# CAPÍTULO I.

# HISTORIA DE LA INTERCONECTIVIDAD DE REDES

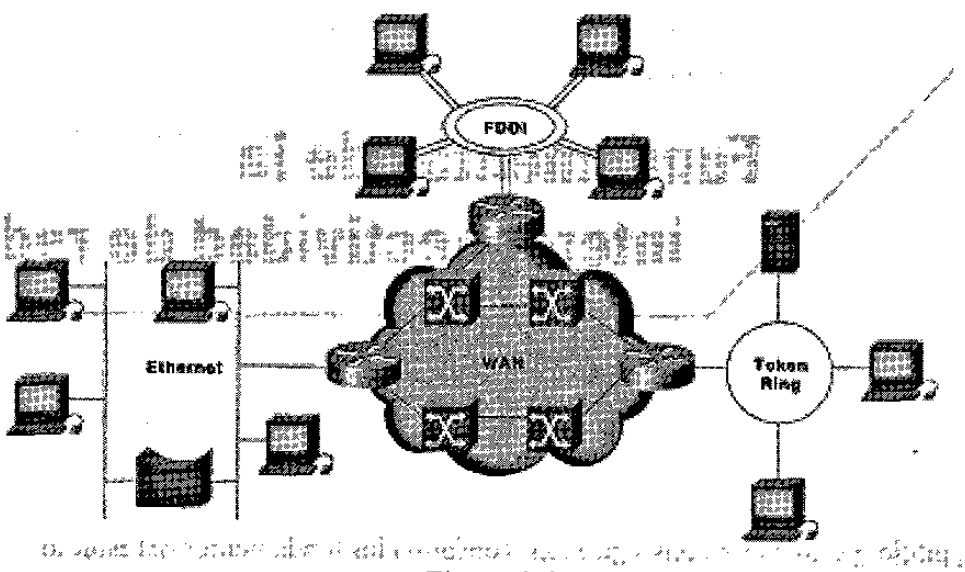



Figura 1-1

Las primeras redes fueron redes de tiempo compartido que utilizaban mainframes y terminales conectadas. Dichos entornos se implementaban con la SNA (Arquitectura de Sistemas de Redes) de IBM y la arquitectura de red de Digital.

Las LANs (Redes de Área Local) surgieron a partir de la revolución de la PC. Las LANs permitieron que varios usuarios ubicados en un área geográfica relativamente pequeña pudiera intercambiar mensajes y archivos, y tener acceso a recursos compartidos como los servidores de archivos.

Las WANs (Redes de Área Amplia) interconectan LANs por medio de líneas telefónicas normales (y otros medios de transmisión) y de esta manera interconectan a usuarios geográficamente dispersos.

Hoy en día se utilizan cada vez más las LANs de alta velocidad y las interredes conmutadas, sobre todo porque operan a velocidades muy altas y soportan aplicaciones de gran ancho de banda como voz y video conferencia.

La tecnología de interconectividad de redes surgió como una solución a tres problemas: LANs aisladas, duplicación de recursos y falta de administración de recursos. Las LANs aisladas imposibilitaban la comunicación electrónica entre diferentes oficinas o departamentos. La duplicación de recursos significaba que se debía suministrar el mismo hardware y software a cada departamento y oficina, así como tener grupos de soporte separados. Esta falta de administración de red provocó que no hubiera un método centralizado para administrar y reparar las redes.

## EL MODELO DE REFERENCIA OSI

OSI (Interconexión de Sistemas Abiertos), conocido como modelo de referencia OSI, describe cómo se transfiere la información desde una aplicación de software en una computadora a través del medio de transmisión hasta una aplicación de software en otra computadora. OSI es un modelo conceptual compuesto de siete capas; en cada una de ellas se especifican funciones de red particulares. Fue desarrollado por la ISO (Organización Internacional de Estándares) en 1984, y actualmente se considera el modelo principal de arquitectura para la comunicación entre computadoras. OSI divide las funciones implicadas en la transferencia de información entre computadoras de red,

en siete grupos de tareas más pequeñas y fáciles de manejar. A cada una de las siete capas se asigna una tarea o grupo de tareas. Cada capa es razonablemente individual, por lo que las tareas asignadas a cada capa se pueden implementar de manera independiente. Esto permite que las soluciones ofrecidas por una capa se puedan actualizar sin afectar a las demás. La lista siguiente detalla las siete capas del modelo OSI:

- CAPA 7 - Capa de aplicación
- CAPA 6 – Capa de presentación
- CAPA 5 – Capa de sesión
- CAPA 4 – Capa de transporte
- CAPA 3 – Capa de red
- CAPA 2 – Capa de enlace de datos
- CAPA 1 – Capa física

La figura 1-2 ilustra el modelo de referencia OSI de siete capas.

## CARACTERÍSTICAS DE LAS CAPAS OSI

Las siete capas del modelo de referencia OSI se pueden dividir en dos categorías: capas superiores y capas inferiores.

Las capas superiores del modelo OSI tienen que ver con la aplicación y en general están implementadas sólo en software. La capa superior, la de aplicación, es la más cercana al usuario final. Tanto los usuarios como los procesos de la capa de aplicación interactúan con aplicaciones de software que contienen un componente de comunicación. El término capa superior se usa a veces para referirse a cualquier capa que esté sobre otra capa en el modelo OSI.

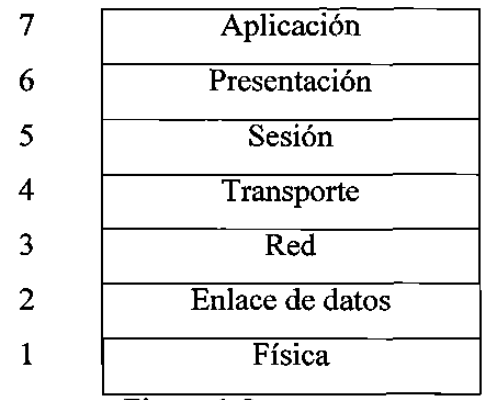



Figura 1-2

Las capas inferiores del modelo OSI manejan lo concerniente a la transferencia de datos. Las capas físicas y de enlace de datos se encuentran implementadas en hardware y software. En general las otras capas inferiores están implementadas únicamente en software. La capa inferior, la física, que es la más cercana al medio de transmisión de la red física (el cableado de la red, por ejemplo), es la responsable de colocar la información en el medio de transmisión.

La figura 1-3 ilustra la división entre las capas superiores e inferiores del modelo OSI.

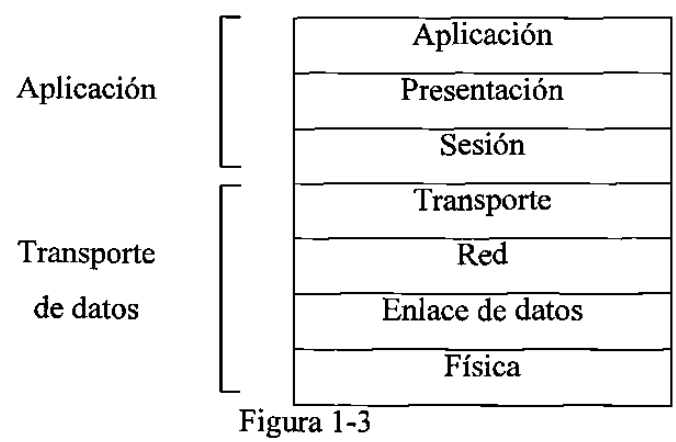



Figura 1-3

## PROTOCOLOS

El modelo OSI proporciona un marco conceptual para la comunicación entre computadoras, pero el modelo en sí mismo no es un método de comunicación. La comunicación real se hace posible al utilizar protocolos de comunicación. En el contexto de la tecnología de redes de datos, un protocolo es un conjunto formal de reglas y convenciones que gobierna el modo en que las computadoras intercambian información por un medio de transmisión de red. Un protocolo implementa las funciones de una o más capas del modelo OSI. Hay una gran variedad de protocolos, pero todos tienden a estar en uno de los grupos siguientes: protocolos LAN, protocolos WAN, protocolos de red y protocolos de ruteo. Los protocolos LAN operan en las capas física y de enlace de datos del modelo OSI y definen la comunicación a través de los diferentes medios de transmisión. Los protocolos WAN operan en las tres capas inferiores del modelo OSI y definen la comunicación a través de los diferentes medios de transmisión de área amplia. Los protocolos de ruteo son protocolos de la capa de red responsables de la determinación de la trayectoria y la conmutación del tráfico. Finalmente, los protocolos de red son los diferentes protocolos de las capas superiores que están en un grupo determinado de protocolos.

## EL MODELO OSI Y LA COMUNICACIÓN ENTRE SISTEMAS

La información que se transfiere de una aplicación en software en un sistema de computadoras a una aplicación en software en otra, debe pasar a través de cada una de las capas del modelo OSI. Si, por ejemplo, una aplicación en software en el Sistema A tiene información para transmitir a una aplicación en su información a la capa de aplicación (Capa 7) del Sistema A. Ésta, entonces, transferirá la información a la capa de presentación (Capa 6), la cual transferirá la información a la capa de sesión (Capa 5), y así sucesivamente hasta la capa física (Capa 1). En esta última, la información se coloca en el medio de transmisión de red física y se envía al Sistema B. La Capa física del Sistema B quita la información del medio físico y, posteriormente, su capa física transfiere la información hasta la capa de enlace de datos (Capa 2), que la transfiere

hacia la capa de red (Capa 3), y así sucesivamente hasta que la información llega a la capa de aplicación (Capa 7) del Sistema B. Finalmente, esta última capa transfiere la información al programa de aplicación receptor para completar el proceso de comunicación.

## INTERACCIÓN ENTRE LAS CAPAS DEL MODELO OSI

Por lo general una capa determinada del modelo OSI se comunica con otras tres capas OSI: la capa ubicada directamente sobre ella, la capa ubicada directamente debajo de ella y su capa equivalente en otro sistema de computadoras en red. Por ejemplo, la capa de enlace de datos del Sistema A se comunica con la capa de red y con la capa física del Sistema A y, además, con la capa de enlace de datos en el Sistema B. La figura 1-4 ilustra este ejemplo.

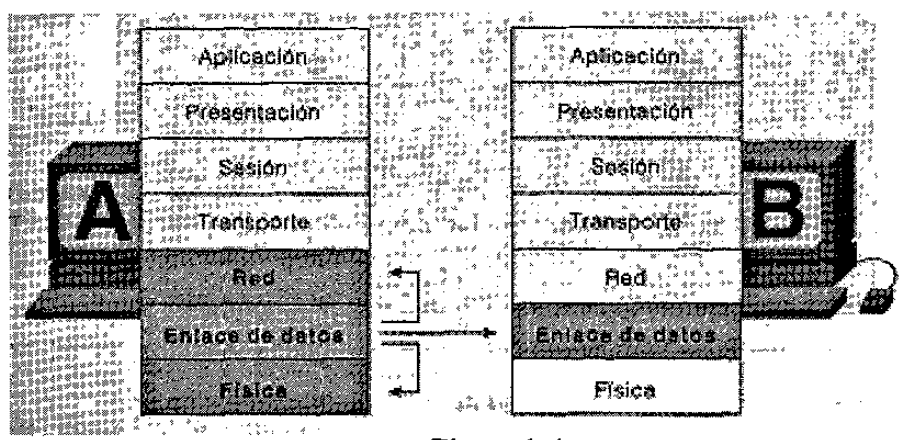



Figura 1-4

## SERVICIOS DE LAS CAPAS DEL MODELO OSI

Una capa OSI se comunica con otra para usar los servicios de la segunda capa. Los servicios proporcionados por capas adyacentes ayudan a una determinada capa del modelo OSI a comunicarse con su equivalente en otros sistemas de computadoras. Hay tres elementos básicos en los servicios de las capas: el usuario del servicio, el proveedor del servicio y el SAP (Punto de Acceso al Servicio).

En este contexto, el usuario del servicio es la capa OSI que requiere servicios de una capa OSI adyacente. El proveedor del servicio es la capa OSI que proporciona servicios a los usuarios. Las capas OSI pueden proporcionar servicios a múltiples usuarios. El SAP es una ubicación conceptual en la que una capa OSI puede solicitar los servicios de otra capa OSI.

La figura 1-5 ilustra cómo estos tres elementos interactúan en las capas de red y de enlace de datos.

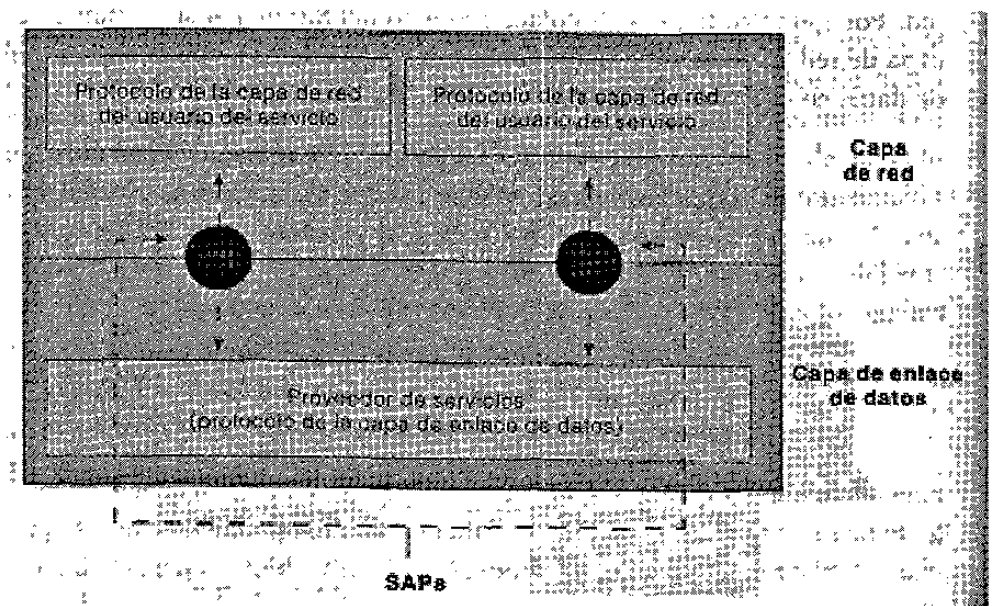



Figura 1-5

## EL MODELO OSI Y EL INTERCAMBIO DE INFORMACIÓN

Las siete capas del modelo OSI utilizan varias formas de información de control para comunicarse con sus capas equivalentes en otros sistemas de computadoras. Esta información de control consta de solicitudes e instrucciones específicas que se intercambian entre capas OSI equivalentes.

De hecho, la información de control toma una de dos formas: encabezados y finalizadores. Los encabezados se agregan al principio de los datos que se han enviado hacia abajo desde las capas superiores. Los finalizadores son añadidos al final de los datos enviados hacia abajo desde las capas superiores. No se requiere una capa OSI para colocar un encabezado o finalizador a los datos de las capas superiores.

Encabezados, finalizadores y datos son conceptos relativos, según la capa que analiza la unidad de información. En la capa de red, una unidad de información, por ejemplo, consta de un encabezado y datos de la Capa 3. En la capa de enlace de datos, sin embargo, a toda la información transferida hacia abajo por la capa de red (el encabezado y los datos de la Capa 3) se le da tratamiento de datos.

En otras palabras, la porción de datos de una unidad de información en una capa OSI determinada puede, potencialmente, contener encabezados, finalizadores y datos de todas las capas superiores. A esto se le conoce como encapsulamiento. La figura 1-6 muestra cómo se encapsulan el encabezado y los datos de una capa en el encabezado de la capa adyacente inferior.

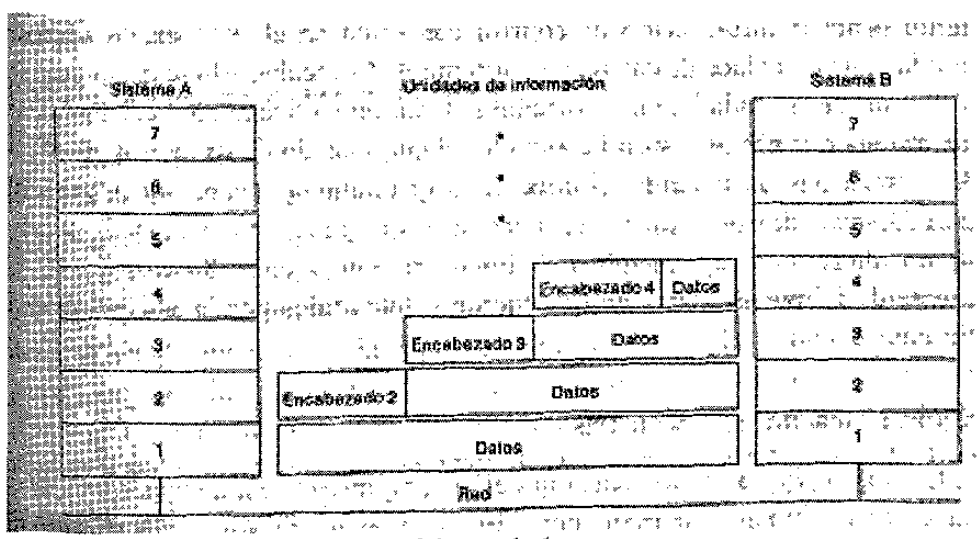



Figura 1-6

# PROCESO DE INTERCAMBIO DE INFORMACIÓN

Este proceso ocurre entre capas OSI equivalentes. Cada capa en el sistema fuente agrega información de control a los datos y cada capa en el sistema de destino analiza y quita la información de control de datos.

