inicio de Trama que es como el preámbulo, sólo que éste termina en dos bits 1 consecutivos. Estos bits anuncian la llegada de la trama y sincronizan a todos los receptores en la LAN.

Dirección destino: típicamente consiste de 2 a 6 bytes (pueden ser únicamente dos), y especifica quién o quienes van a recibir la trama. La dirección destino puede especificar solo un nodo, múltiples nodos o todos los nodos de la red. Esas direcciones son conocidas como "*unicast*" "*multicast*" o "*broadcast*" respectivamente.

Dirección fuente: La dirección fuente de la trama se encuentra a continuación de la dirección destino, y su longitud también es de seis bytes. Para obtener direcciones únicas en todo el mundo, la IEEE se ha responsabilizado de asignar los primeros tres bytes a cada vendedor de hardware para incorporarlas dentro de cada tarjeta de red. El vendedor generalmente asigna los últimos tres bytes de cada una de sus tarjetas.

Longitud de los datos: El campo de longitud consiste de dos bytes e indica el número de bytes de datos que se encuentran antes del campo de secuencia de chequeo de la trama (FCS *Frame Check Sequence*). Este número indica cuantos bytes de datos hay en la trama, no incluye los bytes de relleno que pueden preceder al FCS.

Datos y relleno (pad): el campo de datos contiene los datos de la trama. El número de esos bytes citados en el campo de longitud constituyen el paquete IEEE 802.2 LLC. El "relleno" incluye cualesquiera otros bytes antes del FCS, de acuerdo a lo que se indica a continuación.

IEEE 802.3 tiene algoritmos que detectan tramas defectuosos y colisiones. Esos algoritmos requieren que cada trama sea lo suficientemente larga para que el principio de éste se propague a través de la LAN y la señal de detección de colisiones sea transmitida de regreso antes que el transmisor termine de enviar su trama. El tamaño mínimo de un paquete IEEE 802.3 es de 64 bytes. Cuando los datos a transmitir son muy pocos, el transmisor "rellena" el campo de datos. El receptor elimina cualquier trama menor a 64 bytes.

Chequeo de secuencia de la trama: El transmisor realiza un chequeo cíclico redundante (CRC) con los valores de los campos de dirección fuente y destino, longitud, datos y "relleno". El valor resultante del CRC es colocado en el campo de 4 bytes del FCS. Una vez recibida la trama, el receptor computa el CRC y lo compara con el valor localizado en el campo FCS. El receptor descarta cualquier trama cuyo CRC no coincida con el valor por él calculado.

IEEE 802.3 especifica solo la primer mitad de la capa de enlace de datos del modelo OSI, mientras que Ethernet especifica la capa completa. Generalmente IEEE 802.3 se basa en IEEE 802.2 para especificar la porción superior del nivel de enlace de datos. La siguiente tabla compara Ethernet contra la combinación de IEEE 802.2/IEEE 802.3.

Características	Ethernet	IEEE 802.2/IEEE 802.3
Medio	Cable coaxial 50-OHM	Fibra óptica Par trenzado Cable coaxial 50-OHM Cable coaxial 75-OHM
Topologías	Bus	Estrella y Bus
Velocidad	10 Mbps	Variable (1 – 10 Mbps)
Campo de 2 bytes después de la dirección fuente	Tipo	Longitud

Tabla 2.3. Tabla comparativa de Ethernet contra IEEE 802.2/802.3.

Como se muestra en la tabla 2.3 el IEEE 802.2/IEEE 802.3 soporta una mayor variedad de medios, topologías, velocidades y servicio de

enlace de datos, en tanto que Ethernet soporta un solo medio, una topología, una velocidad y un servicio de enlace de datos.

Ethernet e IEEE 802.3 emplean el campo de 2 bytes que sigue a continuación del campo de dirección fuente de diferente manera. Ethernet usa ese campo (tipo de servicio) para indicar el tipo de protocolo de nivel superior que atenderá el paquete contenido dentro del campo de datos de la trama. IEEE 802.3 por su parte espera recibir en este campo la longitud del campo de datos para ser codificado aquí y normalmente se basa en IEEE 802.2 para las especificaciones de los protocolos de orden superior. Generalmente los valores de la IEEE y el campo "tipo de servicio" no se confunden, así que las estaciones pueden fácilmente examinar el valor de dicho campo para determinar si el paquete representa a IEEE 802.3 o a Ethernet.

2.5. REDES WAN.

El nombre genérico dado a las redes que enlazan computadoras y usuarios que están físicamente localizados a través de grandes distancias, algunas veces cruzando fronteras geográficas de ciudades, estados o países es redes de área amplia (WAN *Wide Area Network*).

En sentido estricto, una red de área amplia es una red de redes, en la que se conectan varias redes locales mediante dispositivos que permiten su conectividad local o remotamente, a pesar de que tengan

diferente topología. Estos dispositivos pueden usar o no líneas telefónicas o servicios públicos de transmisión de datos.

2.5.1. RED PÚBLICA DE DATOS.

Los estándares pertenecientes a las WAN´s son aquellos que principalmente han sido desarrollados para ser utilizados por la red pública de datos. Una red pública de datos (PDN *Public Data Network)* es una red establecida específicamente para la transmisión de datos. Un requerimiento fundamental para una PDN es que deberá facilitar la interconexión de diferentes equipos de proveedores, los cuales deberán estar de acuerdo en los estándares establecidos para el acceso y uso de esas redes. Después de muchas discusiones, se llegó a un acuerdo internacional para el establecimiento de estándares a utilizar que fueron aceptados por el CCITT para utilizarse con una serie de redes.

Hay dos tipos principales de PDN´s conmutación de paquetes (PSPDNs *Paquet Switching Public Data Network*) y conmutación de circuitos (CSPDNs *Circuit Switching Public Data Networks*). Diferentes estándares han sido definidos para capa tipo. En general, los estándares para cada una de esas redes se refieren a los tres niveles más bajos del Modelo de Referencia OSI y las funciones de cada uno de esos niveles. Debe recordarse que las características de los niveles dependientes del nivel de red en el Modelo de Referencia OSI son transparentes para los niveles superiores del nivel de transporte.

2.5.2. CONMUTACIÓN DE CIRCUITOS Y PAQUETES.

Antes de describir los diferentes estándares de interfaces asociados con PDNs, esto es necesario para trazar las diferencias entre los dos tipos de conmutación usados en las redes.

De cada conexión establecida a través de una red con conmutación de circuitos da como resultado un canal de comunicación física siendo puesta a través de la red desde el equipo del abonado que realiza la llamada hasta el equipo del abonado que la recibe. Esta conexión es usada exclusivamente por los dos abonados en el tiempo que dure la llamada.

Un ejemplo de una red de conmutación de circuitos es la red pública de conmutación telefónica (PSTN *Public Switching Network*), todas las conexiones establecidas a través del PSTN son del tipo de conmutación de circuitos.

En el contexto de la transmisión de datos, una característica de la conexión de conmutación de circuitos, es que provee efectivamente una velocidad de canal y ambos abonados deben operar en esa velocidad. Antes de que cualquier dato sea transmitido en una conexión semejante, es necesario establecer una conexión a través de la red. Actualmente, el tiempo requerido para colocar una llamada a través del PSTN puede ser relativamente larga debido al tipo de equipo utilizado en cada intercambio.

Por lo tanto, cuando se transmiten datos, una conexión es establecida y mantenida abierta durante la transacción. Sin embargo, la introducción cada vez mayor de conmutación controlada por computadora, aunada al uso de transmisión digital en las redes, significa que el tiempo para establecer una conexión a través del PSTN es cada vez menor (décimas de milisegundos). Además implica usar una velocidad de transmisión mayor. Con esto ha sido posible, la transmisión de datos sin usar módem.

Aunque el tiempo de la conexión asociado con la conmutación de circuitos, completamente digital es relativamente rápido, la conexión resultante sin embargo solo proporcionará un canal con una velocidad fija que deberá ser usada por ambos abonados en la transmisión y recepción. En contraste, con una red de conmutación de paquetes, es posible para dos abonados comunicarse por medio del equipo terminal de datos (DTEs *Data Terminal Equipment*), que es parte de una estación de datos que sirve como fuente o destino de los datos, o ambos, para operar a diferentes velocidades, ya que la velocidad en la cual los datos son transferidos a las dos interfaces de la red son regulados separadamente por el equipo de cada abonado.

También, no se establecen conexiones físicas a través de la red con una conmutación de paquetes. En su lugar, todos los datos a ser transmitidos son primero ensamblados dentro de una o más unidades de mensaje, llamados paquetes, por la DTE fuente. Esos paquetes incluyen las direcciones de red DTE tanto fuente como destino.

Entonces son pasados por el DTE fuente a su central telefónica local (PSE *Paquet Switing Exchange*, Conmutación de Intercambio de Paquetes). En la recepción de cada paquete, el intercambio lo guarda y entonces inspecciona la dirección destino contenida en él. Cada PSE contiene un directorio de ruteo especificando el enlace de salida (la trayectoria de transmisión) para ser usada por cada dirección de red. En la recepción de un paquete, el PSE envía el paquete al enlace apropiado en una velocidad máxima disponible. Este modo de trabajo es también conocido como almacenamiento y envío de paquetes (*packet store-and-forward*).

Similarmente, como cada paquete es recibido (y guardado) en cada PSE intermedio a lo largo de la ruta, es enviado en el enlace apropiado entremezclado con otros paquetes que han sido enviados en ese enlace. En el PSE destino, determinado por la dirección de destino dentro del paquete, es finalmente pasado al DTE destino.

Cada transacción completa ocupa solo una porción (al azar) del ancho de banda disponible en cada enlace. Esto varía desde cero cuando los usuarios no esté transmitiendo ningún dato hasta un ancho de banda completo si se están transmitiendo paquetes continuamente.

Es posible que un número de paquetes llegue simultáneamente a una PSE por diferentes enlaces de entrada y que todos requieran ser enviados en el mismo enlace de salida. Claramente, si un número de paquetes particularmente largo están esperando a ser transmitidos en el mismo enlace, otros paquetes pueden experimentar un gran retardo.

Para prevenir que esto suceda y asegurar que la red tenga un tiempo transito confiable y rápido, una longitud máxima es permitida para cada paquete. Es por esta razón que cuando una red de conmutación de paquetes es usada, un mensaje colocado en el nivel de transporte dentro del DTE, puede primero tener que ser dividido por el protocolo de transporte fuente en un número de unidades de paquete pequeñas antes de la transmisión. En su momento serán reensambladas dentro de un mensaje por el correspondiente protocolo de transporte en el DTE destino.

Otra diferencia entre CSPDN y PSPDN es que en el primero la red no aplica ningún control de flujo de errores en los datos transmitidos. Lo cual debe ser ejecutado por él usuario. Con un PSPDN, sin embargo, un control de error sofisticado y un procedimiento de control de flujo son aplicados en cada enlace por las PSE de la red. Consecutivamente, la clase de servicio ofrecida por un PSPDN es normalmente mejor que la ofrecida por un CSPDN.

2.5.2.1. TÉCNICA DE CONMUTACIÓN DE CIRCUITOS.

Las características operacionales de la interfaz física a una red de conmutación de circuitos se definen en la recomendación X.21. La intención es proveer al usuario con una trayectoria de transmisión de datos con sincronización *full-duplex*, esto es que tenga la capacidad de transmitir simultáneamente datos en ambas direcciones, la cual está disponible durante la duración de la llamada.

2.5.2.2. TÉCNICA DE CONMUTACIÓN DE PAQUETES.

Con no poca frecuencia se dan casos de existir varios sistemas informáticos mutuamente incompatibles en una misma empresa, sobre todo si se trata de una multinacional. Las diversas modalidades de tráfico de datos, la adquisición de nuevas filiales dotadas de equipos distintos, las diferentes condiciones relativas a los servicios de apoyo locales, incluso consideraciones de orden político, contribuyen a la proliferación de sistemas diferentes dentro de la misma organización. Existen varias maneras de soslayar este problema, entre ellas la más obvia la constituye la unificación. Hay proveedores que se concentran justamente en este problema, ofreciendo métodos de conversiones de protocolo realizados a propósito para la interconexión de sistemas diferentes.

La solución brindada por la técnica de conmutación de paquetes –norma X.25– es algo distinta, haciendo innecesaria en la mayoría de los casos la aplicación de soluciones concretas realizadas a propósito, y ha sido acatada por todos los principales proveedores de equipos de transmisión de datos, y compañías operadoras de los servicios de telecomunicación de cada país. En la tabla 2.3. se muestra su evolución tecnológica durante las dos últimas décadas y la prevista para la actual.

La técnica de conmutación de paquetes constituye la solución de un problema planteado por el elevado costo de adquisición, por compra o arrendamiento, de líneas de transmisión de datos. Dicho costo aumenta en función de la distancia que separa los diferentes equipos informáticos a conectar.

Tal solución consiste en organizar el flujo de datos entre un gran número de computadoras, terminales, puestos de trabajo y otros elementos interconectados, de manera que sea posible compartir las rutas de transmisión. Esto se hace aprovechando el hecho de que, en la mayoría de sesiones de comunicaciones bidireccionales, los datos fluyen en realidad durante una parte relativamente pequeña de tiempo. Ello permite llenar los "espacios en blanco" de una línea de transmisión con datos que fluyen entre otros dispositivos informáticos.