Si el Sistema A tiene datos de una aplicación de software para enviar al Sistema B, los datos se transfieren a una capa de aplicación. La capa de aplicación en el Sistema A transfiere entonces cualquier información e control que requiera la capa de aplicación del Sistema B pero antes agrega un encabezado a los datos. La unidad de información resultante (un encabezado y los datos) se transfiere a la capa de presentación, la cual agrega antes su propio encabezado que contiene información de control destinada a la capa de presentación del Sistema B. La unidad de información aumenta en tamaño a medida que cada capa agrega su propio encabezado (y, en algunos casos, un finalizador) que contiene información de control que será utilizada por su capa equivalente en el Sistema B. En la capa física, la unidad de información completa se coloca en el medio de transmisión de la red.

La capa física en el Sistema B recibe la unidad de información y la transfiere a la capa de enlace de datos. La capa de enlace de datos en el Sistema B lee posteriormente la información de control contenida en el encabezado agregado por la capa de enlace de datos en el Sistema A. El encabezado se quita después, y el resto de la unidad de información se transfiere a la capa de red. Cada capa realiza las mismas acciones: La capa lee el encabezado de su capa equivalente, lo retira, y pasa la unidad de información resultante a la capa adyacente superior. Después de que la capa de aplicación lleva a cabo estas acciones, los datos se transfieren a la aplicación de software receptora en el Sistema B, exactamente de la misma forma en que fueron transmitidos por la aplicación en el Sistema A.

# CAPA FÍSICA DEL MODELO OSI

Esta capa define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de redes de comunicaciones. Las especificaciones de la capa física definen características como niveles de voltaje, temporización de cambios de voltaje, velocidades de transferencia de información, distancias máximas de transmisión y como especificaciones LAN o WAN. La figura 1-7 ilustra algunas implementaciones comunes de la capa física en redes LAN y WAN.

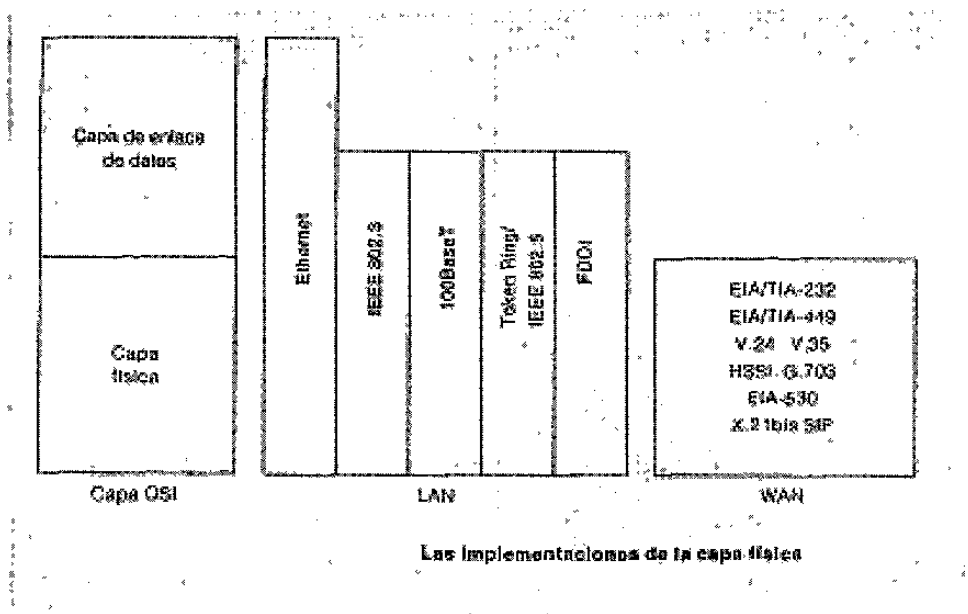



Figura 1-7

# CAPA DE ENLACE DE DATOS DEL MODELO OSI

Proporciona el tránsito confiable de datos a través del enlace de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes características de re y protocolo, incluyendo el direccionamiento físico, la topología de red, la notificación de error, la secuencia de tramas y el control de flujo. El direccionamiento físico (a diferencia del direccionamiento de red), define cómo se nombran los dispositivos en la capa de enlace de datos. La topología de red consiste en especificaciones de la capa de

enlace de datos, que con frecuencia definen la forma en que se conectarán físicamente los dispositivos, en topología bus o en topología anillo. La notificación de error alerta a los protocolos de las capas superiores cuando se presenta un error en la transmisión y la secuencia de tramas de datos reordena las que se han transmitido fuera de secuencia. Finalmente, el control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con más tráfico del que pueda manejar simultáneamente.

El IEEE (Instituto de Ingenieros en Electrónica y Electricidad) ha subdividido la capa de enlace de datos en dos subcapas: LLC (Control de Enlace Lógico) y MAC (Control de Acceso a Medios). La figura 1-8 ilustra las subcapas IEEE de la capa de enlace de datos.

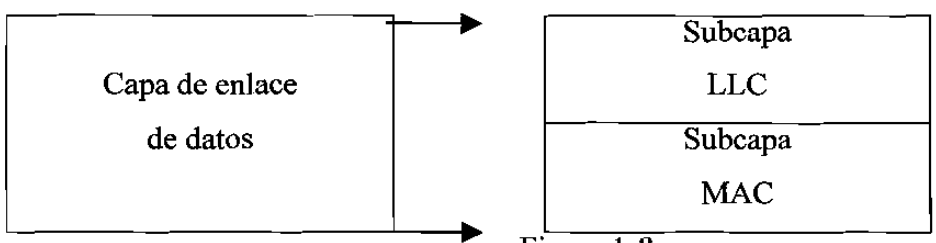



Figura 1-8

La subcapa LLC de la capa de enlace de datos administra las comunicaciones entre los dispositivos unidos por un enlace individual de red. La subcapa LLC está definida en la especificación IEEE 802.2 y soporta los servicios orientados y no orientados a la conexión, utilizados por los protocolos de las capas superiores. El IEEE 802.2 define varios campos en las tramas de la capa de enlace de datos que permiten que varios protocolos de las capas superiores compartan un solo enlace físico de datos. La subcapa MAC de la capa de enlace de datos administra el protocolo de acceso al medio de transmisión físico de la red. La especificación IEEE MAC define las direcciones MAC, las cuales permiten a múltiples dispositivos identificarse de manera única entre sí en la capa de enlace de datos.

## CAPA DE RED DEL MODELO OSI

Esta capa proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos combinarse en una red. Esto se logra a través del direccionamiento lógico (como opuesto al direccionamiento físico) de los dispositivos. La capa de red soporta servicios orientados y no orientados a la conexión de los protocolos de las capas superiores. Los protocolos de la capa de red son de hecho protocolos de ruteo, sin embargo también otro tipo de protocolos están implementados en la capa de red.

Algunos protocolos comunes de ruteo son el BGP (Protocolo de Puerta de enlace Fronteriza), un protocolo de ruteo entre dominios de Internet; el protocolo de compuerta interior OSPF (Algoritmo Abierto de Primero la Trayectoria Más Corta), basado en estado de enlaces y desarrollado para utilizarse en redes TCP/IP y el RIP (Protocolo de Información de Ruteo), un protocolo de ruteo de Internet que utiliza conteo de saltos como su métrica.

## CAPA DE TRANSPORTE DEL MODELO OSI

Implementa servicios confiables de datos entre redes, transparentes a las capas superiores. Entre las funciones habituales de la capa de transporte se cuentan el control de flujo, el multiplexaje, la administración de circuitos virtuales y la verificación y recuperación de errores.

El control de flujo administra la transmisión de datos entre dispositivos para que el dispositivo transmisor no envíe más datos de los que pueda procesar el dispositivo receptor. El multiplexaje permite que los datos de diferentes aplicaciones sean transmitidos en un enlace físico único. Es la capa de transporte la que establece, mantiene y termina los circuitos virtuales. La verificación de errores implica la creación de varios mecanismos para detectar los errores en la transmisión, en tanto que la recuperación de errores implica realizar una acción, como solicitar la retransmisión de los datos para resolver cualquier error que pudiera ocurrir.

Algunas implementaciones de la capa de transporte incluyen el protocolo de control de transmisión, el protocolo de enlace de nombres y protocolos de transporte del estándar OSI. TCP (Protocolo de Control de Transmisión) es el protocolo en el conjunto TCP/IP que proporciona una transmisión confiable de datos. NBP (Protocolo de Enlace de Nombres) es el protocolo que asocia nombres Apple Talk con direcciones. Los protocolos de transporte OSI son una serie de protocolos de transporte en el grupo de protocolos OSI.

## CAPA DE SESIÓN DEL MODELO OSI

Establece, administra y finaliza las sesiones de comunicación entre las entidades de la capa de presentación. Las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red. Estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión. Algunos ejemplos de implementaciones de la capa de sesión incluyen a ZIP (Protocolo de Información de Zona), el protocolo de Apple Talk que coordina el proceso de enlace de nombres y a SCP (Protocolo de Control de Sesión), que es el protocolo de la capa de sesión de DECnet Fase IV.

## CAPA DE PRESENTACIÓN DEL MODELO OSI

Brinda una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema, sea legible por la capa de aplicación de otro sistema. Algunos ejemplos de esquemas de codificación y conversión de la capa de presentación incluyen formatos de representación de datos comunes, esquemas de comprensión de datos comunes y esquemas de encriptación de datos comunes.

Los formatos de presentación de datos comunes o el uso de formatos estándares de video, sonido e imagen, permiten el intercambio de datos de aplicación entre diferentes

tipos de sistemas de computadoras. Los esquemas de conversión se utilizan para intercambiar información entre sistemas utilizando diferentes representaciones de texto y datos, como EBCDIC y ASCII. Los esquemas estándar de compresión de datos permiten que los datos que se comprimen en el dispositivo fuente se puedan descomprimir adecuadamente en el destino. Los esquemas estándar de encriptación de datos permiten que los datos encriptados en el dispositivo fuente sean descifrados de manera adecuada en el destino.

Las implementaciones en la capa de presentación no suelen estar asociadas a un grupo particular de protocolos. Algunos estándares bien conocidos para video son QuickTime y MPEG. QuickTime es una especificación de computadoras Apple para video y audio y MPEG es un estándar de compresión y codificación de video.

Entre los formatos de imágenes gráficas bien conocidos están GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group) y TIFF (Tagged Image File Format). GIF es un estándar para comprimir y codificar imágenes gráficas. JPEG es otro estándar de compresión y codificación para imágenes gráficas y TIFF es un formato estándar de codificación para imágenes gráficas.

## CAPA DE APLICACIÓN DEL MODELO OSI

Ésta es la capa de OSI más cercana al usuario final, lo cual significa que tanto la capa de aplicación de OSI como el usuario interactúan de manera directa con la aplicación de software.

Esta capa interactúa con las aplicaciones de software que implementan un componente de comunicación. Dichos programas de aplicación están fuera del alcance del modelo OSI. Las funciones de la capa de aplicación incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de recursos y la sincronización de la comunicación.

Al identificar socios de comunicación, la capa de aplicación determina su identidad y disponibilidad para una aplicación que debe transmitir datos. Cuando se está determinando la disponibilidad de recursos, la capa de aplicación debe decidir si hay suficientes recursos en la red para la comunicación que se está solicitando. Al sincronizar la comunicación, toda comunicación entre aplicaciones requiere cooperación, y ésta es administrada por la capa de aplicación.

Hay dos tipos clave de implementaciones de la capa de aplicación: las aplicaciones TCP/IP y las aplicaciones OSI. Las primeras son protocolos, como Telnet, FTP(Protocolo de Transferencia de Archivos) y SMTP (Protocolo de Transferencia de Correo Simple); éstos forman parte del grupo de protocolos de Internet. Las aplicaciones OSI son protocolos, como FTAM (Transferencia, Acceso y Administración de Archivos), VTP (Protocolo de Terminal Virtual) y CMIP (Protocolo Común de Información de la Administración), que pertenecen al conjunto OSI.

## FORMATOS DE INFORMACIÓN

Los datos y la información de control que se transmite a través de las redes puede tomar varias formas. Los términos para hacer referencia a estos formatos de información en la industria de la interconectividad no se utilizan de manera consistente sino intercambiable. Trama, paquete, datagrama, segmento, mensaje, celda y unidad de datos, pertenecen a los formatos comunes de información.

Una trama es una unidad de información cuyo origen y destino son entidades de la capa de enlace de datos. Una trama está compuesta por el encabezado de la capa de enlace de datos (y, posiblemente, un finalizador) y los datos de la capa superior. El encabezado y el finalizador contienen información de control para la entidad de la capa de enlace de datos en el sistema de destino. Los datos de las entidades de las capa superiores se encapsulan en el encabezado y el finalizador de la capa de enlace de datos. La figura 1-9 ilustra los componentes básicos de la trama de la capa de enlace de datos.

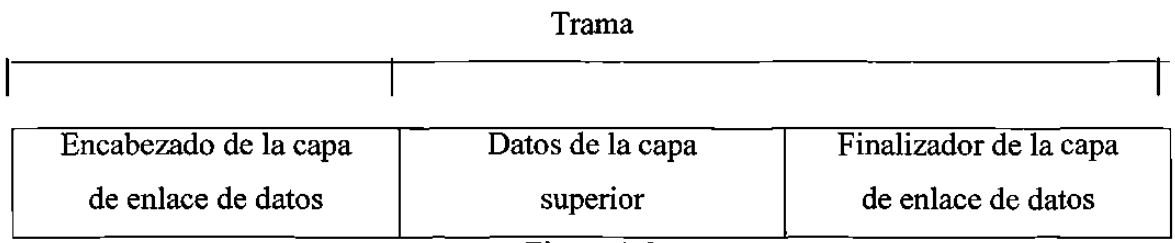



Figura 1-9

Un paquete es una unidad de información cuyo origen y destino son entidades de la capa de red. Un paquete se compone de un encabezado de la capa de red (y, posiblemente un finalizador) y datos de la capa superior. El encabezado y el finalizador contienen información de control para la entidad de la capa de red en el sistema de destino. Los datos de las entidades de la capa superior están encapsulados en el encabezado y el finalizador de la capa de red. La figura 1-10 muestra los componentes básicos de un paquete de la capa de red.

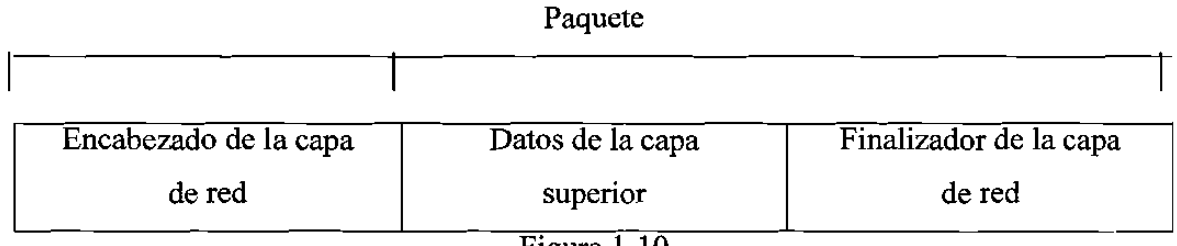



Figura 1-10

El término datagrama, por lo general, se refiere a una unidad de información cuyo origen y destino son entidades de la capa de red que utilizan servicios de red no orientados a la conexión.

El término segmento, en general, se refiere a una unidad de información cuyo origen y destino son entidades de la capa de transporte.

Un mensaje es una unidad e información cuyas entidades origen y destino están sobre la capa de red (a menudo, en la capa de aplicación).

Una celda es una unidad de información de tamaño fijo cuyo origen y destino son las entidades de la capa de enlace de datos. Las celdas se utilizan en entornos conmutados, como son las redes ATM (Modelo de Transferencia Asíncrona) y las redes de SMDS (Servicio de Datos Conmutados a Velocidades de Megabits). Una celda se compone de un encabezado e información útil. El encabezado contiene la información de control para la entidad de destino de la capa de enlace de datos y tiene 5 bytes de longitud. La información útil contiene datos de la capa superior que está encapsulada en el encabezado de la celda y suele tener una longitud de 48 bytes.

La longitud de los campos encabezado e información útil siempre es exactamente la misma para cada celda. La figura 1.11 muestra los componentes de una celda.

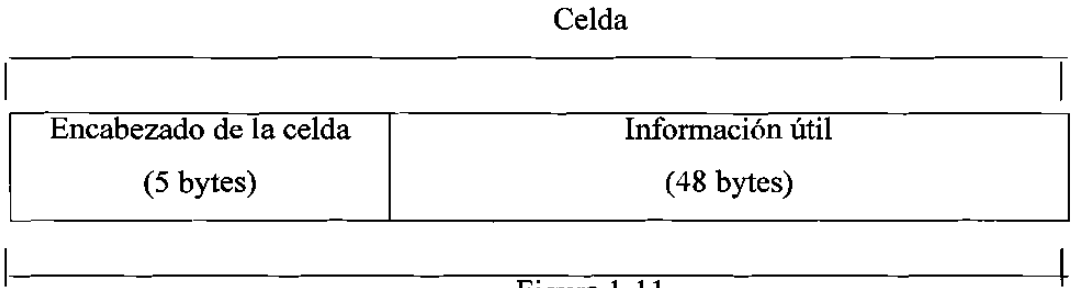



Figura 1-11

Una unidad de datos es un término genérico que se refiere a varias unidades de información. Algunas de las unidades de datos que más se utilizan son las SDUs (Unidades de Datos de Servicio), las unidades de datos de protocolo y las BPDUs (Unidades de Datos de Protocolos de Puente). Las SDUs son unidades de información de los protocolos de las capas superiores que definen una solicitud de servicio a un protocolo de capas inferiores. El PDU es un término dentro de OSI que se utiliza para describir un paquete. Los BPDUs son utilizados como mensajes Hello por el algoritmo del árbol de recubrimiento.