1970	1980			1990	2000
Técnicas	Combinación de conmutación de paquetes (X.25) y proceso de protocolos (PAD)	Conmutación de paquetes (Proceso separado de protocolo)		Transmision de tramas (Frame Relay)	Conmutacion rápida de paquetes (Fast Packet Switching, ATM Cell Relay)
Arquitectura Hardware	Procesador unico (8/16 bits) Proceso Software	Procesador unico (16/32 bits) Proceso Software	Multiprocesador (16/32 bits) Proceso Software	Procesadores multiples (32 bits) Proc. Soft-Hard	Multicaja Bus de alta velocidad sobre LAN. Logicas bas. Hard
"Troughput" por nodo	10-100 pps Paquete X.25 de longitud variable	100-500 pps Paquete X.25 de longitud variable	500- 30.000 pps Paquetes X.25 de longitud variable	10.000-100.000 pps Tramas por segundo-LAPD	100.000- 1m ÷ Celulas por seg. 48bytes/celula
Estándares	DOD/ARPA CCITT-1976	CCITT-1976	CCITT-1980 CCITT-1984	CCITT Y.144 (1.986 DIS) Q.922 LAPD	ANSI TISI IEEE 802.6

Tabla 2..3. Evolución Tecnología de la Técnica de Conmutación de Paquetes

Técnicamente, los datos se ensamblan para formar unidades de tamaño adecuado, que se denomina "paquetes" de datos, de ahí el

nombre aplicado a la técnica. Cada paquete contiene información de dirección y de control, de modo que llega a su destino correcto cualquiera que sea la línea física por la que se transmite, garantizándose la integridad de la misma.

La red de paquetes de datos suele establecerse con cierto número de líneas de transmisión físicas alternativas dispuestas entre varios nodos. Los paquetes son dirigidos a lo largo de la ruta que resulta ser la óptima en un momento dado, conocida por "circuito virtual". La información de ruta es almacenada en cada nodo por el que pasa el paquete de llamada, lo que permite encaminar por la misma ruta los paquetes de datos subsiguientes.

Los defectos de transmisión son inmediatamente detectados y automáticamente corregidos por retransmisión, ya que los paquetes de datos van almacenados en cada nodo de la red. Además, por existir siempre varias rutas alternativas entre dos puntos cualesquiera de la red, ésta permanece prácticamente inmune a las interrupciones en las líneas de transmisión.

2.5.3. FUNCIONES DE UNA RED DE CONMUTACIÓN DE PAQUETES.

Las redes de conmutación de paquetes disponen de un amplio conjunto de funciones y servicios que lo dotan de una gran flexibilidad para adaptarse a cualquier necesidad, distinguiéndose entre ellas las

siguientes: funciones de conexión, de direccionamiento de seguridad, de gestión y las propias de la red.

2.5.3.1. CONEXIÓN.

Estas funciones definen la forma en que se establece la sesión entre dos dispositivos de la red (terminal/computadoras). En este tipo de redes la conexión se establece mediante circuitos virtuales (canales lógicos); por cada uno de ellos transcurre una sesión, pudiendo existir hasta 4.095 circuitos virtuales en un mismo enlace físico. Otra modalidad es la de datagrama, más simple desde el punto de vista del proceso del nodo, ya que en este caso los paquetes son enviados independientemente de los demás, no existiendo un ordenamiento entre ellos en el punto de recepción, y no pudiéndose garantizar siempre la entrega de los mismos; en esta modalidad cada paquete debe contener las direcciones de origen y destino, consultando cada nodo al recibirlo una tabla propia que le indica para cada dirección de destino la línea de salida a la que debe dirigir el paquete. Existen varios mecanismos básicos para establecer y mantener las comunicaciones:

Llamada virtual: La comunicación entre dos usuarios de la red puede establecerse mediante el procedimiento de llamada virtual, esto es similar en cierto modo a la forma en que se establece una llamada telefónica convencional. El dispositivo que origina la conexión envía a la red un paquete especial conteniendo la dirección de red del dispositivo con el que se desea comunicar. La red se encarga de dirigir ésta solicitud

hasta su destino. Si el dispositivo llamada acepta la conexión, se lo comunicará, a la red, que a su vez, informará al dispositivo que lo originó, estableciendo la conexión. En este momento comenzará la transferencia de datos en ambos.

Para concluir sesión, cualquiera de los dos dispositivos puede enviar a la red un paquete solicitando la liberación de la llamada.

Circuito virtual permanente: Un circuito virtual permanente presenta ciertas analogías con la líneas dedicadas convencionales. Dos dispositivos que dispongan de esta facilidad para comunicarse entre sí, tiene asegurada la conexión en cualquier momento. El dispositivo que desee enviar información entregará los paquetes a la red y ésta se encargará de hacerlos llegar al otro extremo. Por lo tanto, no se precisa ningún procedimiento de establecimiento no de la liberación.

Llamada de selección rápida: Los paquetes involucrados en el establecimiento y liberación de llamadas producen una cierta sobrecarga que en algunas aplicaciones puede ser interesante eliminar. En aquellos casos en que las sesiones sean muy cortas o se realicen transacciones muy breves, el tráfico de control necesario para establecer y liberar las llamadas adquiere un peso importante frente al propio tráfico de datos lo que se traduce en retardos que restan eficiencia al enlace.

La función de selección rápida permite incluir datos de usuario en los paquetes de establecimiento y liberación de las llamadas. De esta forma se agiliza el proceso de conexión/desconexión.

Llamada directa: Esta función permite que un dispositivo realice una llamada virtual a una dirección predefinida sin necesidad de suministrar, en el procedimiento de establecimiento de llamada, la dirección del dispositivo con el que desea establecer la sesión. Para que ello sea posible, debe estar convenientemente definida en la red la dirección a la que es posible llamar mediante este procedimiento. El dispositivo llamado recibe la solicitud de conexión como si el que llama hubiese realizado una llamada convencional.

Circuito virtual permanente/Llamada virtual: Esta función permite establecer una sesión entre dos dispositivos empleando procedimientos de circuito virtual permanente en el extremo que origina la sesión y de llamada virtual en el dispositivo con el que se desea establecer la comunicación.

2.5.3.2. DIRECCIONAMIENTO.

Estas funciones permiten que la red pueda establecer la ruta a seguir por los paquetes, tanto al establecer la llamada como ante la caída de un nodo o la congestión de un enlace entre nodos, realizándose el establecimiento de la ruta alternativa mediante ciertas tablas de rutas o bien dinámicamente.

Dirección de red: Cada dispositivo conectado a la red tiene asignada una dirección que lo identifica ante la misma. Dentro de una red puede existir usuario con direcciones de distinta longitud, no

requiriéndose un formato o sintaxis particular en las mismas, por lo que se pueden emplear distintos planes de numeración. Así mismo, la topología de la red tampoco impone restricciones en el plan de numeración aunque es recomendable que parte del campo de dirección esté relacionado con el nodo o área geográfica a la que pertenece el dispositivo.

Sudbirecciones: En algunos casos los dispositivos pueden no estar conectados directamente a la red, sino a través de un concentrador o subred, conectado a su vez a la red de conmutación de paquetes. En estas circunstancias existirá una dirección de red única para todo el grupo de dispositivos. Para poder seleccionar cada uno de ellos individualmente se emplea. Como subdirección, uno o varios de los tres últimos dígitos del campo de dirección. Esto permite que el concentrador o la subred, empleando este campo, seleccionen el dispositivo adecuado. Los dígitos correspondientes a la subdirección son enviados en forma transparente a través de la red, pues la selección de los dispositivos individuales se realiza fuera de la red de conmutación de paquetes, usualmente en el dispositivo que actúa como concentrador.

Selección por nombre: Para simplificar los procedimientos de conexión es posible definir nombres que equivalgan a direcciones de red. De esta forma, el usuario sólo necesita indicar el nombre correspondiente al destino al que quiere llamar. La red se encarga de convertir el nombre en una dirección de red válida, realizándose los análisis de dirección y encaminamiento en la forma normal. Esto es especialmente útil cuando los nombres reflejan la función o servicio suministrado por la dirección

de red a la que se llama. El usuario no necesita conocer la dirección real. En caso de que ésta cambie, el usuario no necesita modificar su procedimiento de conexión.

Grupo de búsqueda: En algunas circunstancias, un grupo de dispositivos puede dar acceso a un mismo servicio o función (ejemplo: controladores de comunicaciones, etc.). Aunque cada uno de ellos tiene su propia dirección, es posible asignar una dirección de red común para todos los dispositivos del grupo. Las llamadas que vayan dirigidas a un grupo de este tipo serán encaminadas al primer dispositivo del grupo que se encuentre disponible. A los dispositivos que forman el grupo puede también accederse empleando su dirección de red propia.

La dirección de un grupo de búsqueda puede ser empleada como una dirección de red válida por cualquier usuario de la red que desee comunicarse con alguno de los dispositivos que pertenecen al grupo.

2.5.3.3. SEGURIDAD.

Las redes de conmutación de paquetes disponen de funciones para controlar y restringir el acceso a la red, con el objeto de dotarlas de una mayor seguridad.

Grupo cerrado de usuarios: Mediante esta función es posible restringir el acceso de grupos predefinidos de usuarios a determinadas funciones. Los usuarios que forman parte de un grupo cerrado sólo puede

comunicarse con otros miembros del grupo, aunque un usuario puede pertenecer a más de un grupo. En este último caso, uno de los grupos será considerado como preferente.

Es posible asignar accesos de salida a algunos usuarios de un grupo cerrado. Esto les permite realizar llamadas a usuarios no pertenecientes a dicho grupo. Analógicamente, es posible asignar a algunos usuarios de un grupo cerrado acceso de entrada para recibir llamadas procedentes de usuarios que no pertenezcan al grupo.

Obstrucción de llamadas entrantes/salientes: Mediante esta función es posible restringir los accesos de entrada/salida a los usuario de la red.

Es posible impedir que un dispositivo conectado a la red acepte llamadas dirigidas a él. Cualquier intento de acceso hacia un usuario definido así, será rechazado por la red. Analógicamente, es posible impedir que un usuario realice llamadas.

2.5.3.4. RED.

Las redes de conmutación de paquetes disponen de una serie de funciones que las dotan de cierta inteligencia. La gestión de encaminamientos, la confirmación de la recepción de mensajes, la integración de diversos sistemas, la difusión automática de paquetes, etc., son funciones que elevan las presentaciones de estas redes.

Encaminamiento: Cada uno de los nodos dispone de funciones de análisis de direcciones y encaminamientos. Estas funciones se activan durante el proceso de establecimiento de un circuito virtual, basándose en la información de direccionamiento, explícita o implícita, suministrada en el procedimiento de llamada. En el caso de circuitos permanentes, la información de direccionamiento se extrae de las definiciones hechas por el operador de la red.

En análisis de dirección y encaminamiento es realizado por cada nodo de la red. En primer lugar, el nodo determina su la dirección de destino corresponde a una terminal conectada a otro nodo. Si esto es así, deberá determinar el camino adecuado para llegar al nodo correspondiente. Este análisis lo realiza mediante unas tablas de encaminamiento definidas en cada nodo. En dichas tablas se especifica un conjunto de rutas primarias y alternativas para alcanzar cada uno de los nodos vecinos.

Si se produce un problema en una ruta (caída de un enlace, congestión de un nodo intermedio, etc.) se selecciona otra ruta alternativa que permita continuar las sesiones que se hayan visto afectadas por la interrupción de la ruta inicial.

Clases de prioridad: Para gestionar óptimamente los recursos de transmisión de una red de conmutación de paquetes, se emplean mecanismos de prioridad de tráfico que son utilizados principalmente cuando se produce una situación de congestión en la red. En virtud a las

prioridades asignadas se decidirá qué nuevas llamadas serán rechazadas y cuáles de las ya establecidas deberán ser canceladas.

Los mecanismos de prioridad también se emplean para distribuir el tráfico en la red de acuerdo con las aplicaciones que la utilizan. A cada usuario de la red se le asigna una prioridad de tráfico. Por ejemplo, transacciones que requieran tiempos de respuesta muy cortos deberán tener una prioridad alta, mientras que los procesos batch tendrán menos prioridad. De esta forma se puede definir un esquema de prioridades que se adapte perfectamente a las necesidades de los usuarios de la red.

Control de congestión: Para mantener lo más fluido posible el tráfico en la red es necesario evitar situaciones de congestión, ya que la red, como un todo, posee una capacidad limitada de almacenamiento y proceso siendo por ello necesario controlar aquellos recursos que puedan producirla (procesadores, memoria, colas de transmisión, velocidad de los enlaces, etc.). Los mecanismos de control de congestión minimizarán los efectos de excesivos volúmenes de tráfico, interrupciones temporales de los enlaces, mal dimensionamiento de la capacidad de enlaces, memoria o procesadores.

Este control se realiza restringiendo la aceptación de nuevas llamadas en los recursos que se encuentran sobrecargados. Las restricciones se aplican gradualmente en función de la prioridad de las llamadas. El operador de la red puede especificar los niveles de congestión a partir de los mecanismos de control que entran en

funcionamiento, así como su impacto sobre los distintos tipos de tráfico (prioridades).

Su contenido consiste en integrar todas las modalidades de tráfico de datos que existen en el seno de una organización, ya se trate de la transmisión por tandas de gran cantidad de datos, o de la comunicación interactiva entre terminales y computadoras primarias o computadora central (*mainframe*) situados a distancia.