# JERARQUÍA ISO PARA LAS REDES

Las redes grandes suelen estar organizadas en forma jerárquica. Una organización jerárquica presenta varias ventajas, como facilidad de administración, flexibilidad y la reducción del tráfico innecesario. Por lo tanto, la ISO (Organización Internacional de Estándares), ha adoptado varias convenciones para referirse a las entidades de red. Los siguiente son algunos términos clave que se definen en esta sección: ES (Sistema Terminal), IS (Sistema Intermedio), área y AS (Sistema Autónomo).

Un ES es un dispositivo de red que no realiza un ruteo u otras funciones de direccionamiento de tráfico. Los ESs comunes incluyen dispositivos como terminales, computadoras personales e impresoras. Un IS es un dispositivo de red que rutea y efectúa otras funciones de direccionamiento de tráfico. Los ISs incluyen dispositivos como ruteadores, switches y puentes. Hay dos tipos de redes IS: IS interdominio e IS intradominio. Un IS intradominio se comunica dentro de un solo sistema autónomo, en tanto que un IS interdominio se comunica dentro y entre sistemas autónomos. Un área es un grupo lógico de segmentos de red y sus dispositivos conectados. Las áreas son subdivisiones de los sistemas autónomos. Un AS es un conjunto de redes que está bajo una administración común que comparte una estrategia de ruteo. Los sistemas autónomos se subdividen en áreas y, a veces, a un AS se le llama dominio. La figura 1-12 muestra una red jerárquica y sus componentes.

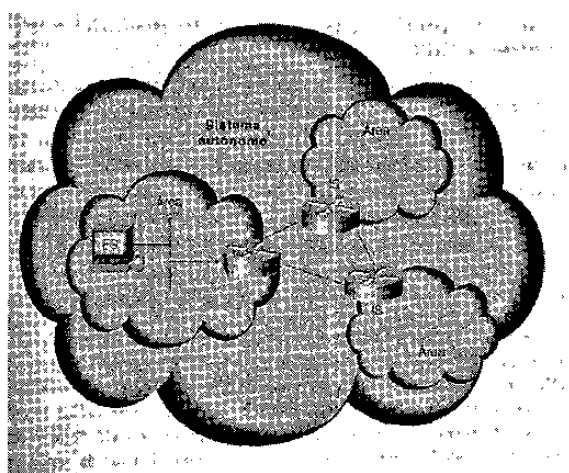



Figura 1-12

# SERVICIOS DE RED ORIENTADOS Y NO ORIENTADOS A LA CONEXIÓN

En general, los protocolos de conectividad de redes y el tráfico de datos que soportan se pueden caracterizar como orientados o no orientados a la conexión. En pocas palabras, el manejo de datos orientados a la conexión implica el uso de una trayectoria específica que se establece durante el tiempo que dura la conexión. El manejo de datos no orientado a la conexión implica la transferencia de datos a través de una conexión establecida en forma permanente.

El servicio orientado a la conexión tiene tres fases: el establecimiento de la conexión, la transferencia de datos y la terminación de la conexión.

Durante la fase del establecimiento de la conexión, se determina una sola trayectoria entre los sistemas origen y destino. De hecho, los recursos de la red se reservan en este momento para asegurar un grado de servicio constante, es decir, un rendimiento eficiente total garantizado.

En la fase de transferencia de datos, los datos se transmiten en forma de secuencia por la trayectoria que se ha establecido. Los datos siempre llegan al sistema destino en el orden en que fueron enviados.

Durante la fase de la terminación de la conexión, se termina una conexión establecida que ya no se vaya a utilizar. Si se requiriera más comunicación entre los sistemas origen y destino, serían necesario establecer una nueva conexión.

Los servicios de red orientados a la conexión tienen dos desventajas principales respecto a los no orientados a la conexión: la selección de una trayectoria estática y la reservación estática de los recursos de la red. La selección de la trayectoria estática puede causar problemas, ya que todo el tráfico debe viajar por la misma trayectoria

estática. La ocurrencia de una falla en cualquier punto a lo largo de la trayectoria provoca el fallo de la conexión. La reservación estática de los recursos de la red puede ser de difícil manejo porque requiere un rendimiento eficaz total garantizado y, por lo tanto, un compromiso de recursos que otros usuarios de la red no pueden compartir. A menos que la conexión utilice el canal de manera total e ininterrumpida, el ancho de banda no se utilizará eficientemente.

Los servicios orientados a la conexión, sin embargo, son muy útiles para la transmisión de datos de aplicaciones que no toleran retardos y secuenciación de paquetes. Las aplicaciones de voz y video se suelen basar en servicios orientados a la conexión.

Otra desventaja que presentan los servicios de red no orientados a la conexión es que no predeterminan la trayectoria desde el sistema de origen hasta el de destino, ni hay garantías en cuanto a la secuenciación de paquetes, el rendimiento eficaz total, y otros recursos de la red. Cada paquete debe especificar completamente la dirección del nodo al que está dirigido, ya que se pueden seleccionar diferentes trayectorias a través de la red para los distintos paquetes con base en diversos factores. Cada paquete es transmitido de manera independiente por el sistema origen y manejado de la misma forma por los dispositivos intermedios de la red.

Sin embargo, el servicio no orientado a la conexión tiene dos importantes ventajas respecto al servicio orientado a la conexión: la selección dinámica de la trayectoria y al asignación dinámica del ancho de banda. La selección dinámica de la trayectoria permite que el tráfico sea ruteado de modo que se evite su paso por las fallas de red, pues las trayectorias se seleccionan paquete por paquete. Con una asignación dinámica del ancho de banda, éste se utiliza de manera más eficiente al no asignarse ancho de banda a recursos de la red que no lo requieren.

Los servicios no orientados a la conexión son muy útiles en la transmisión de datos de aplicaciones que pueden tolerar cierta cantidad de retardo y resecuen ciación. Las aplicaciones de datos se basan en servicios no orientados a la conexión.

# CAPÍTULO 2.

# TECNOLOGÍAS LAN'S

Métodos diferentes de acceso a medios, los métodos de transmisión, las topologías y los dispositivos que se usan en una LAN (Red de Área Local). Los temas giran en torno a los métodos y dispositivos que se utilizan en Ethernet/IEEE 802.3, Token Ring/IEEE 802.5 y la FDDI (Interfase de Datos Distribuida por Fibra óptica). La figura 2-1 muestra el esquema básico de estas tres implementaciones.

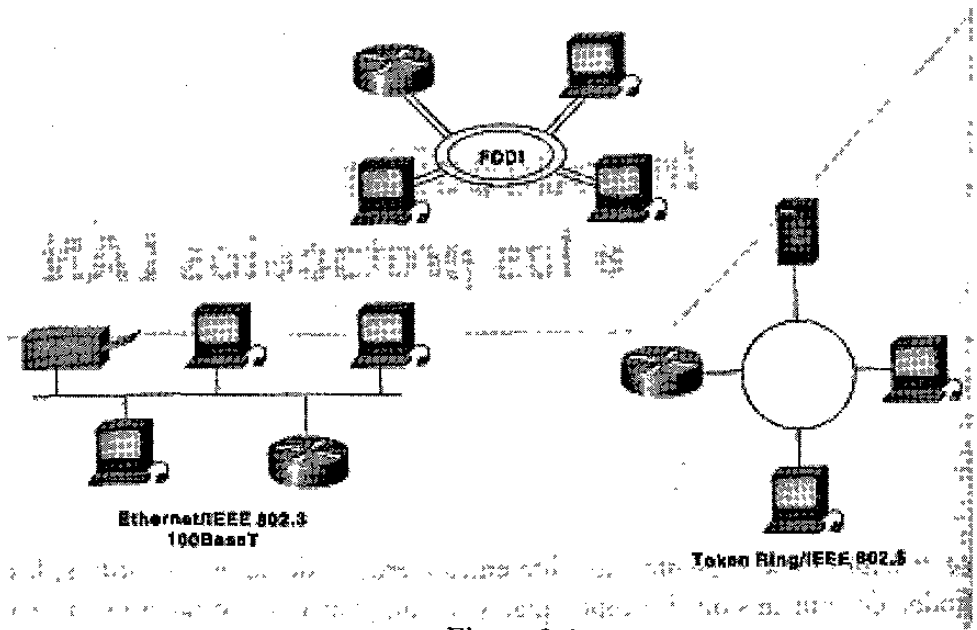



Figura 2-1

## ¿QUÉ ES UNA LAN?

Una LAN es una red de datos de alta velocidad, tolerante a fallas, que cubre un área geográfica relativamente pequeña. Por lo general conecta estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. Las LANs tienen muchas ventajas para los usuarios de computadoras, entre otras el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos entre los usuarios conectados y la comunicación entre usuarios vía correo electrónico y otras aplicaciones.

## LOS PROTOCOLOS LAN Y EL MODELO DE REFERENCIA OSI

Estos protocolos operan en las dos capas más bajas del modelo de referencia OSI entre la capa física y la capa de enlace de datos. La figura 2-2 muestra cómo se como se comparan algunos protocolos LAN muy conocidos con el modelo de referencia OSI.

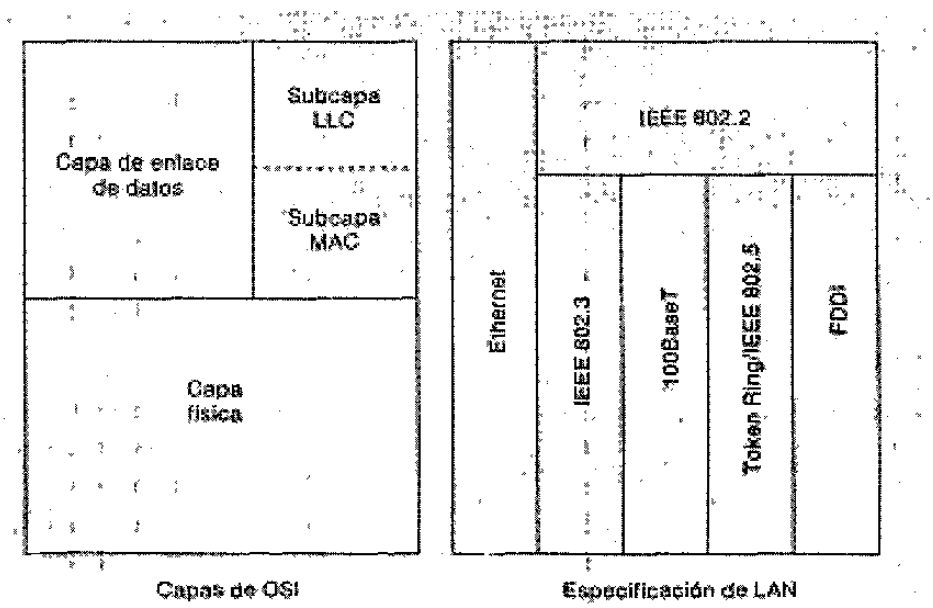



Figura 2-2

## MÉTODOS DE ACCESO A MEDIOS DE LAN

Los protocolos LAN suelen utilizar uno de dos métodos para accesar el medio físico de la red: CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de colisiones) y estafeta circulante.

En el esquema de acceso a medios CSMA/CD, los dispositivos de la red compiten por el uso del medio de transmisión físico de la red. Por esta razón, al CSMA/CD a veces se le llama acceso por contención. Ejemplos de LANs que utilizan el esquema de acceso a medios CSMA/CD son las redes Ethernet/IEEE 802.3, incluyendo a 100Base T.

En el esquema de acceso a medios llamado estafeta circulante, los dispositivos de la red accesan el medio de transmisión con base en la posesión de una estafeta. Ejemplos de LAN que utilizan el esquema de acceso a medios de estafeta circulante son Token Ring/IEEE 802.5 y FDDI.

## MÉTODOS DE TRANSMISIÓN EN LAS LAN

La transmisión de datos en las LAN cae dentro de tres clasificaciones: unidifusión, multidifusión y difusión. En cada tipo de transmisión, se envía un solo paquete a uno o más nodos.

En las transmisiones de unidifusión, se envía un solo paquete desde el origen a un destino de la red. Primero, el nodo origen direcciona el paquete utilizando la dirección del nodo de destino. Luego el paquete es enviado a la red y, finalmente, la red transfiere el paquete a su destino.

Las transmisiones de multidifusión constan de un solo paquete de datos que se copia y envía a un subconjunto específico de nodos en la red. Primero, el nodo origen direcciona el paquete utilizando una dirección de multidifusión. Luego, el paquete es

enviado a través de la red, la cual genera copias del paquete y envía estas copias a cada uno de los nodos que se indican en la dirección de multidifusión.

Las transmisiones de difusión constan de un solo paquete de datos que se copia y envía a todos los nodos de la red. En este tipo de transmisiones, el nodo origen dirige el paquete utilizando la dirección de difusión. El paquete es, luego, enviado a través de la red, la cual hace copias del paquete y las envía a cada uno de los nodos de la red.

## TOPOLOGÍAS DE LAN

Éstas definen la forma organización de los dispositivos de la red. Hay cuatro topologías comunes de LAN: bus, anillo, estrella y árbol. Estas topologías son arquitecturas lógicas, sin embargo, los dispositivos en realidad no necesitan estar ubicados físicamente de acuerdo con estas configuraciones. Por ejemplo, las topologías lógicas en bus y anillo, por lo común están dispuestas como una estrella. Una topología en bus es una arquitectura lineal de LAN en la que los envíos de las diferentes estaciones de la red se propagan a todo lo largo del medio de transmisión y son recibidas por todas las estaciones. Entre las tres implementaciones de LAN de mayor uso, las redes Ethernet/IEEE 802.3, incluyendo la 100 BaseT, implementan una topología en bus, como se ve en la figura 2-3.

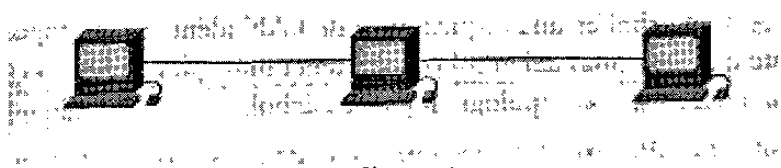


Figura 2-3

Una topología en anillo es una arquitectura de LAN que consta de una serie de dispositivos conectados el uno con el otro por medio de enlaces de transmisión unidireccionales para formar un solo lazo cerrado. Tanto Token Ring/IEEE 802.5, como FDDI implementan una topología anillo. La figura 2-4 muestra una topología lógica en anillo:

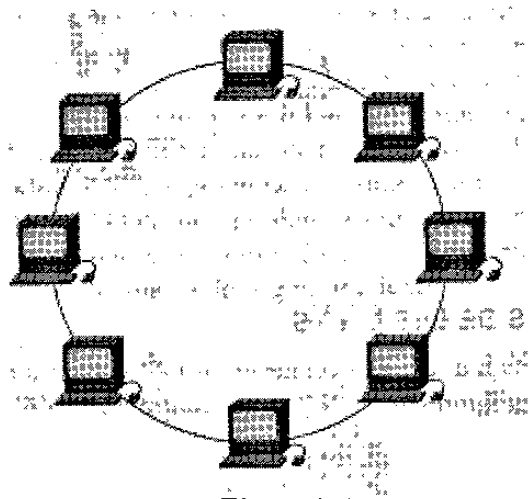


Figura 2-4

Una topología en estrella es una arquitectura de LAN en la que los puntos extremos de la red se conectan hacia un concentrador (hub) central común, o switch, por medio de enlaces dedicados. Las topologías en bus y anillo lógico a menudo se implementan físicamente en una topología en estrella, la cual se ilustra en la figura 2-5.

Una topología en árbol es una arquitectura de LAN idéntica a la topología en bus, excepto que las ramas del árbol pueden tener múltiples nodos en este caso. La figura 2-5 muestra una topología lógica en árbol.

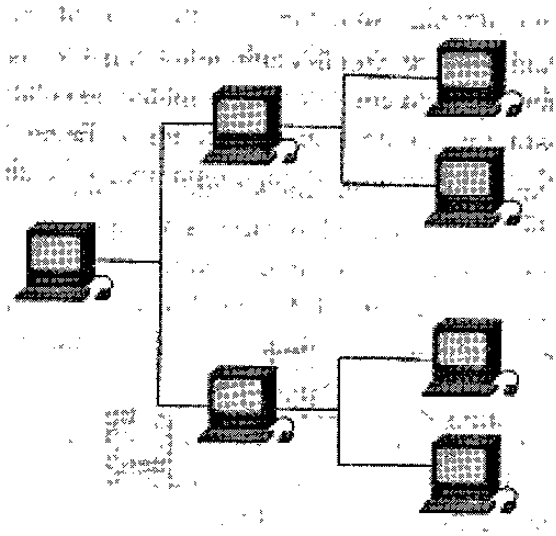


Figura 2-5

# DISPOSITIVOS DE LAS LANs

Entre los dispositivos de uso más común en las LAN están los repetidores, concentradores, extendedores de LAN, puentes, switches de LAN y ruteadores.

Un repetidor es un dispositivo de la capa física que se utiliza para interconectar los segmentos de cable en una red extendida. En esencia, un repetidor hace posible que una serie de segmentos de cable se comporte como un solo cable. Los repetidores reciben señales de un segmento de red y amplifican, resincronizan y retransmiten esas señales hacia otro segmento de la red. Estas acciones evitan el deterioro en la señal provocado por la presencia de tramos de cable de gran longitud y la gran cantidad de dispositivos conectados a la red. Los repetidores no pueden llevar a cabo un filtrado complejo ni otro tipo de procesamiento del tráfico. Además, todas las señales eléctricas, incluyendo los disturbios eléctricos y demás errores, se repiten y amplifican. El total de repetidores y segmentos de red que se pueden conectar está limitado por la temporización y otros problemas. La figura 2-6 muestra un repetidor que conecta dos segmentos de red.

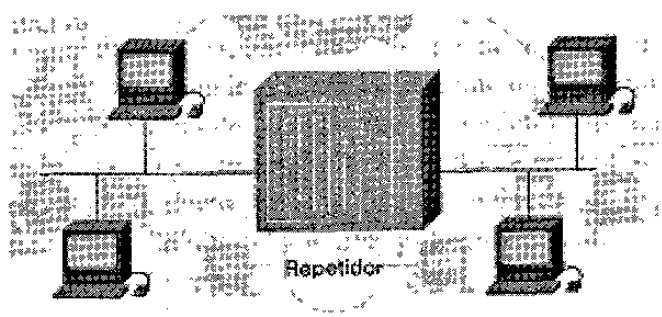



Figura 2-6

Un concentrador (o hub), es un dispositivo de la capa física que conecta varias estaciones de usuario por medio de un cable dedicado. Las interconexiones eléctricas se establecen dentro del concentrador. Los concentradores se utilizan para conformar una red con topología física en estrella que a su vez conserva la topología lógica en bus o la

configuración en anillo de LAN. En algunos aspectos, el concentrador actúa como un repetidor multipuerto.

Un extendedor de LAN es un switch multicapa de acceso remoto que se conecta a un ruteador host. Los extendedores de LAN transfieren el tráfico de todos los protocolos estándar de la capa de red (como IP, IPX y AppleTalk), y filtran el tráfico con base en la dirección MAC o el tipo de protocolo de la capa de red. Los extendedores de LAN son fácilmente escalables debido a que el ruteador host elimina las señales de multidifusión y difusión no deseadas. Los extendedores de LAN, sin embargo, no pueden segmentar el tráfico o crear barreras de protección. En la figura 2-7 se muestran varios extendedores de LAN conectados a un ruteador host por medio de una WAN.

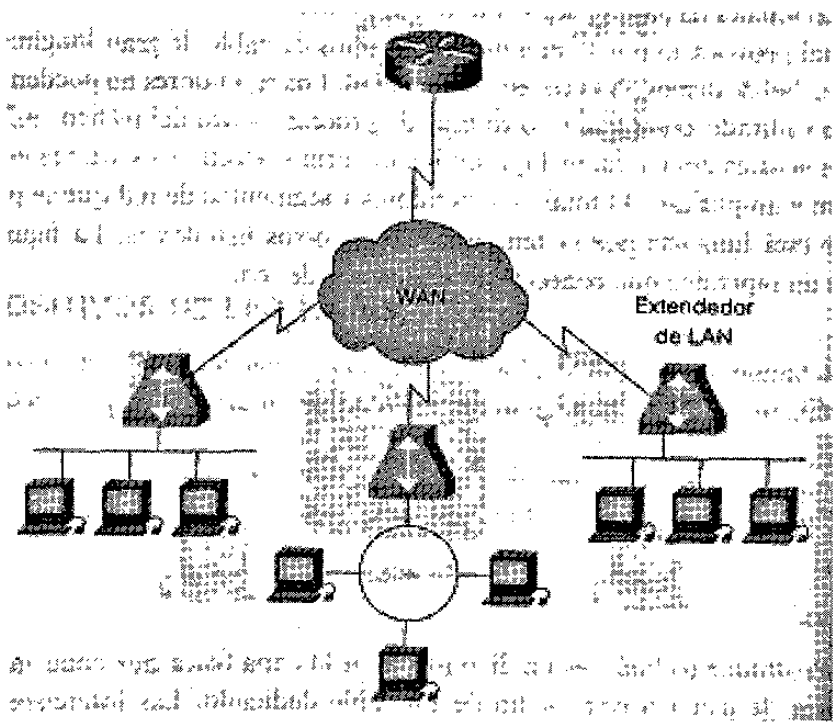



Figura 2-7

# CAPÍTULO 3.

# TECNOLOGÍAS WAN

Diferentes protocolos y tecnologías que se utilizan en los entornos de WAN (Redes de Área Amplia). Entre los temas que se estudian aquí se incluyen los enlaces punto a punto, la conmutación en circuitos, la conmutación en paquetes, los circuitos virtuales, los servicios conmutados y los dispositivos WAN.

## ¿QUÉ ES UNA WAN?

Una WAN es una red de comunicación de datos que tiene una cobertura geográfica relativamente grande y suele utilizar las instalaciones de transmisión que ofrecen compañías portadoras de servicios como las telefónicas. Las tecnologías WAN operan en las tres capas inferiores del modelo de referencia OSI: la capa física, la capa de enlace de datos y la capa de red. La figura 3-1 muestra la relación entre las tecnologías WAN más usuales y el modelo OSI.

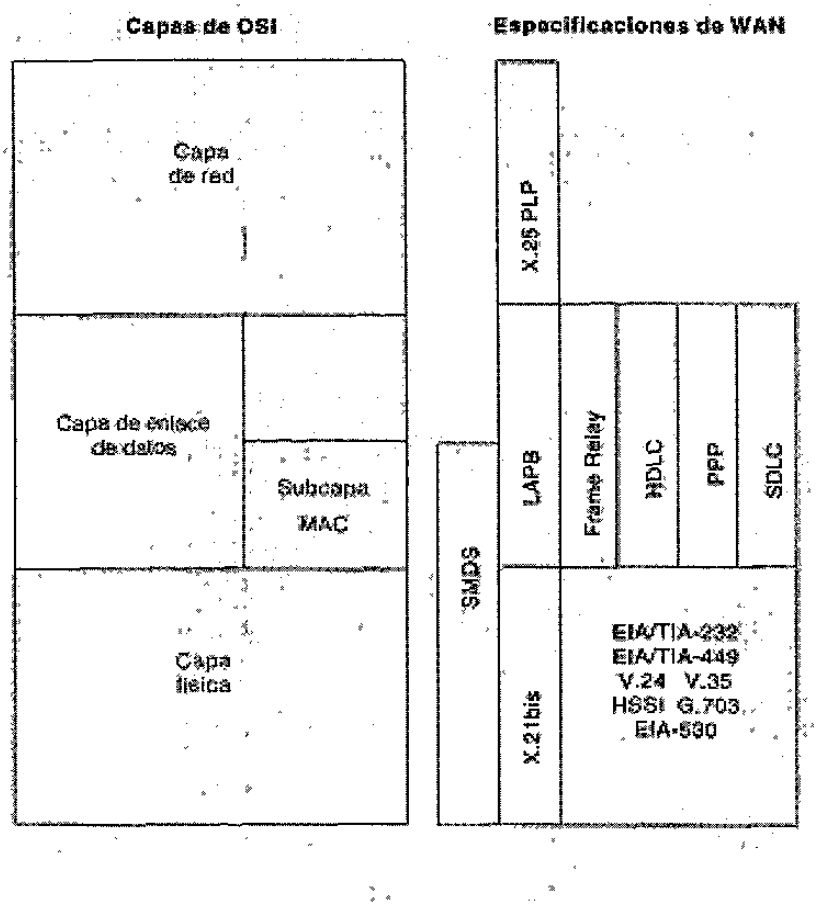



Figura 3-1

## ENLACES PUNTO A PUNTO

Un enlace punto a punto proporciona una sola trayectoria de comunicaciones WAN preestablecida desde las instalaciones del cliente, a través de una red de transporte como una compañía telefónica, hasta una red remota. A los enlaces punto a punto también se les conoce como líneas privadas, puesto que se trayectoria establecida es permanente y fija para cada red remota a la que se llegue a través de las facilidades de larga distancia. La compañía de larga distancia reserva varios enlaces punto a punto para uso exclusivo del cliente. Estos enlaces proporcionan dos tipos de transmisiones: transmisiones de datagramas, que están compuestas de tramas direccionadas de manera individual y

transmisiones de ráfagas de datos, que están compuestas de una ráfaga de datos para la que la verificación de direcciones se presenta sólo una vez. La figura 3-2 muestra un típico enlace punto a punto a través de una WAN.

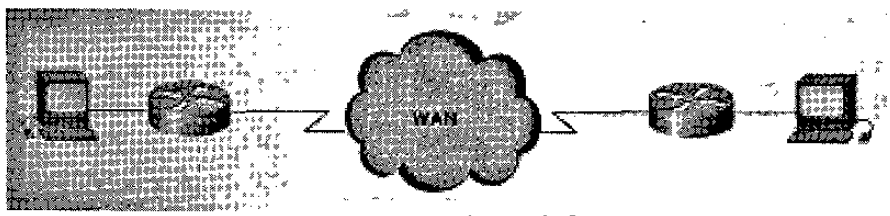



Figura 3-2

## CONMUTACIÓN DE CIRCUITOS

La conmutación de circuitos es un método de conmutación WAN en el que se establece, mantiene y termina un circuito físico dedicado a través de una red de transporte para cada sesión de comunicación. La conmutación de circuitos maneja dos tipos de transmisiones: transmisiones de datagramas, que están compuestas de tramas direccionadas de manera individual, y transmisiones en ráfagas de datos, para la que la verificación de direcciones sólo se presenta una vez. Utilizada de manera muy generalizada en las redes de las compañías telefónicas, la conmutación de circuitos opera de forma muy parecida a una llamada telefónica normal. ISDN (Red Digital de Servicios Integrados) es ejemplo de una tecnología WAN de conmutación de circuitos, la cual se muestra en la figura 3-3.

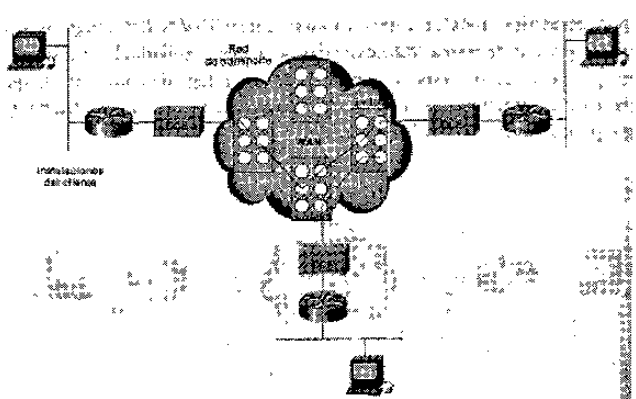


Figura 3-3

## CONMUTACIÓN DE PAQUETES

Éste es un método de conmutación WAN en el que los dispositivos de la red comparten un solo enlace punto a punto para transferir los paquetes desde un origen hasta un destino a través de una red de transporte. El multiplexaje estadístico se utiliza para permitir que los dispositivos compartan estos circuitos. ATM (Modo de Transferencia Asíncona), Frame Relay, SMDS (Servicio de Datos Conmutados a Multimegabits) y X.25, son ejemplos de tecnologías WAN de conmutación de paquetes, las cuales se muestran en la figura 3-4.

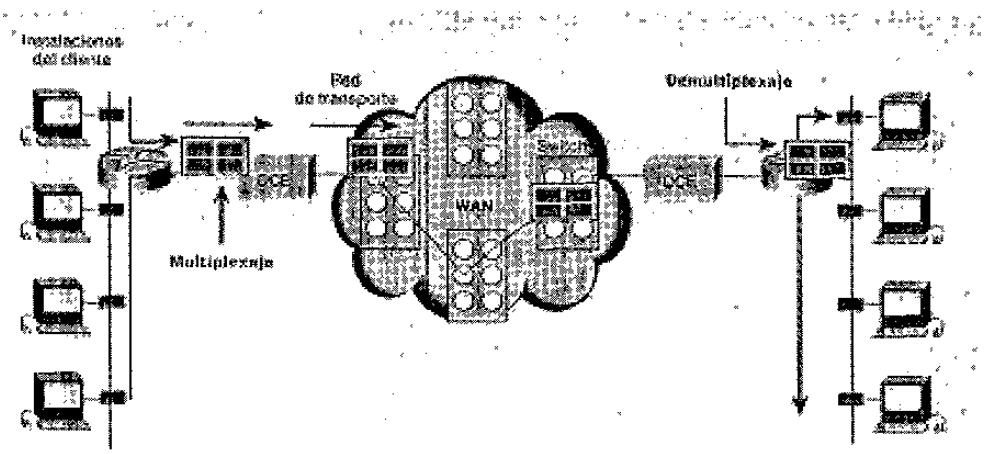



Figura 3-4

## CIRCUITOS VIRTUALES WAN

Un circuito virtual es un circuito lógico creado para asegurar una comunicación confiable entre dos dispositivos de red. Hay dos tipos de circuitos virtuales: SVCs (Circuitos Virtuales Conmutados) y PVCs (Circuitos Virtuales Permanentes).

Los SVC son circuitos virtuales que se establecen dinámicamente por demanda y se terminan al finalizar la transmisión. La comunicación a través de un SVC tiene tres fases: el establecimiento del circuito, la transferencia de datos y la terminación del circuito. La fase del establecimiento implica la creación de un circuito virtual entre los dispositivos origen y destino. La transferencia de datos implica la transmisión de datos

entre los dispositivos a través del circuito virtual, y la fase de terminación del circuito implica la desconexión del circuito virtual entre los dispositivos de origen y de destino. Los SVC se utilizan en situaciones donde la transmisión de datos entre los dispositivos es esporádica, en gran medida porque con los SVC se incrementa el ancho de banda utilizado, debido a las fases de establecimiento y terminación del circuito, pero disminuyen los costos asociados con la disponibilidad constante del circuito virtual.

Un PVC es un circuito virtual que se establece de manera permanente y consta de un solo modo: transferencia de datos. Los PVC se utilizan en situaciones donde la transferencia de datos entre los dispositivos es constante. Con los PVC disminuye el uso del ancho de banda asociado con el establecimiento y terminación de circuitos virtuales, pero se incrementan los costos debido a la constante disponibilidad del circuito virtual.

## SERVICIOS DE MARCADO DE WAN

Los servicios de marcado ofrecen métodos económicos para llevar a cabo la conectividad a través de las WAN. Las dos implementaciones más comunes de los servicios de marcado son el DDR (Ruteo de Marcación por Demanda) y el respaldo de marcación.

DDR es una técnica por medio de la cual un ruteador puede iniciar y terminar, de manera dinámica, una sesión de conmutación de circuitos a medida que las estaciones terminales de transmisión lo requieran. Se configura un ruteador para que considere cierto tráfico interesante (como el tráfico de un protocolo particular) y el resto del tráfico no interesante. Cuando el ruteador recibe tráfico interesante destinado a la red remota, se establece un circuito y se transmite el tráfico de manera normal. Si el ruteador recibe tráfico no interesante, y ya está establecido un circuito en ese momento, ese tráfico también se transmite de manera normal. El ruteador maneja un temporizador que se reinicializa solamente cuando recibe tráfico interesante. Sin embargo, el circuito termina si el ruteador recibe tráfico no interesante antes de que el temporizador expire. De la misma manera, si se recibe tráfico no interesante y no hay ningún circuito, el rueteador

elimina el tráfico. En el momento en el que le ruteador reciba tráfico interesante, iniciará un nuevo circuito. El ruteo DDR se puede utilizar para reemplazar enlaces punto a punto y servicios WAN de multiacceso conmutado.

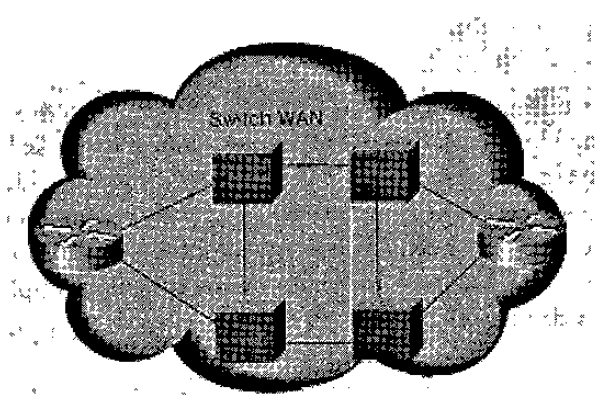
La implementación de respaldo de marcación es un servicio que activa una línea serial de respaldo bajo determinadas condiciones. La línea serial secundaria puede actuar como un enlace de respaldo que se utiliza cuando el enlace principal falla, o como una fuente que proporciona ancho de banda adicional cuando la carga en el enlace principal alcanza un cierto umbral. El respaldo de marcación proporciona protección contra la degradación del desempeño y el tiempo fuera de servicios de una WAN.