Control de flujo: La existencia dentro de la misma red de máquinas de características diferentes, con distinta capacidad de proceso, hace que sea posible que le llegue a una mayor cantidad de información de la que es capaz de procesar, para paliar este inconveniente es por lo que dentro de la red se establecen diferentes mecanismos de control de flujo, siendo los más comunes aquellos, que mediante algún mensaje especial de control, indican el emisor que deje de emitir, o bien aquellos que en caso de un flujo de transmisión relativamente constante, hacen una asignación previa de recursos (por ejemplo durante el establecimiento de un circuito virtual), para que el transmisor ajuste su flujo, de manera que no se sobrepase la capacidad del receptor. En cierta forma, los mecanismos de control de flujo pueden ser utilizados también para el control de congestión; sin embargo y debido a la naturaleza irregular de las transmisiones entre nodos, su eficiencia puede verse muy limitada, ya que si limita el tráfico a una tasa media, los usuarios que transmitan en ráfagas de alto volumen no serán satisfechos, y si se permiten picos de alto tráfico la red será congestionada si coinciden varios usuarios al mismo tiempo enviando gran cantidad de información.

CAPÍTULO III. PROTOCOLOS.

Objetivo:

Describir la implementación de protocolos en el contexto del modelo de referencia OSI, su estructura y su utilización para la comunicación en entre redes de datos.

CAPÍTULO 3. PROTOCOLOS.

Los protocolos de comunicación de datos son usados para coordinar el intercambio de información entre diferentes dispositivos de la red. Ellos establecen el mecanismo para reconocer cual manda información hacia otro. En el mundo de las comunicaciones de hoy, hay un gran número de protocolos en uso, junto con varias estructuras básicas en diferentes aspectos de la comunicación de datos.

En este capítulo, veremos la implementación de protocolos en el contexto del modelo de referencia OSI. Se hablará acerca de su estructura y como utilizarlos para la comunicación en una red.

Antes el dominio radicaba en los pequeños grupos de trabajo y oficinas departamentales, actualmente las redes de área local tiene la mejor plataforma de integración para impulsar la computación. Desde una simple red para 20 usuarios hasta tener una expansión considerable de 5 mil usuarios, dando un gran empuje hacia la interconectividad entre redes, tendiendo una flexibilidad de expansión desde cubículos de oficina hacia zonas distantes.

Con las nuevas plataformas, los protocolos LAN han venido incrementando su poder y flexibilidad. En este capítulo examinaremos los siguientes protocolos para soportar el trabajo de grupos.

- IPX/SPX
- TCP /IP

- SNMP
- X.25
- FRAME RELAY
- ATM

3.1. IPX/SPX

El sistema operativo *NetWare* fue desarrollado por *Novell, Inc.* e introducido al mercado a principios de los años 80´s. Su arquitectura está basada el sistema de Red Xerox (XNS). *NetWare* proporciona soporte a una amplia variedad de estándares de redes LAN (incluyendo Ethernet. 802.3, 802.5, Token-Ring IBM y Arcnet).

Funcionalmente el nivel de red (direccionamiento, ruteo, etc.) es manejado por el protocolo IPX. Arriba de la capa de red, *Netware* provee una amplia variedad de servicios. Por otra parte, el protocolo SPX proporciona la interfaz de la capa de transporte.

3.1.1. IPX.

IPX (*Internetwork eXchange Protocol*) es un protocolo no orientado a la conexión que trabaja al nivel de la capa de red, y es una desviación del protocolo de Xerox IDP (Protocolo de Datagramas Inter-red). IPX ejecuta funciones de direccionamiento y ruteo. Después que los paquetes viajan a través de la red, alcanzan a la estación de trabajo destino o al

servidor de archivos. Las estaciones intermedias usan IPX para rutear los paquetes hasta su destino final.

IPS hace un gran esfuerzo para entregar los paquetes al destinatario y no requiere el reconocimiento o verificación de si los paquetes verdaderamente han llegado al destino IPX trabaja con protocolos de capas superiores como SPX o NCP a quienes proporciona un confiable servicio de flujo de datos.

La función principal de IPX es rutear datos, y toma sus decisiones de ruteo basándose en la información proporcionada por RIP (Protocolo de Información de Ruteo).

La versión del RIP es básicamente la misma que emplean los protocolos de Internet.

Un paquete IPX consiste de un encabezado (*header*) y una sección de datos. El *header* tiene una longitud de 30 bytes. IPX no proporciona facilidades para la fragmentación de paquetes, la implementación de IPX debe garantizar que el paquete enviado sea lo suficientemente pequeño para ser transmitido en cualquier enlace físico que ellos necesiten atravesar. IPX requiere de enlaces físicos que sean capaces de manejar paquetes con una longitud de 576 bytes. La estructura del paquete IPX es mostrada en la figura 3.1.

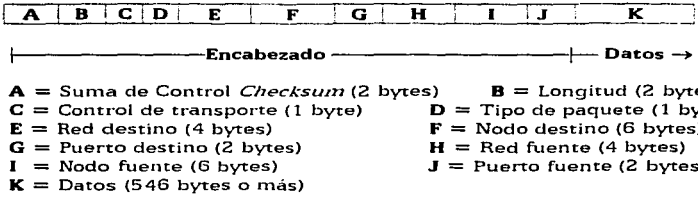


Fig. 3.1. Encabezado del Paquete IPX.

Suma de Control (*Checksum*): No es usado por IPX, todos los bytes son puestos en 1, de acuerdo al encabezado original de XNS.

Longitud: Contiene el número de bytes del datagrama completo de IPX, (*header* y los datos incluidos). La longitud mínima es de 30 bytes (sin datos). No hay un límite máximo, a menos que el paquete sea ruteado (máximo 576 bytes).

Control de transporte: Garantiza que el datagrama nunca regrese en dirección opuesta a la red indebidamente. El campo es inicialmente cero por la estación fuente e incrementa su valor cuando pasa por un ruteador. Cuando el valor de este campo es igual a 16, el datagrama es eliminado.

Tipo de paquete: Define a que protocolo de capas superiores se le debe entregar la información del paquete. IPX define los siguientes cuatro tipos de paquetes.

0	Tipo de paquete desconocido
4	Paquete de intercambio de protocolo
5	Protocolo del paquete de secuencia
17	Núcleo de protocolo Netware

Red destino: Indica la dirección destino de los paquetes. Las direcciones fuente y destino son designadas por el administrador de la red. Cuando los nodos fuente y el destino se encuentran en la misma red, éste campo es cero.

Nodo destino: Contiene la dirección física de destino (generalmente implícita en la tarjeta de red). Las direcciones de algunas redes como IEEE 802.5, IEEE 802.3 y Ethernet requieren de los 6 bytes completos. Cuando la dirección no requiere los 6 bytes, los bytes más significativos que no se usan son llenados con ceros.

Puerto destino: Este campo especifica el puerto destino (*socket*) de los procesos de las capas superiores, Xerox ha asignado números de puertos a algunos procesos incluyendo los protocolos RIP y Echo, además de puertos específicos para ser usados por NetWare de Novell.

La siguiente lista muestra los más importantes números de socket. La "h" que sigue del número significa que este esta representado en hexadecimal.

451h	Paquete de servicio de archivos (FSP)
452h	Protocolo anuncio de servicios (SAP)

453h Protocolo de ruteo de información de Novell (RIP)
455h NetBIOS
456h Diagnósticos

Red fuente: Esencialmente contiene lo mismo que el campo de red destino, excepto que éste mantiene las direcciones de red de la fuente del paquete.

Nodo fuente: Prácticamente es igual al campo de nodo destino, la diferencia consiste es que éste mantiene las direcciones de nodo de la fuente del paquete.

Puerto fuente: Este campo es casi igual al campo de puerto destino, se diferencian en que éste guarda las direcciones del puerto fuente.

Datos: En este campo se encuentran contenidos los datos destinados a ser procesados por las capas superiores. Contiene la información que será enviada a través de la red. Los paquetes de protocolos del nivel superior, son semejantes a SPX, NCP, RIP y SAP, son situados en la sección de datos del paquete IPX. Este proceso de relleno de los paquetes del protocolo del nivel superior, es cargado y encapsulado en la sección de los datos.

IPX mantiene una conexión con la capa de enlace de datos, la cual ensambla los datos en la trama para su transmisión a través de la red. La dirección el nodo destino es proporcionada a IPX en la capa de enlace de datos y depende si el nodo está conectando o es reconocido por la red

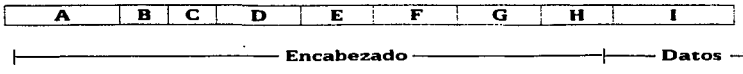
local o una estación remota. Todas las estaciones en la red comparten el mismo número de red.

Si la estación destino es localizada en una red local, la dirección de la estación es manejada dentro de la capa de enlace de datos con el paquete IPX para redireccionar a la estación destino. Si ésta pertenece a una red diferente a la estación fuente, realizará un trabajo extra para realizar esta operación.

3.1.2. SPX

SPX es un protocolo de la capa de transporte de Novell, este es una derivación del Protocolo de Secuencia de Paquetes (SPP), proporciona confiabilidad, orientada a la conexión, servicio de circuitos virtuales entre las estaciones de la red. SPX hace uso de los servicios del datagrama de IPX para proporcionar una secuencia al flujo de datos. Este lleva a cabo dicha implementación para un sistema que requiere reconocer cada paquete enviado, también proporciona un control de flujo entre las estaciones de la red y asegura que no se dupliquen al entregar a los procesos remotos.

SPX incluye 12 bytes en el *header* del paquete IPX, la mayor parte de este transporta información de control de conexión. El número máximo del tamaño para el paquete del SPX es de 576 bytes al igual que el número máximo en el paquete IPX. El encabezado de SPX se muestra en la figura 3.2.



A = Encabezado de IPX (30 bytes) **B** = Control de conexión (1 byte)
C = Tipo de datos (1 byte) **D** = ID de conexión fuente (2 bytes)
E = ID de conexión destino (2 bytes) **F** = Número de secuencia (2 bytes)
G = Número de reconocimiento **H** = Número de localidad (2 bytes)
I = Datos (534 bytes o más)

Fig. 3.2. Encabezado de SPX.

Control de conexión: Proporciona banderas que regulan el flujo de datos en la conexión. Por ejemplo, 10h significa final del mensaje, en tanto que 40h es un reconocimiento solicitado.

Tipo de flujo del mensaje: Identifica la naturaleza de los datos dentro del paquete. Es similar al campo "tipo" en la trama Ethernet.

ID´s conexión fuente y conexión destino: Se emplean para identificar circuitos virtuales. El ID de la conexión fuente es usado para demultiplexar circuitos virtuales separados de un solo puerto.

Número de secuencia: Proporciona un identificador numérico para cada paquete enviado. Es similar en sus funciones al número de secuencia de TCP.

Número de reconocimiento: Identifica el número de secuencia del próximo paquete que el receptor espera recibir.

Número de localidad: Informa al transmisor acerca del número de *buffers* recibidos como disponibles para la conexión. Esta asistencia de SPX con la implementación del control de flujo de la conexión prevé rápidamente al transmisor para manejar una recepción lenta.

Datos: Contiene los datos destinados a ser procesados por las capas superiores.

3.2. TCP/IP.

La *suite* de protocolos de Internet es actualmente el conjunto de protocolos de comunicación más popular para conectar sistemas heterogéneos en diversos ambientes de capa física, siendo los más reconocidos el Protocolo de control de Transmisión TCP (*Transmission Control Protocol*) y el Protocolo de Internet IP (*Internet Protocol*).

La *suite* de protocolos de Internet especifica funciones correspondientes a los niveles que se encuentran arriba de la capa de enlace de datos. La omisión de protocolos de capas inferiores fue intencional, ya que ésta manera permite a la *suite* interactuar con diferentes tecnologías físicas y de enlace de datos, como se puede ver en la figura 3.3. Esta ha sido una de las claves más importantes en el éxito de los protocolos de Internet.

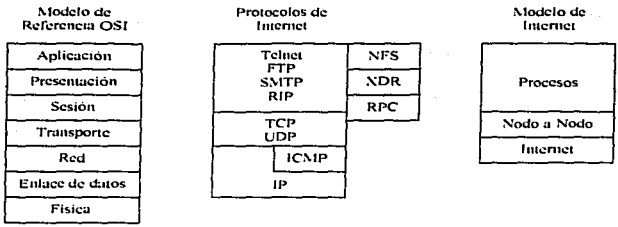


Fig. 3.3. Protocolos de Internet y el Modelo de Referencia OSI.

La *suite* de protocolos Internet precede al modelo de referencia OSI por cerca de una década, sin embargo generalmente puede ser mapeada al modelo. TELNET (Protocolo de Emulación de Terminal), FTP (Protocolo de Transferencia de Archivos), SMTP (Protocolo de Transferencia de Correo Electrónico) y RIP (Protocolo de Ruteo de Información) son protocolos de proceso Internet. Los protocolos de procesos proporcionan al usuario servicios de aplicación y aproximadamente corresponden a las capas de aplicación, presentación y sesión del modelo OSI. TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagrama de Usuario) son protocolos nodo a nodo, éstos entregan y reciben datos de otros protocolos y corresponden aproximadamente a la capa de transporte de OSI. IP y SMTP (Protocolo Internet para Control de Mensajes) son protocolos Internet, estos ayudan a mover los datos a través y entre redes conectando máquinas fuente y destino. Estos coinciden con la capa de red de OSI.