## DISPOSITIVOS WAN

Las WAN utilizan un gran número de tipos de dispositivos específicos para los ambientes WAN. Otros dispositivos que se utilizan en los ambientes WAN y que son exclusivos para las implementaciones de WAN son los ruteadores, los switches ATM y los multiplexores.

## SWITCH WAN

Éste es un dispositivo multipuerto de interconectividad de redes que se utiliza en las redes de transporte. Por lo general, estos dispositivos conmutan tráfico como el de Frame Relay, X.25 y SMDS y operan en la capa de enlace de datos del modelo de referencia OSI. La figura 3-5 muestra a dos ruteadores ubicados en los extremos remotos de una WAN que se encuentran conectados a través de switches WAN.



## SERVIDOR DE ACCESO

Un servidor de acceso actúa como un punto de concentración para conexiones de marcación hacia adentro y hacia fuera. La figura 3-6 muestra un servidor de acceso concentrando las marcaciones hacia fuera en una WAN.

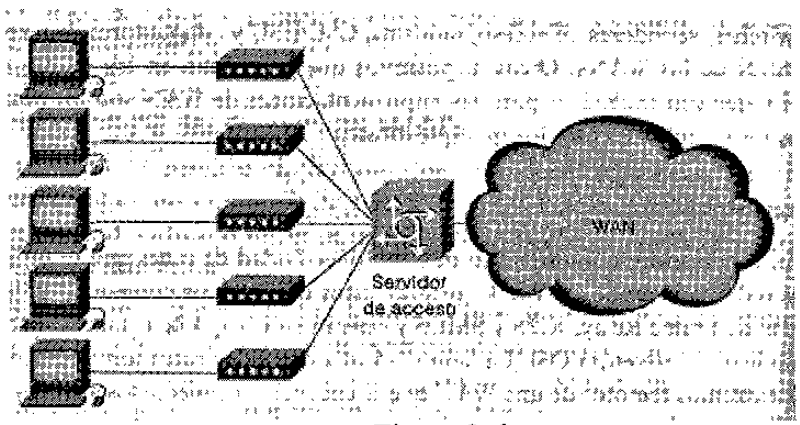



Figura 3-6

## MÓDEM

Un módem es un dispositivo que interpreta señales analógicas y digitales, permitiendo de esta manera que los datos se transmitan a través de líneas telefónicas sonoras. En el punto origen las señales digitales son convertidas a una forma apropiada para su transmisión a través de equipos de comunicación analógica. En el punto destino, estas señales analógicas son convertidas de nuevo a su forma digital original. La figura 3-7 muestra una conexión simple de módem a módem a través de una WAN.

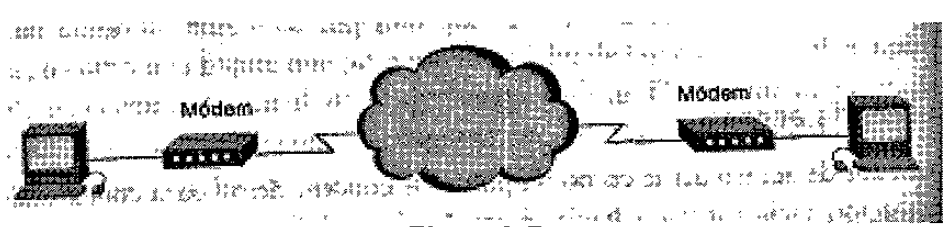



Figura 3-7

## UNIDAD DE SERVICIO DE DATOS

Una CSU/DSU (Unidad de Servicio de Canal/Unidad de Servicio de Datos) es un dispositivo de interfase digital (o, a veces, dos dispositivos digitales separados) que adapta la interfase física de un dispositivo DTE (Equipo Terminal de Datos), como una terminal, a la interfase del dispositivo DCE (Equipo de Comunicación de Datos), como un switch, en una red conmutada de transporte. La CSU/DSU también proporciona la temporización de la señal para la comunicación entre estos dispositivos. La figura 3-8 muestra la localización de la unidad CSU/DSU en una implementación WAN.

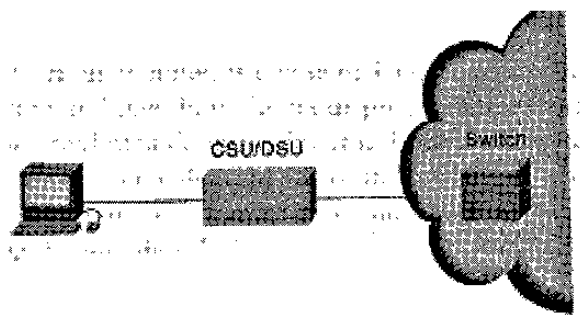
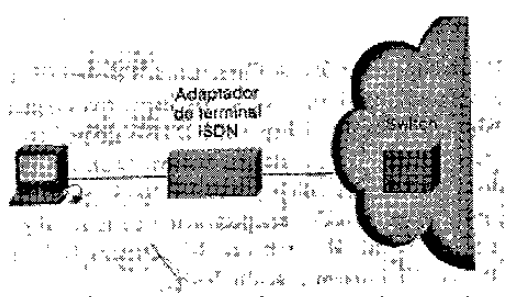



Figura 3-8

## ADAPTADOR DE TERMINAL ISDN

Un adaptador de terminal ISDN (Red Digital de Servicios Integrados) es un dispositivo que se utiliza para conectar la BRI (Interfase de Tasa Básica) de ISDN con otras interfases, como la EIA/TIA-232. Un adaptador de terminal es, en esencia, un




módem ISDN. La figura 3-9 muestra la ubicación del adaptador de terminal en un entorno ISDN.

# CAPÍTULO 4.

# FUNDAMENTOS DEL PUENTEO Y LA CONMUTACIÓN

## ¿QUÉ SON LOS PUENTES Y LOS SWITCHES?

Son dispositivos de comunicación de datos que operan, principalmente, en la Capa 2 del modelo de referencia OSI. Como tales, se les conoce ampliamente como dispositivos de la capa de enlace de datos.

Los puentes estuvieron disponibles en el mercado a principios de los años 80. En ese entonces se usaban para conectar y habilitar el ruteo de paquetes entre redes homogéneas, mas recientemente ya también el puenteo entre redes diferentes ha quedado definido y estandarizado.

Hay diferentes tipos de puenteo que han resultado ser importantes como dispositivos de interconectividad de redes. El puenteo transparente se presenta principalmente en entornos Ethernet, en tanto que el puenteo origen ruta se utiliza sobre todo en entornos Token Ring.

El puenteo de traducción da la traducción entre los formatos y los principios de tránsito de diferentes tipos de medios (generalmente, Ethernet y Token Ring). Por último, el puenteo transparente origen ruta combina los algoritmos del puenteo transparente para permitir la comunicación en entornos combiandos Ethernet/Token Ring.

Hoy en día, la tecnología de la conmutación se ha convertido en la heredera evolutiva de las soluciones de interconectividad de redes basadas en el puenteo. Las implementaciones de conmutación dominan ahora las aplicaciones en las que se implementaron tecnologías de puenteo en diseños de red anteriores. El desempeño superior del rendimiento eficiente total, la mayor densidad de puertos, un menor costo por puerto y mayor flexibilidad, han contribuido a que aparezcan los switches como una tecnología de reemplazo de los puentes y como complemento de la tecnología de ruteo.

## PANORAMA DE LOS DISPOSITIVOS DE LA CAPA DE ENLACE DE DATOS

El puenteo y la conmutación se presentan en el nivel enlace de datos, que controla el flujo de datos, maneja los errores en la transmisión, proporciona el direccionamiento físico (a diferencia del lógico) y administra el acceso al medio físico de transmisión. Los puentes proporcionan estas funciones utilizando diferentes protocolos de la capa de enlace de datos que especifican algoritmos específicos para el control del flujo, el manejo de errores, el direccionamiento y el acceso a medios. Algunos ejemplos muy conocidos de protocolos a nivel enlace de datos son Ethernet, Token Ring y FDDI.

Los puentes y los switches no son dispositivos complicados. Analizan las tramas entrantes, toman decisiones de envío con base en la información contenida en las tramas y envían las tramas a su destino. En algunos casos, como el del puenteo origen ruta, la trayectoria completa hacia el destino está contenida en cada trama. En otros casos, como en el puenteo transparente, las tramas son enviadas hacia su destino de un salto a la vez.

La transparencia de protocolos en las capas superiores es una gran ventaja tanto del puenteo como de la conmutación. Como ambos tipos de dispositivos trabajan a nivel capa de enlace, no es necesario que examinen la información de las capa superiores. Lo anterior significa que, tanto la función de puenteo como la de conmutación, pueden direccionar rápidamente, el tráfico que represente cualquier protocolo de la capa de red. No es raro que un puente transfiera Apple Talk, DECnet, TCKP/IP, XNS y otro tipo de tráfico entre dos o más redes.

Los puentes son capaces de filtrar tramas con base en cualquiera de los campos de la Capa 2. Por ejemplo, un puente se puede programar para rechazar (no reenviar) todas las tramas que se originaron en una red en particular. El hecho de que, con frecuencia, la información de la capa de enlace de datos incluya una referencia a un protocolo de las capas superiores, permite que los puentes, en general, puedan filtrar esta referencia. Además, los filtros pueden ser muy útiles cuando se trata de manejar paquetes de difusión y multidifusión innecesarios.

Los puentes y los switches proporcionan algunas ventajas debido a la fragmentación de redes de gran tamaño en unidades independientes. Como sólo un porcentaje del tráfico es enviado, un puente o un switch reduce el tráfico que circula a través de los dispositivos que están conectados a todos los segmentos. Tanto el puente como el switch actuarán como una barrera de protección contra algunos errores que potencialmente pudieran dañar a la red y ambos proporcionarán comunicación entre un número mayor de dispositivos de los que se podrían soportar en cualquier LAN conectada al puente. Los puentes y los switches extienden la longitud efectiva de un LAN, al permitir la conexión de estaciones distantes que anteriormente no era posible.

A pesar de que los puentes y los switches comparten la mayor parte e sus atributos más importantes, hay algunas diferencias entre ambas tecnologías. Los switches son mucho más rápidos debido a que conmutan en el hardware, en tanto que los puentes lo hacen en el software y también pueden interconectar LANs con diferentes anchos de banda. Por ejemplo, una LAN Ethernet a 10 Mbps y una LAN Ethernet a 100 Mpbs

pueden conectarse por medio de un switch. Asimismo, los switches soportan la conmutación rápida, que reduce la latencia y los retardos en la red, mientras que los puentes soportan solamente conmutación de tráfico de tipo almacenar y reenviar. Por último, los switches disminuyen las colisiones en los segmentos de la red debido a que ofrecen un ancho de banda dedicado exclusivamente a cada segmento de la red.

## TIPOS DE PUENTES

Los puentes pueden agruparse en categorías con base en diferentes características del producto. De acuerdo con un esquema de clasificación muy conocido, los puentes pueden ser locales o remotos. Los puentes locales proveen una conexión directa entre múltiples segmentos de LAN en la misma área. Los puentes remotos conectan múltiples segmentos de LAN en áreas diferentes, en general, a través de líneas de telecomunicaciones. La figura 4-1 muestra estas dos configuraciones.

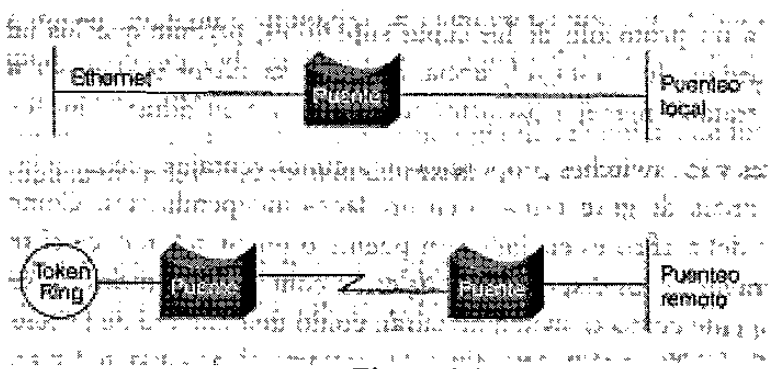



Figura 4-1

El puenteo remoto presenta varios retos de interconectividad de redes que son únicos, uno de los cuales es la diferencia entre las velocidades de las LAN y de las WAN. Aunque actualmente se pueden encontrar varias tecnologías de WAN a alta velocidad en interredes geográficamente dispersas, a menudo las velocidades con que opera una LAN son mayores que las de la WAN. Las diferencias significativas en cuanto a velocidades de la WAN y las LAN pueden hacer que los usuarios no puedan correr aplicaciones de LAN que sean sensibles al retardo en la WAN.

Con los puentes remotos no se puede mejorar la velocidad de las WAN, sin embargo, se pueden compensar las diferencias de velocidad por medio de una capacidad suficiente de almacenamiento. Si un dispositivo de LAN capaz de transmitir a una velocidad de 3 Mbps desea comunicarse con un dispositivo en una LAN remota, el puente local debe regular la ráfaga de datos a 3 Mbps para que no sature el enlace serial a 64 Kbps. Esto se lleva a cabo almacenándose los datos entrantes en memorias montadas en la tarjeta y enviándolos a través del enlace serial a una velocidad que éste pueda soportar. Esta función de almacenamiento en búfer sólo se puede lograr cuando se presentan ráfagas cortas de datos que no saturen la capacidad de almacenamiento del puente.

El IEEE (Instituto de Ingenieros en Electrónica y Electricidad) divide la capa de enlace e OSI en dos subcapas separadas: MAC (subcapa de Control de Acceso a Medios) y LLC (subcapa de Control del Enlace Lógico). La subcapa MAC ofrece y coordina el acceso a medios, como la contención y estafeta circulante, en tanto que la subcapa LLC se encarga del entramado, el control de flujo, el control de errores y el direccionamiento de la subcapa MAC.

Algunos puentes son puentes de la capa MAC, que puentean redes homogéneas (por ejemplo IEEE 802.3 e IEEE 80.3), en tanto que otros pueden traducir entre los diferentes protocolos de la capa de enlace e datos (por ejemplo, IEEE 802.3 e IEEE802.5). Los mecanismos básicos de dicha traducción se muestran en la figura 4-2.

La figura 4-2 muestra un host IEEE 802.3 (Host A) que formula un paquete con información de aplicación y encapsula el paquete en una trama compatible con el estándar IEEE 802.3 para su envío por el medio IEEE 802.3 hacia el puente. En el puente, se retira de la trama su encabezado IEEE 802.3 en la subcapa MAC de la capa de enlace y, después, la trama se transfiere a la subcapa LLC para su procesamiento ulterior. Posteriormente, el paquete se transfiere de regreso al formato del estándar IEEE 802.5, el cual encapsula el paquete en un encabezado IEEE 80.5 para su envío a través de la red IEEE 802.5 hacia el host IEEE 802.5 (Host B).

La función de traducción que realiza un puente para conectar redes de diferente tipo nunca es perfecta, debido a que es muy probable que una red soporte determinados campos de la trama y funciones del protocolo que la otra red no soporta.

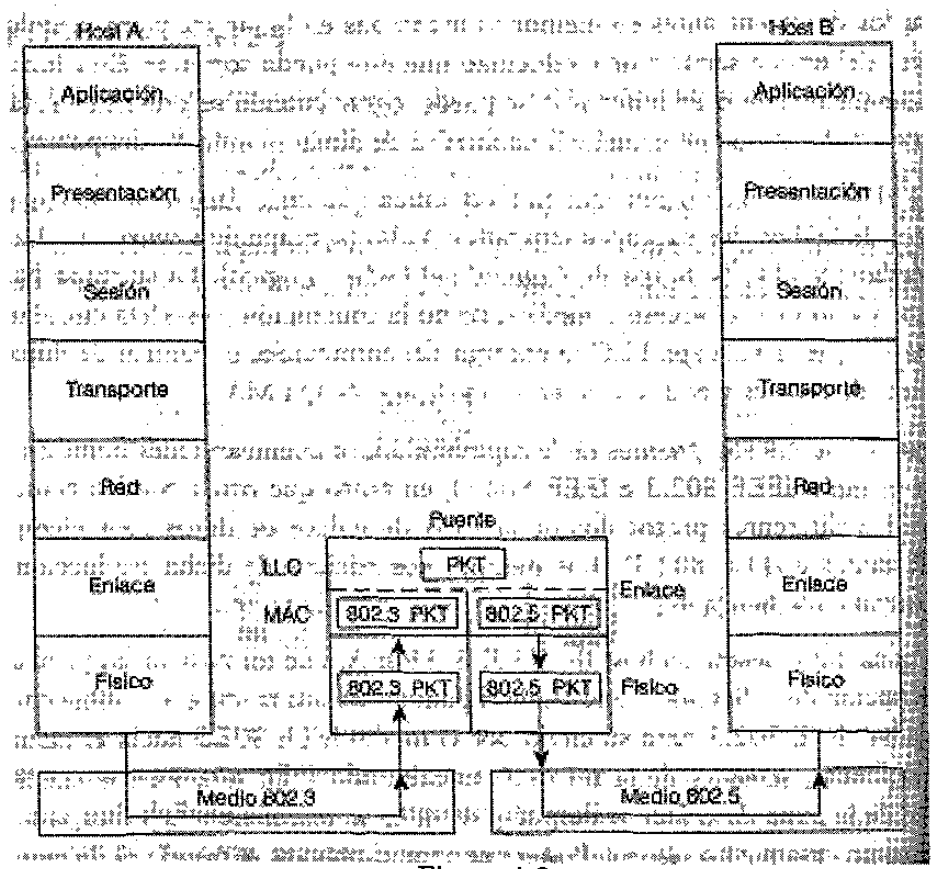



Figura 4-2

## TIPOS DE SWITCHES

Los switches son dispositivos de la capa de enlace de datos que, como los puentes, permiten la interconexión de múltiples segmentos físicos de LAN en una sola red de gran tamaño. Los switches envían y distribuyen el tráfico con base en sus direcciones MAC. Sin embargo, a pesar de que la función de conmutación se lleva a cabo en hardware y no en software, es significativamente más rápida. Los switches utilizan tanto la conmutación almacenar y enviar como la conmutación rápida para reenviar el tráfico.

Hay muchos tipos de switches entre los que se cuentan los switches ATM, los switches LAN y varios tipos de switches WAN.

## LOS SWITCHES ATM

Los switches ATM (Modo de Transferencia Asíncrona) ofrecen una conmutación a alta velocidad y anchos de banda que pueden incrementarse en el grupo de trabajo, la troncal de la red corporativa y en un área de gran cobertura. Los switches ATM soportan aplicaciones de voz, video y datos y están diseñados para conmutar unidades de información de tamaño fijo que se llaman celdas, las cuales se utilizan en las comunicaciones de ATM. La figura 4-3 muestra una red corporativa compuesta por múltiples LANs interconectadas por medio de una troncal de ATM.

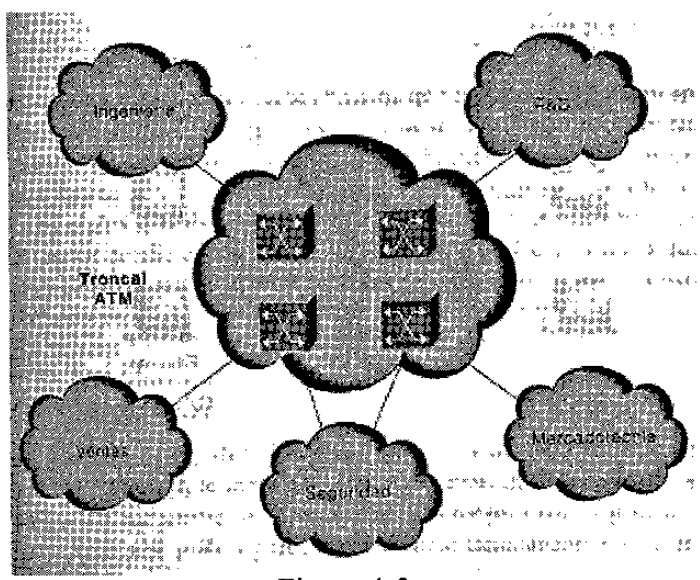



Figura 4-3

## SWITCH LAN

Éste se utiliza para interconectar segmentos múltiples de LAN. La conmutación en LAN representa una comunicación dedicada, libre de colisiones entre los dispositivos de la red, que puede soportar múltiples conversaciones simultáneas. Los switches LAN están diseñados para conmutar tramas de datos a altas velocidades. La figura 4-4

muestra una red simple en la que se interconectan una LAN Ethernet a 10 Mbps y una LAN Ethernet a 100 Mbps, por medio de un switch LAN.

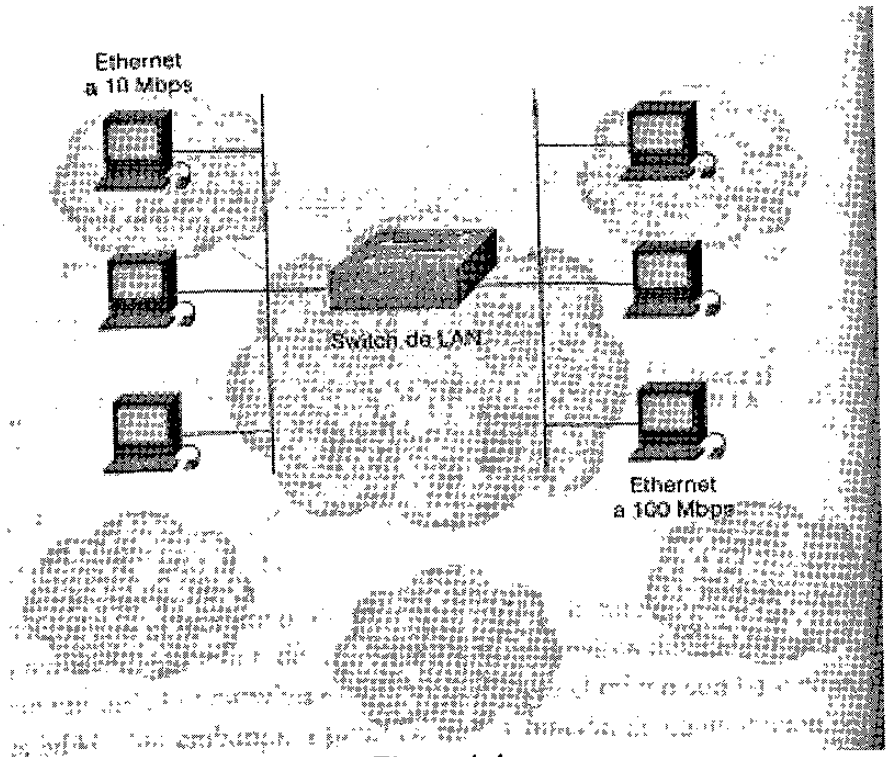



Figura 4-4

# CAPÍTULO 5.

# FUDAMENTOS DEL RUTEO

## ¿QUÉ ES EL RUTEO?

El ruteo es el acto de transferir información a través de una red desde un origen hasta un destino. A lo largo del camino, en general, se encuentra cuando menos un nodo intermedio. A veces el ruteo se compara con el puenteo y al observador común le podría parecer que cumple exactamente con la misma misión. La principal diferencia entre las dos es que el puenteo se presenta en la Capa 2 (la capa de enlace de datos) del modelo de referencia OSI, en tanto que el ruteo se presenta en la Capa 3 (la capa de red). Esta diferencia significa que las funciones de ruteo y puenteo tendrán información diferente para utilizar durante el proceso de transferencia de información desde el origen hasta el destino; amboas funciones cumplen sus tareas en forma diferente.

El tema del ruteo ha sido punto de estudio en la literatura de las ciencias de la computación por más de dos décadas, pero comercialmente, su popularidad se difundió hasta mediados de los años 80. La razón principal de este retraso es que en los años 70 las redes eran entornos muy simples y homogéneos. Por ello, la interconectividad de redes a gran escala se ha generalizado hasta épocas muy recientes.

## COMPONENTES DEL RUTEO

La función de ruteo está formada por dos actividades básicas: la determinación de las trayectorias óptimas de rueteo y el transporte de grupos de información (llamados comúnmente paquetes) a través de una red. En el contexto de los procesos de ruteo, a esto último se le conoce como conmutación. Aunque la conmutación es relativamente directa, la determinación de la trayectoria puede ser demasiado compleja.

## DETERMINACIÓN DE LA TRAYECTORIA

Una métrica es un estándar de medición, por ejemplo la longitud de la trayectoria, que los algoritmos de ruteo utilizan para determinar la trayectoria óptima hacia un destino. Para facilitar el proceso de la determinación de la trayectoria, los algoritmos de rueto inicializan y conservan tablas de ruteo, que contienen información acerca de todas las rutas. Esta información varía dependiendo del algoritmo de ruteo que se utilice.

Los algoritmos de ruteo alimentan las tablas de ruteo con una gran variedad de información. Las asociaciones de salto destino / próximo informan al ruteador que se puede llegar a un destino particular de manera óptima enviando el paquete a un ruteador particular que represente el "próximo salto" en el camino a su destino final. Cuando un ruteador recibe un paquete entrante, verifica la dirección de destino e intenta asociar esta dirección con el siguiente salto. La figura 5-1 muestra el ejemplo de una tabla de ruteo de salto destino / próximo.

| Para conectar con la red: | Enviar hacia: |
|---|---|
| 27 | Nodo A |
| 57 | Nodo B |
| 17 | Nodo C |
| 24 | Nodo A |
| 52 | Nodo A |
| 16 | Nodo B |
| 26 | Nodo A |
| - | - |
| - | - |
| - | - |

Figura 5-1

Las tablas de ruteo también pueden contener otra información, como son los datos acerca de la conveniencia de una trayectoria. Los ruteadores comparan medidas para determinar las rutas óptimas y estas medidas difieren en función del diseño del algoritmo de ruteo que se utilice.

Los ruteadores se comunican entre sí y conservan sus tablas de ruteo a través del envío de una gran variedad de mensajes. El mensaje de actualización de ruteo es uno de ellos, que en general está formado por una tabla completa de ruteo o una porción de la misma. Al analizar las actualizaciones del ruteo de todos los demás ruteadores, un ruteador puede hacerse una idea detallada de la topología de la red. Un anuncio del estado del enlace, otro ejemplo de mensaje enviado entre ruteadores, informa a los demás ruteadores acerca del estado de los enlaces del emisor. Los ruteadores también pueden utilizar la información sobre los enlaces para hacerse una idea completa de la topología de la red, lo que les permite determinar las rutas óptimas hacia los destinos de la red.

# LA CONMUTACIÓN

Los algoritmos de conmutación son relativamente simples y, básicamente, los mismos para la mayoría de los protocolos de ruteo. En la mayoría de los casos, un host decide que se debe enviar un paquete a otro host. Cuando de alguna forma ha conseguido al dirección del ruteador, el host origen envía un paquete direccionado específicamente hacia una dirección física MAC (capa de Control de Acceso a Medios) de un ruteador, esta vez con la dirección de protocolo (capa de red) del host destino.

Conforme examina la dirección del protocolo de destino del paquete, el ruteador determina si sabe o no cómo direccionar el paquete hacia el siguiente salto. Si el ruteador no sabe cómo direccionar el paquete, normalmente lo elimina. Mas si sabe cómo direccionar el paquete, cambia la dirección física de destino a la correspondiente del salto siguiente y transmite el paquete.

De hecho, el salto siguiente puede ser el último host destino. Si no es así, el salto siguiente suele ser otro ruteador que ejecuta el mismo proceso de decisión en cuanto a la conmutación. A medida que le paquete viaja a través de la red, su dirección física cambia, pero su dirección de protocolo se mantiene constante, como se muestra en la figura 5-2.

El análisis anterior describe la función de conmutación entre un origen y un sistema terminal de destino. ISO (Organización Internacional de Estándares) ha desarrollado una terminología jerárquica muy útil en la descripción de este proceso. De acuerdo con esta terminología, a los dispositivos de red que no tienen la capacidad de rutear paquetes entre subredes se les conoce como ESs (Sistemas Terminales), en tanto que a los dispositivos de red que tienen esta capacidad se les llama Iss (Sistemas Intermedios). Los ISs, a su vez, se dividen entre aquellos que se pueden comunicar dentro de dominios de ruteo (ISs de intradominio) y los que pueden comunicarse con y entre diferentes dominios de ruteo (ISs de interdominio). En general, se considera que un dominio de ruteo es parte de una red que está bajo una autoridad administrativa común que está

regulada por un conjunto particular de estatutos administrativos. A los dominios de ruteo también se les llama sistemas autónomos. Con determinados protocolos, los dominios de ruteo se pueden dividir en áreas de ruteo, pero los protocolos de ruteo de intradominio aún se utilizan para la función de conmutación dentro y entre áreas.

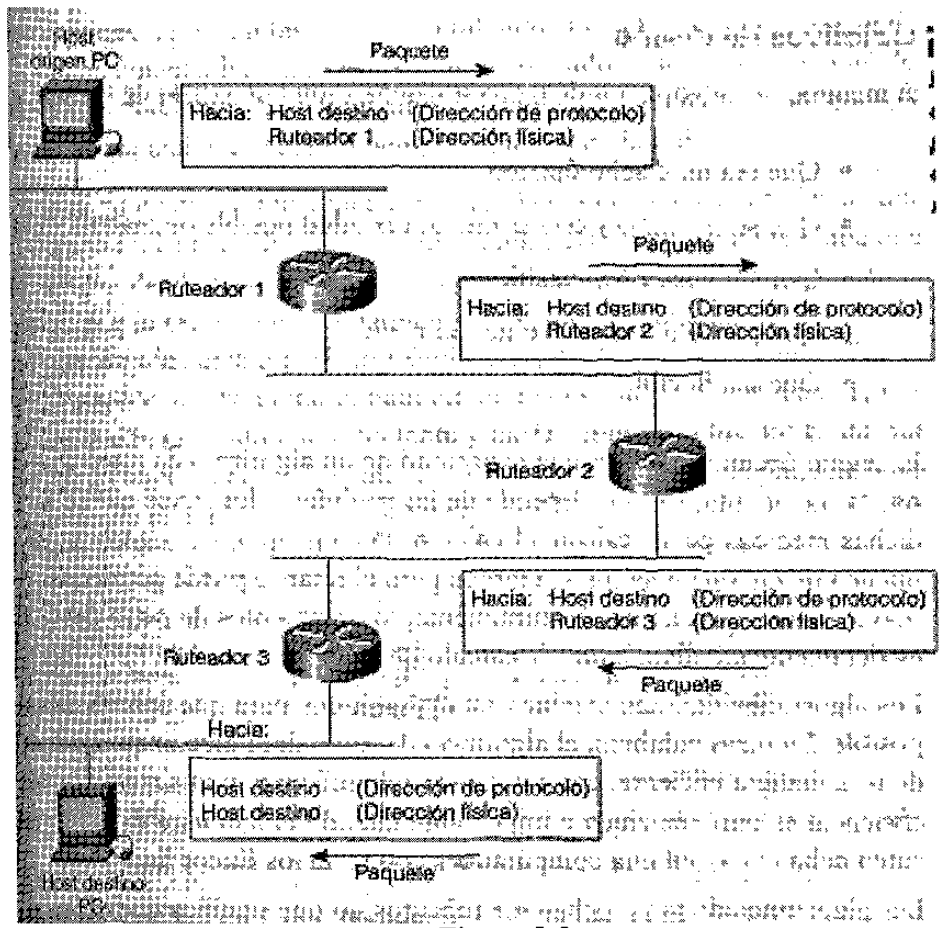



Figura 5-2

## ALGORITMOS DE RUTEO

Los algoritmos de ruteo se pueden diferenciar a partir de determinadas características fundamentales. Primero, los objetivos particulares del diseñador del algoritmo afectan la operación del protocolo de ruteo resultante. Segundo, hay diferentes tipos de algoritmos de ruteo y cada uno de ellos tiene un impacto diferente en los recursos de la red y del ruteador. Por último, los algoritmos de ruteo utilizan una gran variedad de medidas que

afectan el cálculo de las rutas óptimas. En la sección siguiente se describen estos atributos de los algoritmos de ruteo.

## OBJETIVOS DE DISEÑO

A menudo, los algoritmos de ruteo se diseñan con uno o más de estos objetivos:

- Que sea un diseño óptimo
- Que sea sencillo y con la menor cantidad posible de material inútil.
- Que sea robusto y estable.
- Que permita una convergencia rápida.
- Que sea flexible.

El diseño óptimo se refiere a la capacidad de un algoritmo de ruteo de seleccionar la mejor ruta, lo cual depende de las medidas y los pesos que se asignen a dichas medidas para realizar el cálculo. Por ejemplo, un algoritmo de ruteo puede utilizar varios saltos y retardos pero el retardo puede ponderarse con un mayor peso en el cálculo. Naturalmente, los protocolos de ruteo deben definir estrictamente sus algoritmos de cálculo de medida.

Los algoritmos de ruteo también están diseñados para que sean lo más simple posible. En otras palabras, el algoritmo de ruteo debe ofrecer su funcionalidad de una manera eficiente, con un mínimo de software y utilización óptima. La eficiencia es particularmente importante cuando el software del algoritmo de ruteo deba correr en una computadora con recursos físicos limitados.

Los algoritmos de ruteo deben ser robustos, lo que significa que deben desempeñarse correctamente aun cuando se enfrenten a circunstancias poco comunes e imprevistas, como fallas en hardware, condiciones de carga alta e implementaciones incorrectas. Debido a que los ruteadores se ubican en los puntos de unión de la red, pueden causar problemas considerables cuando llegan a fallar. Los mejores algoritmos de ruteo suelen

ser los que han resistido la prueba del tiempo y han demostrado que permanecen estables en una gran variedad de condiciones de la red.

Además, los algoritmos de ruteo deben converger rápidamente. La convergencia es el proceso por el cual todos los ruteadores llegan a un acuerdo con respecto a las rutas óptimas. Cuando un evento en la red provoca que las rutas se caigan o estén disponibles, los ruteadores distibuyen mensajes de actualización de ruteo que penetran las redes, estimulando el recálculo de las rutas óptimas y, ocasionalmente, haciendo que todos los ruteadores lleguen a un acuerdo con respecto a esas rutas. Los algoritmos de ruteo que convergen con lentitud pueden provocar ciclos de ruteo o tiempos muertos en la red.