La *suite* de protocolos de Internet consiste en decenas de protocolos, sin embargo en ésta sección solo describiremos al IP y TCP.

3.2.1. IP.

IP es un protocolo no- orientado a la conexión, que no garantiza la entrega de los paquetes provenientes de la capa de transporte a través de una inter-red. IP puede fragmentar dichos paquetes en unidades menores, y posteriormente reensamblarlos en una estación intermedia (generalmente un ruteador) o un nodo destino. Cada paquete proveniente de la capa de transporte o sus fragmentos, son acoplados con un encabezado de IP y transmitidos como una trama por los protocolos de las capas inferiores.

Dependiendo de la estructura de la red, pueden existir numerosas vías disponibles entre los nodos fuente y destino. IP es usado por TCP y UDP para rutear los paquetes a través de la red. El segmento TCP es colocado en la sección de datos del datagrama IP.

IP mueve los datagramas a través de la inter-red, un salto a la vez. A lo largo de la trayectoria cada ruteador toma una decisión acerca de cual va a ser el próximo salto del datagrama.

Diferentes fragmentos de un paquete proveniente de la capa de transporte pueden tomar distintos caminos durante su viaje, esto puede ocasionar que dichos fragmentos lleguen al destino de manera

desordenada. En este caso, ya en el destino IP reensambla los fragmentos en la secuencia correcta.

El encabezado de IP consiste de numerosos campos. Los cuales se muestran en la figura 3.4. y se describen a continuación de ella.

<table>
<tr><td colspan="2">Versión</td><td>LHI</td><td colspan="2">Tipo de Servicio</td><td colspan="3">Longitud total</td></tr>
<tr><td colspan="5">Identificación</td><td>N F</td><td>M F</td><td>Offset de Fragmentación</td></tr>
<tr><td colspan="2">Tiempo de Vida</td><td colspan="2">Protocolo</td><td colspan="3">Comprobación del Encabezado</td></tr>
<tr><td colspan="7">Dirección Fuente</td></tr>
<tr><td colspan="7">Dirección Destino</td></tr>
<tr><td colspan="7">Opciones (+ relleno)</td></tr>
<tr><td colspan="7">Datos (Variable)</td></tr>
</table>

Fig. 3.4. Encabezado del Protocolo IP.

Versión: Permite a cualquier evolución del protocolo. Los ruteadores y equipos finales deben estar de acuerdo con el número de versión para asegurar que todos entiendan correctamente el encabezado de IP. Tiene una longitud de 4 bits.

Longitud del header Internet (IHL *Internet Header Length*): Indica el tamaño del encabezado del datagrama en palabras de 32 bits (la longitud mínima son 5 palabras). Su longitud es de 4 bits.

Tipo de servicios: Lo emplean las capas superiores para indicarle a IP como se debe manejar un datagrama en particular, uno de los

indicadores es el de importancia del paquete (0 normal, 7 muy importante). Tiene una longitud de 8 bits.

Longitud: Es un campo de 16 bits que contiene la longitud del paquete completo de IP, incluyendo el *headers* y los datos. El límite máximo en el tamaño del datagrama es de 65.535 octetos. En general, el límite de las implementaciones del protocolo Internet es de un largo máximo de 576 octetos de un datagrama.

Identificación: Junto con la dirección IP fuente, el número de identificación sirve para identificar un datagrama. Los fragmentos de una misma fuente con el mismo número de identificación son recolectados y colocados juntos (empleando el contenido del campo de fragmentación) por él ruteador o nodo destino (según sea el caso). Longitud 8 bits.

Banderas: El primer bit está reservado y fijo en cero, los últimos 2 bits de éste campo controlan la fragmentación del datagrama, el primer de ellos (NF no fragmentar) indica cuando el datagrama puede ser fragmentado, y el segundo (MF más fragmentos) especifica cuando el fragmento que se está recibiendo es el último. Su longitud es de 8 bits.

Offset de fragmentación: La implementación de IP en el destino utiliza el contenido de este campo para reensamblar los fragmentos en su paquete proveniente de la capa de transporte original, si cualquier fragmento no es recuperado, todos los demás son eliminados. La longitud de este campo es de 13 bits.

Tiempo de vida: Es un contador que limita la vida del paquete. El contador es decrementado en una unidad cada vez que el paquete pasa por un ruteador. Cuando el valor llega a cero, el paquete es eliminado. Esto evita que se formen ciclos infinitos en la red. La longitud de éste campo es de 8 bits.

Protocolo: Indica que protocolo nodo a nodo (TCP, UDP) va a recibir el paquete proveniente de la capa de transporte después de que lo procese IP. Su longitud es de 8 bits.

Comprobación del encabezado: Se emplea para asegurar la integridad del encabezado de IP. Si el valor incluido en el paquete no coincide con el calculado, el paquete es descartado. Dado que el valor del tiempo de vida es decrementado en cada ruteador, éste campo es recalculado en cada uno de ellos. Es un campo de 16 bits.

Direcciones fuente y destino: Son utilizadas para identificar tanto al que envía como al que debe recibir el paquete. Las direcciones de IP especifican tanto al nodo como a la red a la que pertenecen. Estos campos son de 32 bits de longitud.

Opciones: Este campo es variable y opcional en el datagrama. Sin embargo, todos los nodos y compuertas (*gateway's*) que tienen implementaciones de IP deben soportarlo si éste está presente.

3.2.2. DIRECCIONES DE IP.

Las direcciones usadas por el protocolo IP son llamadas direcciones Internet. Estas direcciones son de valores de 32 bits, las cuales se separan en número de red y número de nodo. Estas direcciones lógicas se acostumbra escribirlas en notación punto decimal, la cual consiste en cuatro números decimales separados por puntos (ejemplo, 192.32.45.1).

Comúnmente se usan tres clases de direcciones, estas se muestran en la figura 3.5.

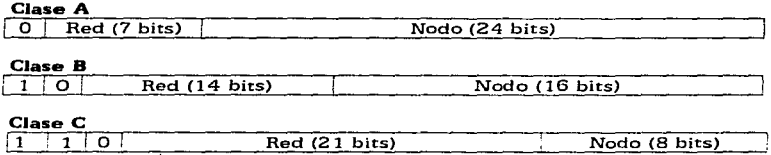


Fig. 3.5. Clase de Direcciones Internet.

- Las redes clase A usan el primer byte para indicar la red, y dentro de él emplean el primer bit para identificar la clase de la dirección, los 24 bits restantes especifican al nodo dentro de la red. Esta clase es muy útil para redes con una gran cantidad de nodos. El rango utilizado para número de red va de 1 a 127.

- En las redes clase B, se usan lo dos bytes iniciales para identificar la red. Los primeros dos bits son fijos y tienen un valor de 1 y 0 e indican

la clase de la dirección, los siguientes 14 bits identifican la red. Los restantes 16 bits identifican al nodo. Esta clase se emplea en redes con un número moderado de nodos. El rango utilizado para número de red va 128 a 191.

- Para las redes clase C, se emplean los primeros tres bits para identificar la red. Los primeros tres bytes son fijos, su valor es 1 1 0 y sirven para indicar la clase de la dirección, los siguientes 21 bits identifican la red. Los siguientes 8 bits especifican el nodo. Esta clase es utilizada por organizaciones pequeñas que tienen pocos nodos. El rango usado para número de red va de 129 a233.

En la figura 3.6 se muestran las limitaciones que tiene cada una de las clases de direcciones IP en base al número de bits utilizados para definir la red y el nodo dentro de ella.

Clase	Núm. máx. de redes	Núm. máx. de nodos por red
A	126	16 777 214
B	16 384	65 534
C	2 097 150	254

Fig. 3.6. Limitaciones de las Clases de Direcciones IP.

3.2.3. TCP.

TCP (*Transmission Control Protocol* Protocolo de Control de la Transmisión), es el protocolo de transporte primario de Internet, además suministra confiabilidad a IP. Es un protocolo orientado a la conexión que acepta mensajes de cualquier longitud que provengan de un protocolo de capas superiores y proporciona, comunicación *full-duplex*, números de reconocimientos y transporte de flujo controlado a otra estación que corra TCP.

TCP garantiza la confiabilidad del flujo del enlace orientado a la conexión nodo a nodo, y confía el material a IP para que se haga cargo de fragmentarlo y reensamblarlo tanto como se requiera.

TCP requiere que la conexión sea establecida entre dos procesos que necesiten comunicarse. Este proceso emplea un cierto tiempo y esfuerzo necesario para ampliar desde el principio hasta el fin de una sesión que afecte el establecimiento o caída de la conexión. Durante el establecimiento de la conexión, los parámetros fundamentales que son usados desde el principio hasta el fin para establecer la conexión incluyen el uso de *socket*, número de secuencia de datos y tamaño de la venta para el control del flujo.

El punto final de la conexión de TCP es llamado *socket*, el cual es la combinación de la dirección de red, dirección del nodo y número de *socket* del nodo local. El *socket* es un concepto lógico que facilita

procesar múltiples aplicaciones para usar el servicio de transporte de TCP en la misma computadora.

El encabezado de TCP consiste de numerosos campos, los cuales se muestran en la figura 3.7. y se describen a continuación de ella.

<table>
<tr><td colspan="3">Puerto Fuente</td><td colspan="4">Puerto Destino</td></tr>
<tr><td colspan="7">Número de Secuencia</td></tr>
<tr><td colspan="7">Número de Reconocimiento</td></tr>
<tr><td>Offset de Datos</td><td>Reservado</td><td>URG</td><td>ACK</td><td>PSH</td><td>PSYT</td><td>SYN</td><td>FIN</td><td>Ventana</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="4">Apuntador de Urgencia</td></tr>
<tr><td colspan="7">Opciones (+ relleno)</td></tr>
<tr><td colspan="7">Datos</td></tr>
</table>

Fig. 3.7. Encabezado de TCP

Puerto fuente: Identifica al protocolo fuente de capa superior. En muchos casos, los puertos son asignados en tiempo real por TCP, sin embargo existe una lista de números de puertos que han sido asignados para protocolos muy empleados, incluyendo TELNET, FTP y SMTP. Su longitud es de 16 bits.

Puerto destino: Es idéntico al puerto fuente excepto a que este se refiere al protocolo destino de capa superior. Su longitud es de 16 bits.

Números de secuencia: Este campo usualmente contiene el número de secuencia asociado al primer byte de datos en el mensaje actual. Si el bit SYN es colocado, el número de secuencia define al número de secuencia inicial (ISN) a ser usado en la transmisión que se recibe.

Cuando un mensaje está dividido en numerosas partes. TCP usa este campo para reensamblar las partes del mensaje en su orden y garantizar la entrega al protocolo de capa superior correspondiente. Su longitud es de 32 bits.

Número de reconocimiento: Si el bit ACK (descrito más adelante) es colocado, el número de secuencia del siguiente byte de datos que el emisor de éste paquete espera recibir, el número de secuencia inicial no inicia con 0. La longitud de este campo es de 32 bits.

Este mecanismo está diseñado para optimizar el uso del ancho de banda. En lugar de requerir un reconocimiento separado y distinto para cada transmisión de datos, TCP puede retardar los reconocimientos hasta que una serie de transmisiones puedan ser reconocidas a la vez.

Offset de datos: Este campo indica el número de palabras de 32 bits incluidas en el encabezado de TCP. La longitud del encabezado puede variar ya que el tamaño de campo "opciones" (se describirá más adelante) es variable. Su longitud es de 4 bits.

Reservado: Este campo se reserva para usos futuros, es de 6 bits (todos ceros). El campo para las banderas de control es de 6 bits de longitud y conecta el siguiente significado a los bits correspondientes.

URG: Indica que el campo del apuntador de urgencia (descrito más adelante) contiene un valor significativo y debe ser usado.

ACK: (Acknowledgment Acuse de recibo): Indica que el número de reconocimiento contiene el número de secuencia y es válido.

PSH: Instruye al TCP emisor a entregar inmediatamente todos los datos a las capas inferiores para su transmisión. También indica al TCP receptor a entregar todos los datos presentes a su protocolo de capa superior.

RST: Inicializa una conexión de transporte a su estado inicial, usualmente como resultado de alguna condición irregular.

SYN: Bandera de control usada para establecer una conexión y sincronizar los números de secuencia, los usan el emisor y el receptor en su primer paquete. Colocar estas banderas indica que se desea establecer y sincronizar una conexión virtual. El procedimiento de "reconocimiento en tres pasos" funciona de la siguiente manera:

- el iniciador de la conexión envía un paquete con el bit SYN activado y un número de secuencia de algún valor X.

- El receptor responde con un paquete que tiene activados los bits ACK y SYN. El campo de reconocimiento en este paquete debe ser X + 1, y el número de secuencia debe ser de valor Y.

- El iniciador de la conexión responde entonces con un paquete que tiene activado el bit CK, y un número de reconocimiento de Y + 1. En éste momento la conexión ha sido oficialmente establecida.

FIN: Indica que el transmisor no tiene más datos y por lo cual termina la conexión.

Ventana: Especifica el número de bytes de datos que el emisor está dispuesto a aceptar. Este campo junto con los campos, número de secuencia y número de reconocimiento, implementan el mecanismo de flujo de control de TCP conocido como "ventaja deslizable". La longitud de este campo es de 16 bits.

Checksum: Se usa para determinar cuando el encabezado ha sido dañado durante el trayecto, si el *checksum* calculado no coincide con el dato incluido en el paquete. Éste es descartado.

Apuntador de urgencia: Especifica dentro de la cadena de datos un punto en donde se localizan datos urgentes. De hecho el valor de este campo apunta al byte que continua inmediatamente al último byte del dato urgente. La longitud de éste campo es de 16 bits.

Opciones: Este campo, si está presente, se localiza a continuación del campo de apuntador urgente. La opción más común es "tamaño máximo del segmento", la cual es usada durante el establecimiento de la conexión para indicar el mayor segmento que puede aceptar.

3.3. SNMP.

Los dispositivos inteligentes de una red (como puentes, ruteadores y concentradores) son ahora comunes. Tienen la habilidad de recolectar información y comunicarla a través de los protocolos de administración de la red hasta el punto en el que el personal que no pertenece al área técnica, pueda fácilmente identificar y corregir fallas de la red. Los proveedores planean sus productos teniendo la administración de la red en mente. La mayoría de estos productos usan el Protocolo Simple de Administración de Redes (SNMP *Simple Network Management Protocol).*

SNMP nació en 1988 con el fin de administrar los dispositivos de la red TCP/IP más grande, que une ambientes domésticos e internacionales en universidades, institutos de investigación, dependencias de gobierno y corporaciones privadas. Pronto se convirtió en estándar.

SNMP es el protocolo más popular para la administración de redes en la actualidad. Su éxito se puede medir por el aumento de más del 30 % en los proveedores que participaron durante los últimos cuatro años en la creación de productos basados en SNMP y lo que es más importante: los productos ya están en el mercado funcionando.

El éxito de SNMP en parte se debe a su simplicidad y pocos comandos (solo tienen tres). A pesar de que se deriva del ambiente TCP/IP, sus comandos requieren solamente de servicios de transporte básicos, lo que hace al protocolo independiente. Esto significa que la

información en SNMP se puede intercambiar con casi cualquier protocolo de red local. Tiene tres componentes.

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

Estos tres componentes junto con los integrantes de soporte (comandos y transporte) comprenden el marco de trabajo del SNMP.

A continuación se definirán estos componentes y se explicarán la forma en que interactúan para desempeñar las funciones de administración necesarias.

Administrador de red: No son muchos los años que han transcurrido desde la instalación de la primera red en nuestro país y son muchos los adelantados tecnológicos que esta área ha tenido. Constantemente salen al mercado nuevos productos para la función de administración de redes lo que complica seleccionar adecuadamente la mejor opción.

El administrador se ubica en una computadora dentro de la red y tiene la capacidad para enviar y recibir mensajes directos a todos los dispositivos que se encuentran conectadas a ella. La estructura de los mensajes están definidos por el estándar SNMP. Los administradores se comunican con los agentes se basa en un esquema de Protocolo de

Datagrama de Usuario (UDP *User Datagram Protocol*), es decir no requieren establecer una sesión entre los dispositivos.

MIB: es la base de datos en el mercado de SNMP, contiene un conjunto estándar de variables que es soportado por los agentes y administradores. Dos ejemplos de variables estándar son la dirección de dispositivos y el número de paquetes IP transmitidos MIB también contiene los recursos para mejorar el manejo de sus propios recursos.

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

La introducción de los nuevos productos basados en SNMP, trajo una proliferación de nuevos MIB´s. para controlar esta situación se han formado comités para desarrollar estándares para la creación de MIB en los diferentes tipos de productos.

SNMP es comúnmente referido a un protocolo de estimulo-respuesta, es decir, para cada solicitud emite una respuesta. Hay tres verbos básicos en su conjunto de comandos: *Get, Set y Trap*. Al usar el comando de *GetRequest* el administrador le solicita la información al agente, este le manda la información que necesita con un comando de

GetResponde. El administrador deberá usar el comando de *SetRequest* para controlar el dispositivo cambiado el valor de una variables del MIB. Así el agente responde con el comando de *GetResponde*. El agente también alerta al administrador, vía el comando *Trap* cuando encuentra algún problema (por ejemplo un puerto particionado) y entonces el administrador libera una alarma. Los mensajes de *Get, Set, y Trap* se manejan entre el administrador y los agentes, a través de un protocolo de transporte. Como el SNMP es un protocolo independiente, puede usar cualquier vehículo de paquete.

3.4. X.25

X.25 fue el primer protocolo liberado definiendo la conmutación de paquetes.

Las velocidades de acceso oscilan hasta 56 Kbps. Los conductos entre los modos de la red están limitados a 56 Kbps / 64 Kbps (con capacidad para velocidades fraccionales T1 bajo implementaciones propietarias).

X.25 contiene la detección y corrección de errores y control de flujo que requerían las obsoletas redes de comunicación analógicas de los ochenta.

Pero la mayor parte de esa saturación e intensas operaciones de proceso no son necesarias en las redes de fibra óptica actuales.

La conmutación de paquetes es únicamente un servicio que no requiere conexiones y que es efectivo para la transmisión cuya información no dependa del tiempo de respuesta, pero es poco recomendable para las conexiones orientadas y de voz y vídeo que requieren velocidad.

La conmutación de paquetes pasa información a través de la red de nodo a nodo empleando un esquema de encolamiento para el amortiguamiento y la transacción de datos.

La información es recibida y procesada si el ancho de banda se encuentra disponible. Si no lo está, la información es almacenada en la cola de espera hasta que éste se encuentra disponible (y la extensión del *buffer* de la memoria).

Los nodos de los extremos son los responsable de la detección y corrección de errores.

Los servicios de paquetes rápidos más recientes no realizan esta función de encolamiento, en su lugar éstos desechan el tráfico adicional que no puede ser transmitido en un red congestionada. El congestionamiento es un parámetro que aún no ha sido resuelto en estos nuevos servicios.

X.25 admite varios circuitos virtuales en la misma ruta física y puede transportar tamaños de paquetes hasta de 4096 KB. Tanto los Circuitos Virtuales Permanentes como los Circuitos Virtuales

Conmutados son soportados en X.25 y el esquema de direccionamiento permite que cualquier usuario envíe o reciba información de otro usuario. El tráfico puede también ser clasificado por prioridades.

X.25, es el servicio de conmutación de paquetes líder en todo el mundo, es muy usado para aplicaciones tales como en las máquinas de los cajeros automáticos, sistemas de aprobación de tarjetas de crédito, control de inventario, proceso de aplicación de préstamos y procesos de registros médicos. X.25 es una especificación de interfaz que describe como un ruteador u otro DE accesa la red de conmutación de un paquete. Definido como un ajuste de protocolos divididos en capas basados en el modelo OSI, X.25 proporciona transferencia de datos confiable de extremo a extremo a través de una red de área amplia (WAN).

El soporte a X.25 de los ruteadores debe cumplir con las recomendaciones X.25 CCITT de 1988 para ofrecer una interfaz en base a estándares para las capas físicas, de enlace de datos y de los protocolos de red. La especificación X.25 corresponde al modelo de referencia OSI (véase en la figura 3.8).

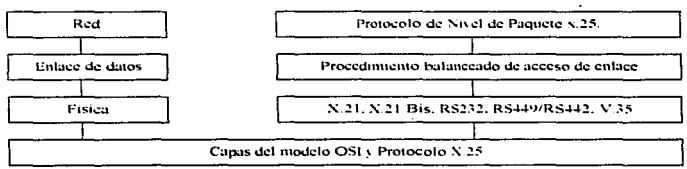


Fig. 3.8.

La capa física de los protocolos manejan la transmisión de bits a través de la conexión física especificando el requerimiento eléctrico, mecánico y de procedimiento para la comunicación de datos. La recomendación X.25 CCITT especifica una capa física de protocolo llamada X.21, es una interfaz sincrona de 8 cables, ampliamente utilizada en las redes de datos de circuitos conmutados en Europa , pero no en Norteamérica. Para cumplir con los requerimientos de América del Norte el CCITT ha especificado X.21. Bis que es también conocido como EIA232C o RS232C. para la mayoría de las aplicaciones los protocolos X.25 pueden funcionar sobre cualquier conexión sincrona y son soportados por las interfaces síncronas RS232, RS449/422 y V.35.

La recomendación X.25 para la capa de enlace de datos describe los procedimientos para el intercambio de información entre un dispositivo DTE (ruteador) y un dispositivo DCE (conmutador del paquete). La ayuda es asegurar un intercambio de información confiable en forma ordenada. La capa de enlace de datos del protocolo especificado para X.25 es un protocolo de Control de Enlace de Alto Nivel (HDLC *High-Level Data Link Control*) denominado Procedimiento Balanceado de Acceso de Enlace (LAP-B *Link Access Procedure: Balanced*).

Las unidades de información que pasa entre el ruteador y el conmutador del paquete, se llaman bloques LAP-B. Cada bloque LAP-B consiste de bits de transmisión de señales a cada extremo, campos de direccionamiento, control, información de longitud variable y campo de secuencia de verificación del bloque (FCS).

Los paquetes de datos X.25 conviven dentro del campo de información de los bloques LAP-B. Todos los paquetes de datos X.25 consisten en un encabezado de 3 bytes y un campo de datos.

Los primeros cuatro bits del encabezado del paquete de datos X.25 configuran el Identificador de Formato General (IFG), que indica el formato para el encabezado restante del paquete. Los bits 1 y 2 del IFG se usan en combinación para indicar la numeración secuencial del paquete utilizado (módulo 8 o módulo 128). El bit 3 es la letra D o bit de confirmación de entrega, que indica si el tipo de reconocimiento de capa del paquete requerido cuenta con importancia local de extremo a extremo. El bit 4 IFG es la Q o bit calificador de datos que indica si el paquete carga datos convencionales o información de control. El número de canal lógico actual especificado para una conexión determinada es una combinación de los dos próximos campos del paquete, el número del Grupo de Canal Lógico de 4 bits y el Número de Canal Lógico de 8 bits. Algunas redes tratan a estos 12 bits como un campo continuo.

El tercer bit en el encabezado del paquete de información X.25 es el campo de Identificación del Tipo del Paquete (ITP). El ITP se utiliza para detectar diferencias entre 28 posibles tipos de paquetes.

Cuando el receptor obtiene un bloque LAP-B. Éste realiza un cálculo usando contenidos en el campo FCS. Entonces los resultados son comparados con el número del campo FCS del bloque recibido. Si el resultado combina (es igual al número FCS del bloque), el receptor responde con un bloque de Receptor en Estado de Alerta.

Si el resultado no coincide con el FCS, el receptor responde con un bloque de rechazo que indica al transmisor la retransmisión del bloque.

Tres tipos de bloques son implementados por la información LAP-B o bloques-I, bloques supervisores o bloques-S y sin numerar o bloques-U.

Los bloques–I transportan datos a través del enlace. A cada bloque-I es asignado un número secuencial del 0 al 7 para asegurar que los bloques no se pierdan o se interprete fuera de servicio en su destino.

El flujo de control de información de los bloques-S requiere retransmisiones y reconocimiento de bloques-I. Cuando un conmutador recibe un bloque-I, éste responde ya sea con un Bloque Receptor en Estado Alerta o un bloque Receptor No Alerta. Los bloques Receptor en Estado de Alerta indican que el paquete ha sido aceptado y que el conmutador se encuentra listo para recibir más bloques-I. Un bloque Receptor no Alerta indica que el conmutador no puede procesar más bloques-I en ese momento. Los bloques-U procesan funciones de control de enlace adicionales como inicialización de enlace y desconexión y rechazo de bloques inválidos.

En el ambiente X.25, la capa de la red es conocida como la capa del paquete. La capa del paquete X.25 maneja la transferencia de paquetes desde el extremo de una conexión X.25 a la otra. X.25 utiliza circuitos para establecer rutas de transmisión a través de la red. Un circuito virtual consta de un conmutador individual de paquete (conmutación lógica al paquete ruteador) a conmutador de paquete y de ahí a

conexiones del ruteador. Cada conexión lógica en un circuito virtual es un enlace punto a punto identificado por un número único en el LCN del encabezado del paquete de datos X.25.

Los ruteadores X.25 soportan dos tipos de Circuitos Virtuales, Circuitos Virtuales Conmutados (SVC´s) y Circuitos Virtuales Propietarios (PVC´S). un circuito virtual conmutado es analógico a una conexión de marcación sobre la red telefónica y requiere tres fases por separado; establecimiento de llamada, transferencia de datos y desconexión de llamada. Un circuito virtual propietario proporciona una conexión fija punto a punto. Los circuitos virtuales propietarios se establecen por el intercambio de solicitud de llamada y paquetes de aceptación de llamada que permanecen permanentes disponibles a menos que sean sacados del servicio con comandos específicos del ruteador. X.25 puede soportar hasta 512 circuitos virtuales conmutados por tarjeta de puertos. Cada circuito virtual conmutado puede ser configurado como uno de los tres tipos de circuito de entrada, salida o de dos formas. Los 512 circuitos virtuales conmutados pueden difundirse a través de las cuatro líneas LAP-B en cualquier combinación.

3.5. FRAME RELAY.

Frame Relay es un servicio orientado a conexión que emplea PVCs y SVC en forma similar a la conmutación de paquetes. Sesiones múltiples (de hasta 100 PVCs) pueden realizarse sobre un solo circuito físico a través de velocidades T1 y E1 fraccionadas, y hasta un T1 y E1.