En el ciclo de ruteo que se muestra en la figura 5-3, un paquete llega al ruteador 1 en el tiempo t1. El ruteador 1 ya ha sido actualizado y, por lo tanto, sabe que la ruta óptima de destino pide que la siguiente parada sea el ruteador 2. El ruteador 1, por lo tanto, envía el paquete al ruteador 2, como éste aún no ha sido actualizado, cree que el host óptimo siguientes es el ruteador 1. Por lo tanto, el ruteador 2 direcciona el paquete de regreso hacia el ruteador 1, y el paquete se queda saltando hacia delante y hacia atrás entre los dos hasta que el ruteador 2 recibe su actualización de ruteo o bien hasta que el paquete haya sido conmutado el máximo de veces permitido.

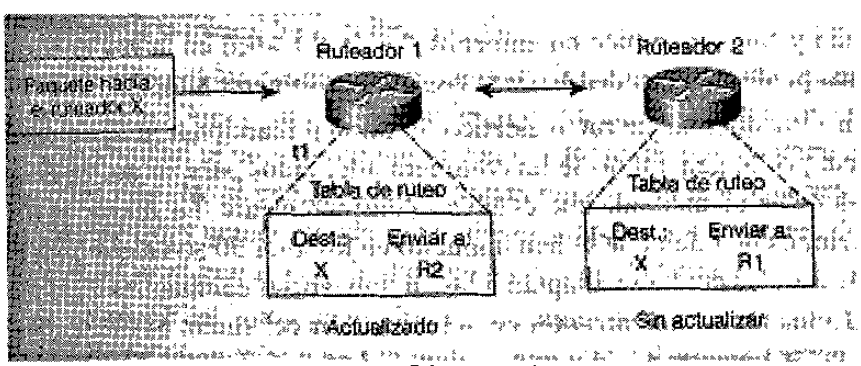



Figura 5-3

Los algoritmos de ruteo también deben ser flexibles, lo que significa que se deben adaptar rápidamente y con precisión a una gran variedad de circunstancias de la red. Suponga, por ejemplo, que un segmento de la red ha fallado. A medida que detectan el

problema, muchos algoritmos de ruteo seleccionarán rápidamente la mejor trayectoria siguiente para todas las rutas que normalmente utilizan ese segmento. Los algoritmos de ruteo pueden ser programados para adaptarse a los cambios en el ancho de banda de la red, el tamaño de la cola del ruteador y el retardo de la red, entre muchas otras variables.

## TIPOS DE ALGORITMOS

Los algoritmos de ruteo se pueden clasificar por tipo. Diferencias fundamentales:

- Estáticos versus dinámicos.
- Una sola trayectoria versus multitrayectoria.
- Planos versus jerárquicos.
- Host inteligente versus ruteador inteligente.
- Intradominio versus interdominio.
- Basados en estado de enlaces versus vector de distancia.

## ESTÁTICOS *VERSUS* DINÁMICOS

Los algoritmos de ruteo estático no se pueden considerar verdaderos algoritmos, sino que son mapeos de tablas que el administrador de la red establece antes de empezar el ruteo. Estos mapeos no varían a menos que el administrador de la red las cambie. Los algoritmos que utilizan rutas estáticas son de fácil diseño y funcionan bien en entornos donde el tráfico en la red es hasta cierto punto predecible y el diseño de la red es relativamente simple.

Como los sistemas de ruteo estático no pueden reaccionar ante los cambios en la red, por lo general no se les considera adecuados para su uso en las grandes redes de la actualidad, que cambian constantemente. La mayor parte de los algoritmos de ruteo que se han impuesto en los años 90 son algoritmos de ruteo dinámico, los cuales se adaptan a las circunstancias cambiantes en la red analizando los mensajes entrantes de actualización del ruteo. Si el mensaje indica que se ha presentado un cambio en la red, el

software de ruteo recalcula las rutas y envía nuevos mensajes de actualización de ruteo. Estos mensajes penetran la red y, al hacerlo, estimulan a los ruteadores a correr de nuevo sus algoritmos y cambiar sus tablas de ruteo de acuerdo con las circunstancias.

Los algoritmos de ruteo dinámico se pueden complementar con rutas estáticas cuando sea conveniente. Un ruteador de último recurso ( o sea aquél al que se envían todos los paquetes no ruteados), por ejemplo, puede ser diseñado para que actúe como un dispositivo de almacenamiento de todos los paquetes que no se han podido rutear y de esta manera garantizar que todos los mensajes sean procesados al menos de alguna forma.

## UNA SOLA TRAYECTORIA *VERSUS* MULTITRAYECTORIA

Algunos protocolos sofisticados de ruteo soportan múltiples trayectorias hacia el mismo destino. A diferencia de los algoritmos de una sola trayectoria, estos algoritmos de multitrayectoria permiten el multiplexaje de tráfico a través de múltiples líneas. Las ventajas de los algoritmos de multitrayectoria son evidentes: proporcionan confiabilidad y rendimiento eficiente total sustancialmente mejores.

## PLANOS *VERSUS* JERÁRQUICOS

Algunos algoritmos de ruteo operan en un espacio plano en tanto que otros utilizan jerarquías de ruteo. En un sistema que utilice ruteo plano, todos los ruteadores son equivalentes entre sí. En un sistema de ruteo jerárquico, algunos ruteadores forman lo que constituye una troncal de ruteo. Los paquetes de los ruteadores que no pertenecen a la troncal viajan hacia los ruteadores de la troncal, a donde son enviados a través de la tronal hasta que alcanzan el área general del destino. En este punto, viajan desde el último ruteador de la troncal a través de uno o más ruteadores que no pertenecen a la troncal hacia el destino final.

Los sistemas de ruteo suelen designar grupos lógicos de nodos, llamados dominios, sistemas autónomos y áreas. En los sistemas jerárquicos, algunos ruteadores pertenecientes a un dominio se pueden comunicar con ruteadores de otros dominios, en tanto que otros más sólo se pueden comunicar con ruteadores pertenecientes a su dominio. En redes muy grandes puede haber niveles jerárquicos adicionales, donde los ruteadores del nivel jerárquico más alto forman la troncal de ruteo.

La ventaja principal del ruteo jerárquico es que imita a la organización de la mayor parte de las compañías y, por lo tanto, soporta muy bien sus patrones de tráfico. La mayor parte de la comunicación de red se da en grupos pequeños dentro de la compañía (dominios). Como los ruteadores de intradominio necesitan conocer solamente a otros ruteadores dentro de su dominio, sus algoritmos de ruteo pueden simplificarse y, dependiendo del algoritmo de ruteo que se esté utilizando, el tráfico de actualización del ruteo puede disminuir en la misma medida.

## HOST INTELIGENTE *VERSUS* RUTEADOR INTELIGENTE

Algunos algoritmos de ruteo suponen que el nodo terminal de origen determinará la ruta completa. A esto se le conoce en general como ruteo de origen. En los sitemas que utilizan el ruteo de origen, los ruteadores solamente actúan como dispositivos de almacenar y enviar: envían el paquete al punto siguiente sin pensarlo.

Otros algoritmos suponen que los hosts no saben nada acerca de las rutas. En estos algoritmos, los ruteadores determinan la trayectoria a través de la red con base en sus propios cálculos. En el primer tipo de sistema, los hosts tienen la inteligencia para el ruteo; en el segundo, son los ruteadores los que la poseen.

Lo que se gana con el ruteo donde la inteligencia está en el host versus el ruteo donde la inteligencia está en el ruteador, es la optimización de la trayectoria versus el tráfico inútil. Los sistemas en que la inteligencia está en el host seleccionan las mejores rutas con más frecuencia, ya que normalmente descubren todas las rutas posibles hacia el

destino antes de que se envíe el paquete. Después, escogen la mejor trayectoria con base en la definición de "óptima" de ese sistema en particular. Sin embargo, el acto de determinar todas las rutas suele requerir un tráfico de descubrimiento muy intenso y el consumo de una gran cantidad de tiempo.

## INTRADOMINIO *VERSUS* INTERDOMINIO

Algunos algoritmos de ruteo operan solamente dentro de los dominios; otros trabajan dentro y entre dominios. La naturaleza de estos dos tipos de algoritmos es diferente. Por lo tanto, es razonable que un algoritmo óptimo de ruteo intradominio no necesariamente sea un algoritmo óptimo de ruteo interdominio.

## BASADOS EN ESTADO DE ENLACES *VERSUS* VECTOR DE DISTANCIA

Los algoritmos basados en estado de enlace (también conocidos como algoritmos abiertos de primero al ruta más corta) distribuyen la información de ruteo a todos los nodos en la red. Sin embargo, cada ruteador envía solamente la porción de la tabla de ruteo que describe el estado de sus propios enlaces. Los algoritmos basados en vector de distancia (también conocidos como algoritmos Bellman-Ford) promueven que cada ruteador envía toda o sólo una parte de su tabla de ruteo a sus vecinos. En esencia, los algoritmos basados en estado de enlaces envían pequeñas actualizaciones a todos lados, en tanto que los algoritmos basados en vector de distancia envían actualizaciones más grandes pero sólo a los ruteadores vecinos.

Como convergen más rápido, los algoritmos basados en estado de enlaces son de alguna manera menos susceptibles a los ciclos de ruteo que los algoritmos basados en vector de distancia. Por otro lado, los algoritmos basados en estado de enlaces requieren más potencia de CPU y memoria que los algoritmos basados en vector de distancia; por lo tanto, los algoritmos basados en estado de enlaces pueden ser más caros de

implementar y soportar. A pesar de sus diferencias, sin embargo, ambos tipos de algoritmos tienen un buen desempeño en casi cualquier circunstancia.

## MÉTRICAS DE RUTEO

Las tablas de ruteo contienen información que es utilizada por el software de conmutación para seleccionar la mejor ruta. Pero, ¿cómo se construyen, específicamente, las tablas de ruteo? ¿Cuál es la naturaleza específica de la información que contienen? ¿Cómo determinan los algoritmos de ruteo que una ruta es mejor que las otras?

Los algoritmos de ruteo han utilizado muchas y diferentes métricas para determinar cuál es la mejor ruta. Los algoritmos sofisticados de ruteo pueden basar la selección de rutas en múltiples medidas al combinarlas en una sola métrica (híbrida). Se han utilizado todas las métricas siguientes:

- Longitud de la trayectoria.
- Confiabilidad.
- Retardo.
- Ancho de banda.
- Carga.
- Costos de comunicación.

LA LONGITUD DE LA TRAYECTORIA es la métrica de ruteo más común. Algunos protocolos de ruteo permiten que los administradores de red asignen costos arbitrarios a cada uno de los enlaces de la red. En este caso, la longitud de la trayectoria es la suma de los costos asociados con cada uno de los enlaces por los que se pasa. Otros protocolos de ruteo definen un conteo de saltos, una métrica que especifica el número de veces que un paquete pasa a través de los productos que conforman la red, por ejemplo ruteadores, en su trayecto desde un origen hasta un destino.

LA CONFIABILIDAD en el contexto de los algoritmos de ruteo, se refiere a la dependencia (generalmente descrita en términos de la tasa de errores) de cada enlaces de la red. Algunos enlaces de red pueden caerse con mayor frecuencia que otros. Cuando falla una red, algunos enlaces en la red pueden repararse más fácil o rápidamente que otros. Cualquier factor de confiabilidad se puede tomar en cuanta en la determinación del valor de la misma, ya que son valores numéricos arbitrarios asignados generalmente a los enlaces de red por los administradores del sistema.

EL RETARDO de ruteo se refiere al periodo de tiempo que se requiere para transferir un paquete desde el origen hasta el destino a través de la red. El retardo depende de muchos factores entre los cuales se cuentan el ancho de banda de los enlaces intermedios de la red, las colas en los puertos de cada ruteador a lo largo del camino, la saturación de la red en todos sus enlaces intermedios y la distancia física a recorrer. Como el retardo es un conglomerado de algunas variables importantes, es una métrica muy común y útil a la vez.

EL ANCHO DE BANDA se refiere a la capacidad de tráfico disponible de un enlace. Si todos los demás parámetros son iguales, sería preferible un enlace Ethernet a 10 Mbps, en vez de una línea privada a 64 Kbps. Aunque el ancho de banda es una medida del rendimiento eficiente total máximo que se puede alcanzar en un enlace, las rutas que pasan a través de enlaces con un ancho de manda mayor no necesariamente son mejores rutas que las que viajan a través de enlaces más lentos. Si, por ejemplo, un enlace más rápido está muy ocupado, puede requerir más tiempo para enviar un paquete a su destino.

LA CARGA se refiere a qué tan ocupado está un recurso de la red, como un ruteador, por ejemplo. La carga se puede calcular de muchas maneras, entre otras la utilización del CPU y el número de paquetes procesados por segundo. La supervisión continua de estos parámetros puede consumir por sí misma muchos recursos.

LOS COSTOS DE COMUNICACIÓN son otra métrica importante, sobre todo porque a algunas compañías no les importa tanto el desempeño de una red como los costos de operación de la misma. A pesar de que el retardo de la línea puede ser más grande, enviarán paquetes a través de sus propias líneas en vez de hacerlo por líneas públicas, las cuales tienen un costo asociado en función del tiempo de uso.

## PROTOCOLOS DE RED

Los protocolos ruteados se transportan por medio de ruteo a través de una red. En general, los protocolos ruteados en este contexto también se conocen como protocolos de red. Estos protocolos de red desempeñan una gran variedad de funciones necesarias para la comunicación entre aplicaciones de usuario en dispositivos de origen y destino, y estas funciones pueden variar mucho entre las diversas arquitecturas de protocolos. Los protocolos de red se presentan en las cuatro capas más altas del modelo de referencia de OSI: La capa de transporte, la capa de sesión, la capa de presentación y la capa de aplicación.

Es común que haya confusión entre los términos protocolo ruteado y protocolo de ruteo. Los protocolos ruteados son aquellos que se rutean a través de una red. Algunos ejemplos de dichos protocolos son el IP (Protocolo Internet), DECnet, Apple Talk, Novell, NetWare, OSI, Banyan VINES y XNS (Xerox Network System). Los protocolos de ruteo, por otro lado, son aquellos que implementan algoritmos de ruteo. De manera más sencilla, los protocolos de ruteo dirigen los protocolos de red a través de una interred. Algunos ejemplos de estos últimos son IGRP (Protocolo de Ruteo de Compuerta Interior), IGRP Mejorado (Protocolo de Ruteo de Compuerta Interior Mejorado), el protocolo OSPF (Algoritmo Abierto de Primero la Trayectoria más Corta), EGP (Protocolo de Compuerta Exterior), BGP (Protocolo de Compuerta Fronteriza), IS-IS (Protocolo de Sistema Intermedio a Sistema Intermedio) y RIP (Protocolo de Información de Ruteo).

# CAPÍTULO 6.

# ADMINISTRACIÓN DE REDES

## PERSPECTIVA HISTÓRICA

A principio de los años 80 el uso de las redes experimentó una tremenda expansión. A medida que las compañías se dieron cuenta de los beneficios en cuanto a costo y ganancias en productividad que se derivaban de la tecnología de las redes, empezaron a agregar redes y expandir las ya existentes casi a la misma velocidad con que aparecían en el mercado las nuevas tecnologías de red y los productos. A mediados de los años 80, algunas compañías experimentaron el dolor del crecimiento, al usar tecnologías de red diferentes (y, en algunos casos, incompatibles).

Los problemas asociados con la expansión de la red afectaron tanto la administración de la operación diaria de la red como la planeación estratégica de su crecimiento. Cada nueva tecnología de red requiere su propio grupo de expertos. A principios de los años 80, la sola necesidad de contratar personal para administrar grandes redes heterogéneas creó una crisis en muchas organizaciones. Resultó entonces imperativo crear una administración de redes automatizada (incluyendo lo que se llama la planeación de la capacidad de la red) que estuviera integrada en los diversos entornos de red.

# ¿QUÉ ES LA ADMINISTRACIÓN DE REDES?

La administración de redes significa diferentes cosas para diferentes personas. En algunos casos, implica a un consultor de redes solitario que supervisa la actividad en la red con un analizador anticuado de protocolos. En otros, la administración de redes involucra una base de datos distribuida, un autosondeo de dispositivos de red y estaciones de trabajo high-end, que generar vistas gráficas en tiempo real de los cambios de la topología de la red y del tráfico. En general, la administración de la red es un servicio que utiliza una gran variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de la red a supervisar y mantener las redes.

# ARQUITECTURA DE LA ADMINISTRACIÓN DE LA RED

La mayoría de las arquitecturas de administración de la red utilizan el mismo conjunto de relaciones y estructura básicos. Las estaciones terminales (dispositivos administrados), como sistemas de computación y otros dispositivos de red, corren software que les permite enviar señales de alerta cuando descubren que hay problemas (por ejemplo, cuando se excede uno o más de los niveles de umbral fijados por el usuario). En el momento en que reciben estas señales de alerta, las entidades de administración se programan para reaccionar ejecutando una, varias o un grupo de acciones, incluyendo la notificación del operador, el registro de eventos, el corte del sistema y los intentos automáticos de reparación del sistema.