Frame Relay es sólo un servicio de transportación y no emplea el proceso del paquete de X.25, lo que garantiza un control de errores y flujo de polo a polo. Las necesidades de telecomunicaciones modernas han hecho necesarios el surgimiento de nuevos estándares y en el caso de la comunicación de redes de área amplia multipunto surge el estándar Frame Relay. Este no es otra cosa que una derivación de la tecnología denominada de conmutación de paquetes, es decir, un protocolo de comunicación muy similar a X.25 mediante el cual, cualquier usuario puede conectar su nodo a un servicio de comunicación provisto normalmente por una empresa pública de transmisión de datos.

Al estar conectado al servicio de comunicación, el nodo puede tener acceso mediante circuitos virtuales a cualquier otro nodo que se encuentre conectado también a este proveedor de servicios de comunicación, formando lo que se puede entender como una nube de circuitos virtuales, mientras que Frame Relay puede funcionar en un sistema de conmutación, es más eficiente cuando se implementa en tecnología del tipo *Fastpacket*, la cual minimiza los retardos, maximiza la utilización del ancho de banda y asegura un rendimiento confiable. De hecho, existe un alta relación costo beneficio asociada en la implementación de *backbones* del tipo ATM de banda angosta.

Para ofrecer un servicio eficiente el proveedor de servicios de conmutación debe crear red entretejida de nodos de conmutación que por su forma le dan el nombre a la nube y que están conectados con múltiples accesos entre sí.

Frame Relay, elimina gastos significativos de múltiples módulos en cada ruteador o *Front End Processor* (FEP) para comunicaciones en línea, porque en lugar de estos ofrece una simple interfaz física para soportar circuitos virtuales con muchos destinos.

Como podemos entender Frame Relay es un estándar de acceso a la nube que no se fija en lo que el *switch* con cada una de las tramas, lo único que importa es que el flujo de datos llegue a su destino de la misma manera que entró. De una manera sencilla podemos decir que transmite información en tramas de longiud variable solamente cuando las aplicaciones lo necesitan, evitando tener circuitos reales cuando no hay nada que transmitir.

A partir de que está característica limita la capacidad de Frame Relay de soportar aplicaciones de voz, vídeo o multimedia, tiene el gran beneficio de reducir costos al contar con la empresa pública de los servicios de comunicación.

Por otro lado, para implantar Frame Relay en las instalaciones del usuario, se requiere simplemente una actualización al software de los ruteadores y controladores de comunicación que ya existen en la actualidad.

A diferencia de X.25 el estándar Frame Relay es mucho más rápido y eficiente ya que no pide al nodo destino confirmar que la trama ha sido recibida, sino que parte del principio que las líneas de comunicación actuales de fibra óptica ofrecen una probabilidad muy baja de que la

trama no llegue a su destino. De todas formas, en caso de no recibirlo, el nodo destino simplemente pide que se reenvíe.

3.6. ATM.

ATM (Modo de Transferencia Asincrona) es un estándar muy reciente que define técnicas de alta velocidad, tanto para redes de área local (LAN) como para redes de área amplia (WAN), por lo cual toda la industria está a la expectativa de sus avances.

ATM es una técnica de red que usa un medio conmutado es decir mediante switcheo de paquetes. Puede ser instalado tanto sobre cable par trenzado como fibra óptica, esto explica el porqué ATM soporta velocidades de transmisión que varían desde los 25 MB hasta 622 MB, y se tiene planes de llevar esta velocidad hasta 2,488 GB.

ATM tiene la característica de transmitirse de manera asincrona, puesto que no utiliza tramas convencionales como en las otras técnicas de redes locales, en lugar de esto, ATM crea celdas de información de tamaño fijo de 53 bytes, 5 bytes son usados por el encabezado y los resultados de esto son la simplificación y la reducción de los costos del hardware, además de una gran flexibilidad.

Un punto muy importante es que, ATM aprovecha al máximo la velocidad de un medio físico, puesto que no crea tramas con información de control de errores; la eficiencia de los medios físicos ha llegado a ser

bastante confiable, y no es necesario un control de errores tan intensivo. Por otro lado, al tratar de obtener interoperabilidad entre ATM y otras técnicas de red, por lo que se necesitará de un mecanismo de conversión.

Debido a que ATM puede servir a todo tipo de configuraciones de red (incluso redes mundiales) y para distintos tipos de nodos y aplicaciones, es impredecible el tráfico transmitido y por lo tanto, asíncrono. Gracias a que el tamaño de las celdas es fijo, el retraso en ATM puede calcularse sin problemas. Al tener tan altas velocidades de transmisión pueden implementarse aplicaciones interactivas basadas en multimedia o audio y vídeo garantizados.

3.6.1. CELL RELAY.

Como Frame Relay es simplemente un estándar de acceso a la nube, los diversos fabricantes de ruteadores y multiplexores se han dado a la tarea de desarrollar actualizaciones de software para permitir a sus equipos entregar a la nube su flujo de datos en el formato predeterminado por Frame Relay.

El verdadero reto de telecomunicaciones se presenta al reducido grupo de fabricantes que desarrollan los equipos de conmutación interna de la nube, es decir los equipos que reciben el formato Frame Relay, pero luego deben de enviarlo de manera eficiente a través de circuitos virtuales a su nodo destino.

Cada fabricante de equipo de conmutación ha ideado una manera diferente de enviar la información dentro de ellos destaca Stratacom como el primer promotor de la tecnología Celll Relay para hacer altamente eficiente el manejo interno de los Circuitos Virtuales permanentes (PCV) de la nube.

Cell Relay a diferencia de Frame Relay es una tecnología que se usa para transportar la información dentro de la nube, es decir para comunicar los diferentes switches entre sí.

El principio básico de operación de Cell Relay es el de recibir flujo , en este caso de datos, vídeo o multimedia y convertirlo a segmentos muy cortos de longitud fija llamados celdas (cells) y transmitidas por caminos alternos hasta su nodo destino en donde se restablecen de la misma manera que llegaron.

Es importante no confundir en estos momentos las tramas que entran a la nube que son de longitud variable y que llegan en un formato predeterminado estándar con las celdas en las que son convertidas, que son de longitud fija y una vez que llegan al switch destino son reintegradas nuevamente en tramas y entregarlos al nodo destino Frame Relay.

En el caso de Cell Relay a diferencia de Frame Relay la celda puede contener información proveniente de voz, vídeo, datos o multimedia dado que los switches que componen la nube tiene una gran capacidad de

procesar las celdas desmenuzando y volviendo a armar su contenido sin importar sus características.

Esta tecnología de celdas fija y su formato de transmitirse es denominada conmutación rápida de paquetes, Fast Packet Switching, Cell Relay o más recientemente ATM (Modo de Transferencia Asíncrono).

3.6.2. ATM BANDA ANCHA Y BANDA ANGOSTA.

Cell Relay, mejor conocido como ATM tiene dos modalidades, una existe desde 1986 desarrollada por Startacom que utiliza anchos de banda de hasta 2 MB (E1), y otra recientemente homologada que utiliza anchos de banda de hasta 34 MB (E3) la primera se denomina Narrow Band ATM es decir transmisión asíncrona en banda angosta y la segunda se denomina Broad Band ATM es decir transmisión asíncrona en banda ancha

Broad Band ATM es el estándar recientemente emitido por CCITT que segmenta la información en celdas de 53 bytes de los cuales 5 bytes son utilizados para el direccionamiento de la celda en tanto que Narrow Band ATM segmenta la información en celdas de 24 bytes utilizando 3 bytes para el direccionamiento de la celda.

Dado que la mayoría de las aplicaciones del presente no requieren y no pueden justificar a un el costo de los equipos de Broad Band ATM, en la actualidad muchas más redes de equipo Narrow Band ATM han sido

instaladas durante los últimos dos años, y gracias a que maneja una celda más pequeña es más eficiente cuando las velocidades de la Red varían entre 128 KB hasta 2 MB. Solamente unas cuantas Broad Band ATM empiezan a aparecer en aquellos proveedores de servicios que han detectado una utilización de tráfico masivo de sus clientes.

La siguiente figura muestra una WAN que utiliza Broad Band ATM en el backbone de la LAN. En este caso, las velocidades de transmisión ATM en la red local son de 100 Mbps llegando a nodos ruteadores que se conectan a redes Ethernet o Token-Ring.

En este sentido es que se dice que ATM en su modo local es un estándar que substituirá rápidamente a FDDI ya que no solo ofrece la misma velocidad de 100 Mbps sino claras ventajas compatibilidad en el ambiente remoto. La pelea sin embargo aún no comienza dado que FDDI lleva desde '1990 creando base instalada mientras que las primeras implementaciones de ATM local aparecieron a finales de 1993.

CAPÍTULO IV. INTERCONECTIVIDAD.

Objetivo:

Enumerar y describir los dispositivos que sirven para la comunicación entre redes WAN y LAN, sus características y formas de funcionamiento.

CAPÍTULO 4. INTERCONECTIVIDAD.

Conforme las redes de área local (LAN) van creciendo en tamaño y complejidad, y conforme las instituciones van confiando en ellas, surge la necesidad de comunicarlas entre sí ya sea en una misma ciudad o en ciudades diferentes. Así se forma lo que comúnmente se denominan como Redes de Área Amplia (WAN). Los dispositivos que se emplean para conectar las redes o los segmentos de red son conocidos como dispositivos de interconectividad (internetworking).

Los dispositivos de interconectividad están divididos en categorías de acuerdo a la capa del modelo OSI en que operan. Los repetidores operan al nivel de la capa física, los puentes trabajan a nivel de la capa de enlace de datos, los ruteadores funcionan a nivel de la capa de transporte y los servidores de intercomunicación (gateways) lo hacen generalmente en cualquiera de las capas que se encuentran arriba del nivel de red. Los equipos anteriormente descritos, son las cajas negras que nos permiten utilizar diferentes topologías y protocolos dentro de un solo sistema heterogéneo. Cada uno de estos elementos tiene ventajas y desventajas, así como aplicaciones específicas.

4.1. REPETIDORES.

Las señales analógicas y digitales que transportan información digital, solo pueden ser transmitidas a una distancia limitada antes que la atenuación o el ruido pongan en riesgo la integridad de los datos. Para

solucionar este problema un simple amplificador no es una buena alternativa, ya que su uso no solo amplificaría la señal, también lo haría con el ruido.

Dado que el repetidor trata con la reproducción de señales y la transmisión de datos, se considera un dispositivo de capa física (FIGURA 4.1). Un repetidor no incorpora ningún cambio ni analiza el direccionamiento o la estructura de los datos asociados con otras capas simplemente "reacondiciona" los datos recibidos y los transmite.

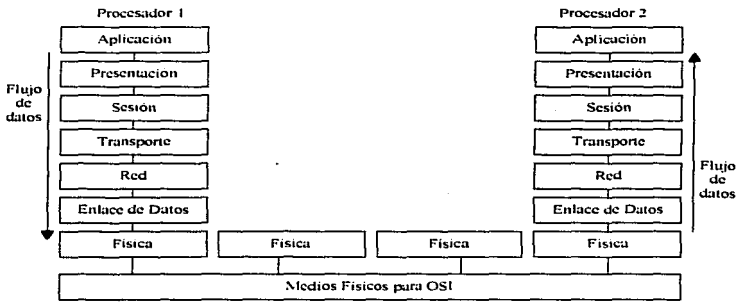


Fig. 4.1. Modelo OSI de un Repetidor.

Después de recibir y salvar los datos, reconstruye y retransmite la señal. La nueva señal es un duplicado exacto de la señal original transmitida, capaz de viajar a través de un nuevo segmento de red (un segmento, es una porción de red que no contiene dispositivos de

internetworking). Teóricamente, esta función puede ser realizada tantas veces como sea necesario. En la práctica, muchas redes limitan el número de repetidores entre una estación transmisora y una receptora.

4.2. PUENTES (BRIDGES).

Un puente se emplea para conectar dos segmentos de LAN a nivel de capa de enlace de datos (FIGURA 4.2), por lo tanto tiene acceso a la información de la dirección física de la estación. En otras palabras, puede determinar las direcciones físicas de las estaciones fuente y destino involucradas en una transferencia de datos. Una vez determinada, los puentes pueden permitir o negar el acceso a un nuevo segmento basado en dirección físicas. A diferencia de los repetidores, los puentes son selectivos con el tráfico al que le permiten circular.

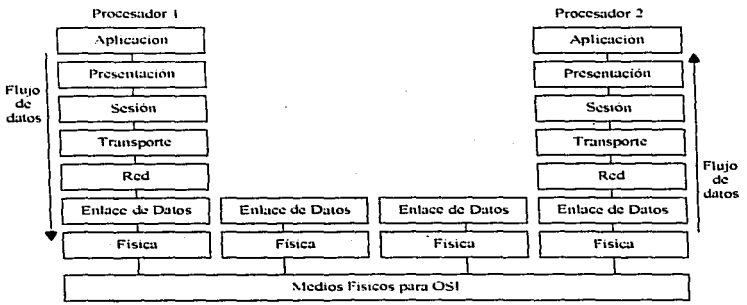


Fig. 4.2. Modelo OSI de un puente.

Como resultado de su capacidad para filtrar las direcciones de estaciones, los puentes son empleados para dividir una red con demasiado tráfico en segmentos separados, como resultado de la aplicación de ésta estrategia el tráfico por segmento efectivamente se reduce. Los puentes pueden interconectar segmentos de red a través de medios físicos distintos, como son dos Ethernet.

Existen básicamente dos tipos de puentes: transparentes (algunas veces llamados árbol expandible o SPANNING TREE) y los puentes de ruteo de origen (SOURCE ROUTING BRIDGE).

4.2.1. PUENTES TRANSPARENTES (TRANSPARENT BRIDGES).

Los puentes transparentes proporcionan interconexión de redes y/o extensión de servicios para LAN'S que utilizan protocolos idénticos al nivel de la capa física y de enlace de datos. Los puentes transparentes, no representan carga alguna para las estaciones de trabajo (nodo). Desde el punto de vista de un nodo, parecería que todas las estaciones de trabajo están residentes en una sola red extendida con cada una de ellas identificada por una dirección única de MAC.

Los puentes transparentes proporcionan tres tipos de servicios primarios.

1. Aprenden las direcciones de las estaciones contenidas en las redes conectadas al puente.

2. "Liberan" las tramas en base al conocimiento adquirido de las direcciones de las estaciones.

3. Se apoyan en el algoritmo árbol expandible para asegurar una topología libre de ciclos a través de la red extendida.

La forma en que los puentes se aprenden las direcciones de las estaciones de trabajo es observando la dirección fuente de cada trama que recibe. En la medida que estos son recibidos, construyen y actualizan una base de datos (llamada tabla de envío o forwarding) en donde listan cada dirección fuente, la conexión del puente en la qué ubicó la dirección y un valor que indica el tiempo transcurrido desde que se obtuvo dicha información.

La retransmisión de tramas la realizan de acuerdo a los datos de la tabla de envío. Esto es, cuando reciben una trama comparan su dirección destino con las direcciones que conserva en la tabla. Si éstas no coinciden, liberan la trama por todas sus conexiones (excepto aquel de donde fue recibida la trama). Esta acción de repartición múltiple (multicast) se conoce como inundación (flooding).

4.2.2. ALGORITMO DE ÁRBOL EXPANDIBLE.

El comité IEEE generó un estándar (802.1.) Aplicable a todos los puentes de nivel MAC. Gran parte de éste estándar es concerniente a la operación de puentes en ambientes topologicamente complejos en los cuales pueden existir conexiones de puentes pararelas o redundantes entre múltiples LAN's. Semejantes conexiones paralelas no pueden ser toleradas en un ambiente de puentes transparentes.

Las LAN roja y blanca están conectadas por dos puentes paralelos, Puente-1 y Puente-2. Consideramos lo que ocurrira cuando la estación-J en la red roja envía una trama a la estación-K en la red blanca. La trama originada por la estación-J y direccionada a la estación-K está lista tanto en el puente-1 como en el puente-2. Como ésta es la primer trama entre J y K, en ninguna de las tablas de envío de los puentes existe una entrada para las estaciones J y K.

Cada puente actualiza su tabla de envío para indicar que la estación-J se encuentra en la red roja, después de actualizar su respectiva tabla de envío, cada puente transmite la trama por todas sus interfaces (inunda): el puente-1 libera la trama por la interfaz 1 y el puente-2 hace lo propio por las interfaces 2 y 3 (para simplificar el ejemplo, éste último camino no se seguirá).

A continuación la estación-K recibe 2 copias de la trama originada por la estación-J. Si bien la recepción de información duplicada por una

estación generalmente no es fatal, dicha duplicidad representa un uso ineficiente del ancho de banda disponible.

La consecuencia grave resulta al duplicar tramas en los puentes 1 y 2. La trama inundada por el puente-1 en su interfaz finalmente es leída por el puente-2 en su interfaz 2, quien actualiza su tabla de envío para indicar que la estación-J se encuentra en al dirección de la red blanca.De manera similar el puente-1 lee la trama propagada por el puente-2 y también actualiza su tabla de envío en donde la estación-J estará en la dirección de la red blanca. Finalmente el resultado es que las tablas de envío de ambos puentes están corruptas y ninguno de los puentes queda en posibilidad de enviar correctamente información a la estación-J Esta corrupción es ocasionada por la existencia de rutas alternas entre nodos.

El algoritmo de árbol expandible asegura la existencia de una topología libre de enlaces redundantes en redes que contienen puentes paralelos. El algoritmo proporciona una sola ruta (compuesta de los puentes y redes de área local que intervienen) entre dos estaciones finales cualquiera de toda la red. También ofrece un alto grado de tolerancia a fallas, ya que permite la reconfiguración automática de la topología en caso de falla de un puente o una ruta.

Se requiere cinco niveles de administración por derivación de la topología árbol expandibles.

- Especificar todos los puentes de la red expandida.

- Un identificador único de red para cada puente dentro de la red expandida.
- Un identificador único de red para cada interfaz puente/LAN (llamada puerto)
- Una prioridad, especificando la prioridad relativa de cada puerto.
- Un "costo" por cada puerto.

Con esos valores asignados, los puertos difunden y procesan unas tramas especiales para obtener una topología libre de ciclos. El intercambio de estas tramas se realiza rápidamente, minimizándose el tiempo durante el cual el servicio no estará disponible entre las estaciones.

Para construir una topología libre de ciclos, los puentes primero eligen al puente raíz, el cual tendrá el mejor valor de prioridad (el menor), este puente sirve como raíz de la topología libre de enlaces redundantes. Después de determinar dicha identidad, los demás puentes calculan el costo de las rutas, esto es, el costo de la ruta al puente raíz que ofrece cada puerto del puente. Cada puente designa al puerto que ofrece el menor costo de ruta hacia el puente raíz como el puerto raíz a aquel que tenga la mejor prioridad (esto es la más baja).

En cada LAN con la extensión de la red en un puente (aquel cuyo puerto raíz tenga el costo de ruta más bajo hacia el puente raíz) es seleccionado como el puente designado. El puerto que conecta la LAN con el puente designado es seleccionado como el puerto designado.

Este proceso asegura que todos los puertos redundantes (aquellos que proporcionan conexiones paralelas) sean removidos de servicio (puestos en estado de bloqueo). En caso de un cambio topológico, o de una falla en algún puente o ruta, el algoritmo determina una nueva topología que puede mover muchos puertos del estado de bloqueo al de envío.

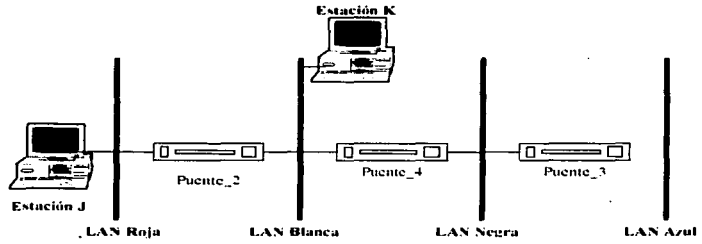


Fig. 4.3. Topología libre de Ciclos.

Tomando como referencia el ejemplo anterior (figura.4.3.), la implementación de este algoritmo podría remover del servicio el puente-1 y bloquear la interfaz-3/puente-3. El resultado proporciona una topología libre de enlaces redundantes con una sola trayectoria entre dos nodos cualesquiera como se muestra en la figura siguiente.

4.2.3. PUENTES DE RUTEO DE ORIGEN.

El término Source Routing Bridge lo utilizó por primera vez IBM para descubrir un método de puntear tramas a lo largo de las redes Token-Ring. Los puentes de ruteo de origen difieren de los puentes transparentes en dos puntos básicos:

1. Permiten tener múltiples caminos entre dos estaciones en una red extendida.

2. El ruteo de origen requiere que el punto de partida del mensaje proporcione la información necesaria para entregar la información a su destinatario. Esto implica que los puentes no necesitan mantener tablas de envío. Más bien toman la decisión de enviar o dejar un mensaje basándose solamente en los datos contenidos dentro de la trama misma. Para instrumentar este esquema cada estación determina el recorrido para llegar a su destino a través de un proceso denominado descubrimiento de ruta, el cual se puede realizar de varias maneras:

Mensaje a través de todos los caminos: Se generan múltiples tramas que circulan por todos los caminos entre las estaciones fuente y destino. Dichas tramas son llamadas exploradores de todos los caminos (APE all-path explorer). Una vez que el puente recibió una trama de exploración, asigna un indicador de ruta el cual toma la siguiente forma:

[LANi [ID-Puente [LANj , donde:

LANi.- Es un número que identifica la LAN a la cual llegó la trama de exploración.

ID-Puente.- Es un número que identifica al puente

LANj.- Es un número único que identifica la LAN a la cual la trama de exploración es enviado por el puente.

Después de colocar el indicador de ruta, cada puente dispersa la trama. En consecuencia, en la LAN pueden aparecer múltiples copias de la trama de exploración, y el receptor puede recibir múltiples copias de esta (una por cada camino a través de la red extendida). Cada trama de exploración recibida contiene una lista con una secuencia única de indicadores de ruta que muestra el camino seguido por la trama a través de la red.

Mensajes de ruteo de árbol expandible: Se genera una sola trama que sigue una ruta libre de ciclos de la fuente al destino. Cada que un puente recibe una de estas tramas la envía por todos los puertos activos excepto a aquel por donde fue recibida la trama. Con éste método, solo aparece una copia de la trama por LAN, y el receptor recibe solamente una de ellas.

Rutas específicas: Se genera una sola trama que cruza por un camino específico designado por la estación fuente. A está trama se le conoce como ruteo específico. Estas tramas contienen una lista de indicadores de ruteo con una trayectoria entre la fuente y el destino a través de la red extendida. Una vez

recibida la trama de ruteo específico cada puente examina la lista de indicaciones de ruteo, y sólo deja pasar a aquel que esté en la ruta correcta de otro modo lo ignora.

Rutas nulas: Se emplean para indicar que la fuente no desea ningún servicio de ruteo de los puentes. Como resultado, las tramas de rutas nulas son restringidas a la LAN en donde reside la estación origen.

4.3. RUTEADORES (ROUTERS)

El siguiente tipo de caja negra es el ruteador, el cual se diferencia de los puentes en que mientras éstos proporcionan servicios de conexión en la capa de enlace de datos, los ruteadores hacen lo mismo pero en la capa de red. La información de la capa 3 generalmente incluye lo que se llama un direccionamiento lógico de la red. El direccionamiento físico no es asignado por el administrador de la red, mientras que el direccionamiento lógico si lo puede ser. Esta es una diferencia importante entre un puente y un ruteador.

El administrador puede usar los direccionamientos lógicos, para asociar un grupo de equipos con alguna característica en común (por ejemplo en un área departamental de un edificio). Estas direcciones proporcionan la flexibilidad que un direccionamiento físico no tiene, sencillamente porque éstos pueden ser agrupados jerárquicamente y cambiarse más fácilmente.

Otra de las ventajas de que los ruteadores se conecten a nivel de la capa de red, es que permiten conectar LAN's de diferentes topología, siempre y cuando cuente con las interfaces necesarias para ello. Por ejemplo si se tiene una red Token-Ring corriendo bajo Netware de Novell, y una Ethernet empleando igualmente Netware, la manera más fácil de conectarlas es emplear un ruteador que tenga interfaces Ethernet y Token-Ring, además de que soporten IPX.

La función básica de un ruteador es enviar paquetes entre redes, y dado que generalmente existen más de una vía entre ellas, los ruteadores deben encontrar la mejor ruta para hacerlo. La forma de determinarlo es mediante el uso los algoritmos de ruteo, de los cuales existe una gran variedad. Los algoritmos modernos de ruteo consideran una variedad de factores, cada uno con un peso diferente. En algunos casos, se pueden cambiar pesos métricos (como el costo de la línea) para adaptarlos a necesidades propias.

Algunos de los criterios empleados para determinar cual es la mejor ruta son: costo de transmisión retraso por tránsito, congestionamiento de red o distancia entre origen y destino del mensaje. La distancia se mide por lo genera en términos de "conteos de saltos" (hop counts). Esto es el número de ruteadores existentes entre un determinado origen y destino.

Como consecuencia de lo anterior, se destaca que la función de los ruteadores es comúnmente más demandante de proceso que la de los puentes. Como resultado, sus velocidades de proceso (generalmente

medidas en paquetes procesados por segundo) no son tan altas. Por otra parte, son capaces de una selección de ruta mucho más sofisticada basada en algoritmos de ruteo.

La mayoría de los ruteadores modernos son realmente una combinación de puente y ruteador, los puentes-ruteadores (brouters) que son una especie de híbrido de ambos. Con frecuencia denominados incorrectamente ruteadores de protocolo múltiple, los brouters ofrecen muchas de las ventajas, tanto de los puentes como de los ruteadores para redes muy complejas. Los ruteadores de protocolos múltiples no contienen las ventajas de puenteo de los brouters; sencillamente permiten que los ruteadores hagan su trabajo con más de un protocolo. Los brouters pueden soportar los protocolos más populares (y sus algoritmos de ruteo) a la vez que proveen una opción para los protocolos sin soporte a la capa de red, como puede ser el tráfico SDLC o Netbios de IBM. En otras palabras, toman la decisión de si un paquete utiliza un protocolo que puede ser ruteable. De éste modo aquello que no es susceptible de rutear lo puentean (en la actualidad SDLC se puede encapsular en TCP/IP). Estos dispositivos son complicados, costosos y difíciles de instalar, pero en redes heterogéneas muy complejas, con frecuencia ofrecen la mejor solución de interconexión.

Algunos fabricantes de puentes han intentado un arreglo opuesto agregando algunas capacidades de ruteo a sus puentes. Estos equipos son comúnmente llamados puentes de ruteo. Estos pueden realizar algunas de las opciones de rutas selectivas mínimas de los ruteadores. Aunque éstos no tienen acceso a la información de la capa de red del

modelo OSI, si pueden hacer su recorrido en la misma forma que los ruteadores.

Para reconocer las distintas redes, el ruteador almacena tablas de todas las redes a las que puede conectar, especificando el número de ruteadores que se deben cruzar para alcanzarlas. Las tablas de los puentes, en cambio, almacenan las direcciones de todas las estaciones de trabajo, por lo que son mucho más grandes que las de ruteo.

Generalmente los ruteadores operan con múltiples protocolos, ya que solo necesitan reconocer las direcciones origen y destino para tomar la decisión de la ruta más optima. Si el paquete se envía a un medio distinto al origen, el ruteador cambiará el formato del paquete de acuerdo al protocolo de acceso al medio correspondiente, ya sea encapsulado (como en X.25) o fragmentado el paquete (como en el caso de Frame Relay). Esta característica no solo permite manipular varios protocolos simultáneamente sino transportarlos vía enlaces con distinto protocolo de acceso al medio (como CSMA/CD o Token-Ring), o distinto protocolo de ruteo.

4.3.1. ALGORITMOS O PROTOCOLOS DE RUTEO.

Los ruteadores mantienen bases de datos conocidas como tablas de ruteo. Estas le dicen al ruteador la ubicación de cada red con respecto a su posición en la red de redes. Cuando un ruteador recibe un paquete, está en posibilidad de enviarlo al dispositivo destino o enviarlo a través

de otro ruteador, hasta que el paquete pueda ser entregado por un ruteador físicamente conectado a la misma red que el dispositivo destino.

Este paso de un paquete de un ruteador hacia otro es comúnmente conocido como un salto. La mayoría de los algoritmos de ruteo limitan, o permiten administrar un margen en cuanto al número de saltos permitidos.

La construcción y mantenimiento de las bases de datos de ruteo es realizada generalmente por una aplicación de administración de ruteo (trabajando en capas superiores del modelo OSI y está basada en los algoritmos de ruteo).

Los protocolos de ruteo proporcionan un camino a los ruteadores para comunicarse con otros, para lo cual necesitan realizar algunas funciones específicas, como son:

- Descubrir rutas.
- Mantener lainformación de ruteo actualizada.
- Alertarse unos a otros si las rutas están congestionadas o tienen fallas.
- Indicar el costo para cada ruta.

Básicamente los algoritmos de ruteo se dividen en dos grandes grupos que son:

1. Vector de distancia
2. Estado de enlace

4.3.1.1. VECTOR DE DISTANCIA.

Los algoritmos de vector de distancia construyen sus tablas calculando las rutas hacia todas las redes basándose en la información que reciben de los ruteadores vecinos. Si un ruteador vecino informa que él puede alcanzar la red X en 3 saltos, entonces el primer ruteador asume que la puede alcanzar en 4 saltos. En caso de existir rutas duplicadas, se usa la de menor costo (generalmente medido en saltos). Es por esto que se dice que emplea información de segunda mano. Después de calcular su tabla de ruteo, la comparte con el resto de los ruteadores para que ellos a su vez construyan las propias.

Este algoritmo usa información más actualizada para elaborar sus tablas de ruteo. Cuando un ruteador recibe información actualizada, recalcula las rutas y entonces pasa la información (su nueva tabla de ruteo) a los ruteadores.

Las ventajas de usar algoritmo de vector de distancia son por que es el más estándar y fácil de implementar. El ancho de banda requerido y el uso del procesador del ruteador no es muy elevado. Fue el algoritmo de ruteo inicial y por tanto es una tecnología madura y soportada por la gran mayoría de los vendedores.

Las desventajas son el tiempo que tarda la información en difundirse a todos los ruteadores, conocido como tiempo de convergencia. Durante todo el tiempo empleado en actualizar información hacia todos los ruteadores en la red, el mecanismo de ruteo

es detenido y los paquetes tienen una mayor probabilidad de perderse o ser mal ruteados. A este fenómeno se le conoce como "conteo al infinito"

4.3.1.2. ESTADO DE ENLACE.

Los ruteadores de estado de enlace construyen sus tablas basándose en información de primera mano, y no tienen que recalcular sus rutas antes de que ocurran cambios. Esto significa que la convergencia después de un cambio de rutas es más rápido que en vector de distancia. Al igual que el ruteo de vector de distancia , el ruteo de estado de enlace selecciona las rutas con el costo más bajo.

Los ruteadores de estado de enlace aprenden su ambiente primeramente descubriendo a sus vecinos. Esto se puede hacer con un protocolo hola (hello). Esta información es enviada a sus vecinos en un paquete especial llamado paquete de estado de enlace o PEE (link-State Packet LSP). Los vecinos lo envían a las demás redes excepto aquella por donde llegó. De éste modo todos los ruteadores guardan un PEE de los demás ruteadores de la red.

La única información reportada por cada ruteador en sus PEE concierne a sus enlaces directamente conectados y sus costos. Ya que el ruteador tiene una copia de todos los ruteadores, entonces tiene las piezas para formar un mapa confiable de la red.

El ruteo de enlace de estado tiene ciertas ventajas cobre el ruteo de vector de distancia, por ejemplo:

El tiempo de convergencia del ruteo de estado de enlace es menor porque no se tiene el problema de conteo al infinito que presenta el ruteo de vector de distancia, además la información que emplean es directa, con lo que la probabilidad de error al determinar las rutas es menor. Finalmente la información acerca de la red puede ser obtenida pregúntandole solo a un ruteador. Todos los ruteadores guardan una copia de todos los PEE's.

La principal desventaja (y no es muy significativa), es que una implementación incorrecta puede causar que un ruteador envíe continuamente PEE's, y el efecto de inundación (flooding) podría causar suficiente tráfico como para perjudicar a la red.

4.4. SERVIDOR DE INTERCOMUNICACION (GATEWAY)

Los servidores de intercomunicación generalmente son más lentos que un puente o un ruteador, ya que como se menciono al principio de éste capítulo trabajan en las capas que se localizan arriba del nivel de red. Un gateway es una combinación de software y hardware (usualmente una PC 386, 486 o mayor) el cual cuenta con su propio procesador y memoria los cuales emplea para realizar la conversión de protocolos.

Los Servidores de Intercomunicación ofrecen el mejor método para conectar segmentos de red y redes a computadoras centrales (mainframes). Se selecciona un gateway cuando se tienen que interconectar sistemas que se construyeron totalmente con base en diferentes arquitecturas de comunicación. Generalmente estos equipos trabajan en las capas superiores del modelo OSI.

Un gateway es la solución para compartir información y recursos remotos. Comunican redes locales a otros recursos (mainframes, servicios de información, bases de datos públicas, otras redes locales etc.), y crean una red de área amplia en el proceso. La interconexión es por lo general trasparente para el usuario final, lo que permite que la información fluya libremente a través de la red WAN.

La función de un gateway es proporcionar el acceso de los usuarios de una red local a un mainframe por medio de la emulación de terminales. Existen dos géneros de gateways que dependen del protocolo que se emplee en el computador central. El primero, es para accesar equipos IBM, con protocolos SNA. El segundo es para accesar equipos que utilicen protocolos propietarios o ISO/ASCII, como HP, Tanderm, Unisys y DEC.

En el mundo IBM, se aplica el concepto Arquitectura de Redes de Sistemas (SNA System Network Arquitecutre), para el acceso a redes locales, esto se logra a través de un gateway 3270 o 5250 (que depende del modelo del mainframe) y Comunicación avanzada a programa. (APPC, Advanced Program to Program Communication).

El gateway elimina la necesidad de tener una línea dedicada para cada PC de la red ya que este permite que con solo una línea dedicada todos los usuarios de la red local accesen al mainframe. Diferentes tipos de protocolos se pueden aprovechar en esta línea, como SDLC, X.25 (QLLC), Token-Ring o Ethernet.

Para satisfacer los requisitos de conectividad a diferentes plataformas un gateway de red local, debe ofrecer la capacidad de acceso a numerosos y diferentes sistemas de información.

La tecnología Packet-Switching X.25 TCP/IP, a diferencia de otras, permite el acceso a múltiples usuarios a múltiples destinos empleando múltiples protocolos. Esto significa, que con solo enlace X.25 o TCP/IP el gateway en una red local hace posible el acceso a múltiples destinos, donde cada destino utiliza un protocolo diferente a los demás.

Por ejemplo, con una sola conexión física, los usuarios de una red local pueden accesar simultáneamente a un mainframe IBM, un AS/400, un HP9000, una Tandem, un Unisys y una o varias redes locales. Cada usuario de la red tiene la libertad de escoger uno o varios destinos donde se encuentre la información que requiere. Esto es posible, gracias al soporte de múltiples circuitos virtuales, cada uno capaz de llevar simultáneamente diferentes comunicaciones.

CONCLUSIONES

Durante los últimos años la estructura de las redes ha evolucionado en forma notable. Las soluciones de computo centralizadas y basadas en un solo proveedor ya son cosas del pasado; la gran mayoría de las redes de la actualidad se basan en el cómputo de Cliente-Servidor, con los datos y las aplicaciones distribuidas en diversos sistemas esparcidos por la red.

A medida que las computadoras de escritorio interconectadas en redes locales se hacen más potentes, los archivos que intercambian se hacen más grandes por lo que demandan mayores anchos de banda dentro de las redes conocidas como LAN's que atienden a una o varias oficinas en el mismo edificio a velocidades de 10 Mbps o más.

Las redes de voz convencionales nunca han sido lo ideal para el transporte de tráfico que no sea de voz, tales como la interconexión de redes locales o la transferencia de archivos entre centros de computo que requieren grandes cantidades de ancho de banda por periodos relativamente largos (la duración de las llamadas).

Como alternativa, los transportistas de información (carriers) y los usuarios privados han instalado redes separadas de paquetes para proporcionar anchos de banda sobre pedido. No obstante, en su forma tradicional esta tecnología tiene capacidades limitadas.

De la misma manera que en todo el mundo, en México la modernización de las redes de datos es inminente. En este momento el panorama demuestra que la mayoría de las redes geográficamente distribuidas utilizan tecnología X.25, o bien de ruteadores multiprotocolos y puentes. No obstante, se ha iniciado rápidamente la instalación de plataformas Frame Relay y ATM en redes públicas y privadas.

El número de redes locales interconectadas está creciendo 35% anualmente y el tráfico que sale de cada red local a una red de área amplia llega a crecer 30% al año.

Con demandas adicionales de redes locales con tecnología de fibra óptica que operan a 100 Mbps, pronto existirá una necesidad de nuevas redes de área amplia con altas capacidades y bajos retrasos para interconectar redes de área local.

Actualmente, empiezan a aparecer las redes públicas que ofrecen servicios de transmisión de datos a mayores velocidades como tecnologías Frame Relay y ATM. Por lo que se puede esperar que gradualmente se conviertan en redes internacionales.

Las tecnologías que más se han empleado en México para interconectar redes de datos son X.25 (46.67%), ruteadores multiprotocolos (21.7%) y puentes (20.0%) figura c.1. Por otro lado el servicio de transmisión de datos esta siendo atendido principalmente a través de redes públicas o redes privadas que utilizan como medio de

transmisión líneas digitales rentadas a Telmex o frecuencias satelitales arrendadas a Telecom.

Según estadísticas realizadas en nuestro país en 1995 existe un alto nivel de integración de redes de área local y de área amplia principalmente entre los grandes usuarios:

- El 95.5% de las grandes empresas cuentan con redes de área local (LAN's)
- De las redes instaladas en toda la República, el 42% se encuentran conectadas entre si formando una red de área amplia (WAN).

En la mayoría de los negocios las redes se han convertido en algo crítico para la misión esto quiere decir, la misión principal de las empresas confían en la red, si la red falla la compañía no podría cumplir con su misión. Para muchas compañías que tienen una clara visión la red es un recurso estratégico; es una fuente de ventaja competitiva. Bien desarrollada, la red puede ser la ventaja del negocio sobre sus competidores.

BIBLIOGRAFÍA

Redes de Area Local, la Siguiente Generación
Thomas W. Madron
Ed. Megabyte y Grupo Noriega

Bussines Data Communications
Davis A. Stamper
The Benjamin/Cummins Publishing, Third Edition

Enterprise Series Connectivity: Local Area Networks
Drew Heywood, John Jerney
New Riders Publishing

Redes de Comunicaciones
José Manuel Huidobro
Ed. Paraninfo

Data Communications, Computer Networks and Open Systems
Fred Halsall
Ed. Addison-Wesley, Third Edition

Future Trens in Telecommunications
R.J Horrocks, R. W. A. Scarr
Ed. Willey

Revista RED año III numero 19
Gateways de redes de área local
Como Funcionan las Herramientas de conectividad avanzada

Revista RED Edition Especial
El ABC de las Redes locales
Dispositivos para armar Redes de Area Amplia

Wellfleet Configuration Guide
Volumen I
Wellfleet Communications Inc. 1992

FN/LN/CN Operations Management
Wellfleet Communications Inc. 1992

Networking Technologies
Novell Netware

Seminario de Interconectividad Avanzada
Intersys

Fundamentals of Internetworking, Desing and Management
Novell Netware