Las entidades de administración también pueden sondear a las estaciones terminales para verificar los valores de determinadas variables. El sondeo puede ser automático o iniciado por el usuario, pero los agentes en los dispositivos que se están administrando responden a todos los sondeos. Los agentes son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por último la ponen a disposición (de manera proactiva o reactiva) de las entidades de administración que forman parte de los NMSs (Sistemas de Administración de la Red)

vía un protocolo de administración de red. Entre los protocolos más conocidos de administración de redes están SNMP (Protocolo Simple de Administración de Redes) y CMIP (Protocolo de Información de Administración Común). Los proxies de administración son entidades que proporcionan información de administración de parte de otras entidades. La figura 6-1 muestra una arquitectura habitual de administración de red.

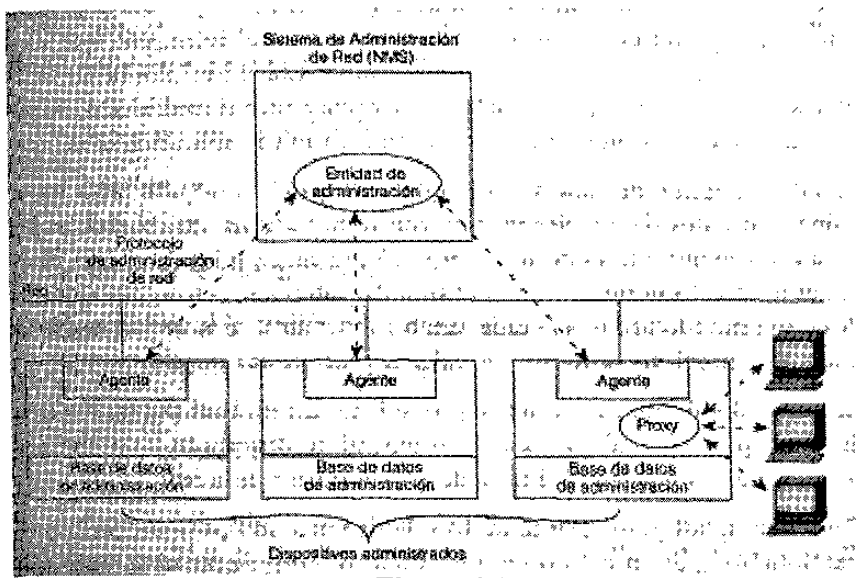



Figura 6-1

## MODELO DE ADMINISTRACIÓN DE RED DE LA ISO

La ISO ha contribuido en gran medida a la estandarización de las redes. Su modelo de administración de redes es el medio que más puede ayudar al lector a comprender las funciones principales de los sistemas de administración de redes. Este modelo consta de cinco áreas conceptuales:

- Administración del desempeño
- Administración de la configuración
- Administración de la contabilidad
- Administración de fallas
- Administración de la seguridad

# ADMINISTRACIÓN DEL DESEMPEÑO

El objetivo de la administración del desempeño es medir y hacer disponibles diferentes aspectos del desempeño de la red para que el desempeño total de la interred se pueda mantener a un nivel aceptable. Como ejemplos de las variables de funcionamiento que se pueden proporcionar están el rendimiento eficiente total de la red, los tiempos de respuesta del usuario y la utilización de la línea.

La administración del desempeño implica tres pasos principales. Primero, se reúnen los datos del funcionamiento con respecto a la variables de interés para los administradores de la red. Segundo, se analizan los datos para determinar los niveles normales (niveles base). Por último, se determinan umbrales de desempeño adecuados para cada variable importante, de modo que excederlos indique un problema de red al cual valga la pena prestar atención.

Las entidades de administración supervisan de manera continua las variables del desempeño. Cuando se excede un umbral de desempeño, se genera una señal de alerta y se envía al sistema de administración de la red.

Cada uno de los pasos que se acaban de describir son parte del proceso de establecimiento de un sistema reactivo. Cuando el desempeño de la red se hace inaceptable por haberse excedido un umbral definido por el usuario, el sistema reacciona enviando un mensaje. La administración del desempeño también permite el uso de métodos proactivos; por ejemplo, se puede utilizar una simulación de la red para hacer una proyección de cómo se verán afectados los parámetros por el desempeño del crecimiento de la red. Dicha simulación puede poner en alerta a los administradores de la red para que traten de retrasar la aparición de problemas y tomen medidas tendientes a eliminarlos.

## ADMINISTRACIÓN DE LA CONFIGURACIÓN

El objetivo de la administración de la configuración es supervisar la red, así como la información referente a la configuración del sistema, para que se puedan registrar y administrar los efectos de las diferentes versiones de los elementos de software y hardware sobre la operación de la red.

Cada dispositivo de red tiene una amplia gama de información respecto a la versión asociada con él. Una estación de trabajo de ingeniería, por ejemplo, puede configurarse de la manera siguiente:

- Sistemas operativos, Versión 3.2
- Interfase de Ethernet, Versión 5.4
- Software TCP/IP, Versión 2.0
- Software NetWare, Versión 4.1
- Software NFS, Versión 5.1
- Controlador de comunicaciones seriales, Versión 1.1
- Software X.25, Versión 1.0
- Software SNMP, Versión 3.1

Los subsistemas de administración de la configuración almacenan esta información en una base de datos para tener fácil acceso a ella. Cuando se presenta un problema, se puede buscar esta base de datos para tratar de encontrar claves que ayuden a resolver el problema.

## ADMINISTRACIÓN DE LA CONTABILIDAD

El objetivo de la administración de la contabilidad es medir los parámetros de la utilización de la red, para que el uso de la misma, tanto individual como de grupo, pueda regularse de manera adecuada. Con dicha regulación se reducen los problemas de la red (ya que los recursos de la misma pueden dividirse en cantidades iguales dependiendo de

las capacidades de los recursos) y se hace más justo el acceso a la red para todos los usuarios.

Tal como sucede con la administración del desempeño, el primer paso hacia una administración adecuada de la contabilidad es medir la utilización de todos los recursos importantes de la red. El análisis de los resultados permite hacerse una idea de los patrones de uso actuales y en ese punto, establecer cuotas de uso. Por supuesto, será necesario hacer correcciones para alcanzar las prácticas de acceso óptimo. A partir de este punto, la medición del uso del recurso puede proporcionar información de facturación, así como información que servirá para analizar continuamente la utilización óptima y justa de los recursos.

## ADMINISTRACIÓN DE FALLAS

El objetivo de la administración de fallas es detectar, registrar, notificar a los usuarios y (en la medida de lo posible) arreglar automáticamente los problemas de la red para mantenerla en operación de manera eficiente. Como las fallas pueden dejar fuera a la red o causar una degradación inaceptable de la misma, la administración de fallas es quizás uno de los elementos de la administración de redes ISO de mayor implementación.

La administración de fallas implica, en primera instancia, la determinación de los síntomas y el aislamiento de problema. Entonces se repara el problema y se prueba la solución en todos los subsistemas importantes. Por último, se registran la detección y la solución del problema.

## ADMINISTRACIÓN DE LA SEGURIDAD

El objetivo de la administración de la seguridad es controlar el acceso a los recursos de la red de acuerdo con los lineamientos locales, para que la red no pueda ser saboteada (intencional o no intencionalmente) y que personal sin autorización no tenga acceso a información de alta seguridad. Por ejemplo, un subsistema de administración de la

seguridad puede supervisar el acceso a un recurso de la red, y niega el acceso a usuarios que no ingresen los códigos de acceso correctos.

Los subsistemas de administración de la seguridad funcionan dividiendo los recursos de la red en áreas autorizadas y no autorizadas. Para algunos usuarios, el acceso a cualquier recurso de la red está prohibido, principalmente porque dichos usuarios son, en general, gente ajena a la compañía. A otros usuarios (internos) de la red, se les pude rehusar el acceso a la información que se origina desde un departamento en particular. El acceso a los archivos de recursos humano, por ejemplo, puede ser denegado a los usuarios que no pertenezcan al departamento de recursos humanos.

Los subsistemas de la administración de la seguridad llevan a cabo varias funciones. Identifican los recursos de alta seguridad dentro de la red (incluyendo sistemas, archivos y otras entidades) y determinan los mapeos entre los recursos de alta seguridad de la red y los grupos de usuarios. También supervisan los puntos de acceso de los recursos de alta seguridad de la red y registran el acceso no autorizado a los mismos.

# CAPÍTULO 7.

# TECNOLOGÍAS ETHERNET

## ETHERNET E IEEE 802.3

La red Ethernet es una especificación de LAN banda base inventada por la empresa Xerox Corp., que opera a 10 Mbps y utiliza CSMA/CD (Método de Acceso Múltiple con Detección de Portadora) a través de cable coaxial. Ethernet fue creada por Xerox en la década de los 70. Sin embargo, actualmente este término se utiliza para referirse a todas las LAN que utilizan CSMA/CD. La red Ethernet se diseñó para que operara en redes que requirieran manejar tra´fico esporádico y ocasionalmente alto, y la especificación IEEE802.3 se desarrolló en 1980 con base en la tecnología original de Ethernet. La versión 2.0 de Ethernet fue desarrollada conjuntamente por las compañías Digital Equipment Corp., Intel Corp. y Xerox Corp. Es compatible con el IEEE 802.3. La figura 7-1 muestra una red Ethernet.

En general, las redes Ethernet e IEEE 802.3 se implementan ya sea en una tarjeta de interfase o en el hardware de una tarjeta de circuito impreso principal. Las convenciones de cableado de Ethernet especifican el uso de un transceptor para conectar el cable al medio físico de transmisión de la red. El transceptor desempeña la mayor parte de las funciones de la capa física, incluyendo la detección de colisiones. El cable transceptor conecta las estaciones terminales a un transceptor.

La especificación IEEE 802.3 presenta una gran variedad de opciones de cableado; una de ellas es la que se conoce como 10Base 5. Esta especificación es la más cercana a Ethernet. Al cable de conexión se le conoce como AUI (Interfase de la Unidad de Conexión), y al dispositivo de conexión a la red se le llama MAU (Unidad de Conexión a Medios), en vez de transceptor.

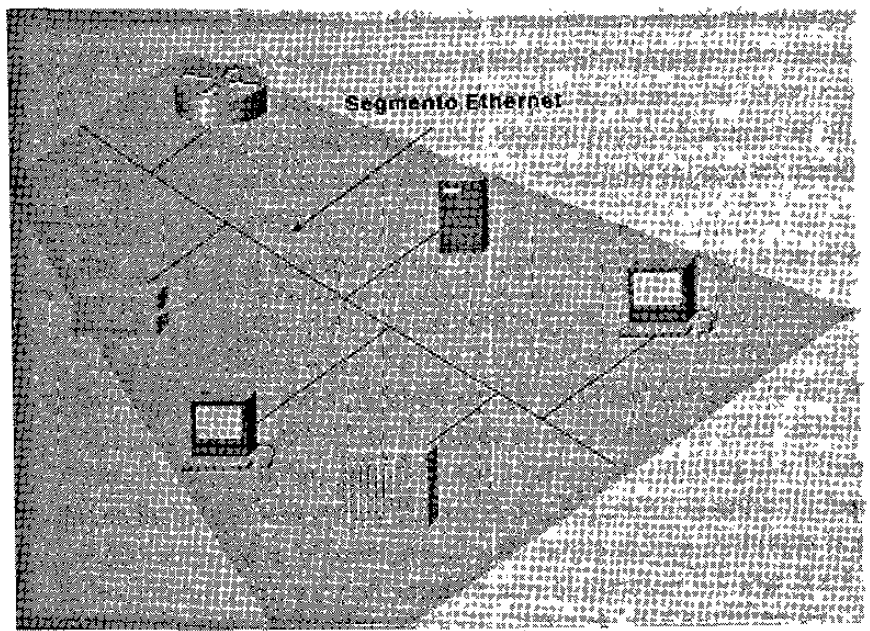



Figura 7-1

## OPERACIÓN DE ETHERNET Y DE IEEE 802.3

En un entorno Ethernet basado en difusiones (broadcast), todas las estaciones ven todas las tramas que están circulando por la red. Después de que alguna estación realiza una transmisión, las demás estaciones deben analizar cada trama para determinar si alguna de ellas es el destino de la trama. Cuando se identifica que alguna trama está dirigida a una determinada estación, se le transfiere a un protocolo de las capas superiores.

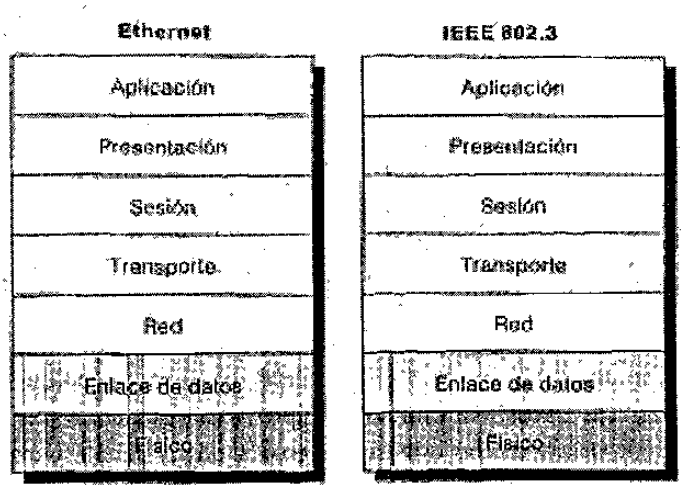
En el proceso de acceso al medio de transmisión, CSMA/CD de Ethernet, cualquier estación en una LAN CSMA/CD puede accesar la red en cualquier momento. Antes de

enviar sus datos, las estaciones CSMA/CD escuchan para ver si hay tráfico en la red. Una estación que quiera enviar datos debe esperar hasta que ya no detecte tráfico en el medio para poder transmitir.

Como método de acceso basado en la contención, Ethernet permite que cualquier estación de la red transmita su información en cualquier momento siempre y cuando el medio se encuentre libre. Se presenta una colisión cuando dos estaciones escuchan el medio de transmisión, detectan que el canal está libre y después, transmiten de manera simultánea. En esta situación, ambos envíos serán afectados y, en consecuencia, las estaciones involucradas deberán retransmitir sus mensajes después de que haya pasado cierto tiempo. Los algoritmos de retransmisión determinan el momento en que las estaciones implicadas deben transmitir de nuevo.

## DIFERENCIAS ENTRE LOS SERVICIOS DE ETHERNET Y DE IEEE 802.3

Aunque las redes Ethernet e IEEE 802.3 son muy similares en muchos aspectos, hay ligeras variaciones en cuanto a sus servicios, lo que las hace diferentes. Los servicios que ofrece Ethernet corresponden a las capas 1 y 2 del modelo de referencia OSI, en tanto que el estándar IEEE 802.3, especifica la capa física (Capa 1) y la porción de acceso al canal de la capa de enlace (Capa 2). Además, la especificación IEEE 802.3, no define un protocolo de control de enlace lógico pero sí establece varias capas físicas, en tanto que Ethernet define solamente una. La figura 7-2 muestra la relación que existe entre Ethernet y el IEEE 802.3 con respecto al modelo de referencia OSI.



Cada protocolo de la capa física del IEEE 802.3 tiene un nombre formado por tres partes que resumen sus características. Los componentes especificados en la convención que se utilizó para asignar nombres corresponden a la velocidad, método de señalización y tipo de medio de transmisión físico de la LAN. La figura 7-3 muestra cómo se utiliza la convención para la asignación de nombres con los que se hace referencia a estos componentes.

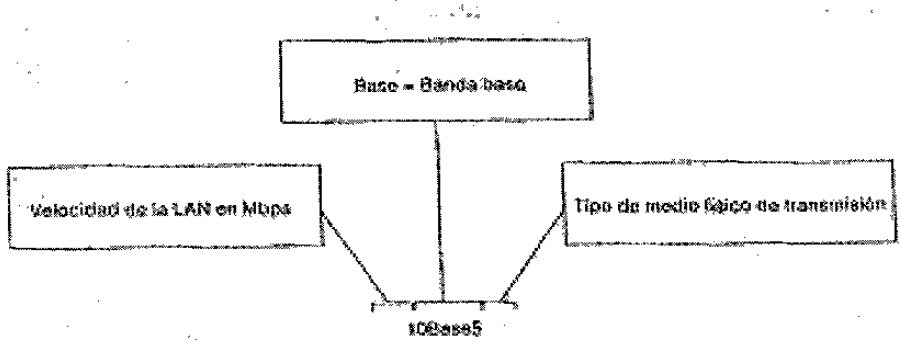



Figura 7-3

La tabla 7-1 muestra las diferencias entre Ethernet e IEEE 802.3, así como las variaciones entre las diferentes especificaciones de la capa física del IEEE 802.3.

| Características | Ethernet Valor | Valores IEEE 802.3 10Base5 | 10Base2 | 10BaseT | 10BaseFL | 100BaseT |
|---|---|---|---|---|---|---|
| Tasa de datos (Mbps) | 10 | 10 | 10 | 10 | 10 | 100 |
| Método de señalización | Banda base | Banda base | Banda base | Banda base | Banda base | Banda base |
| Ancho máximo de segmento (m) | 500 | 500 | 185 | 100 | 2,000 | 100 |
| Medios | 50-ohm coaxial | 50-ohm coaxial | 50-ohm coaxial | Cable de par trenzado sin blindaje | Fibra óptica | Cable de par trenzado sin blindaje |
| Topología | Bus | Bus | Bus | Estrella | Punto a punto | Bus |

Tabla 7-1

# FORMATOS DE TRAMA ETHERNET E IEEE 802.3

La figura 7-4 muestra los campos de la trama asociados con las tramas Ethernet e IEEE 802.3.

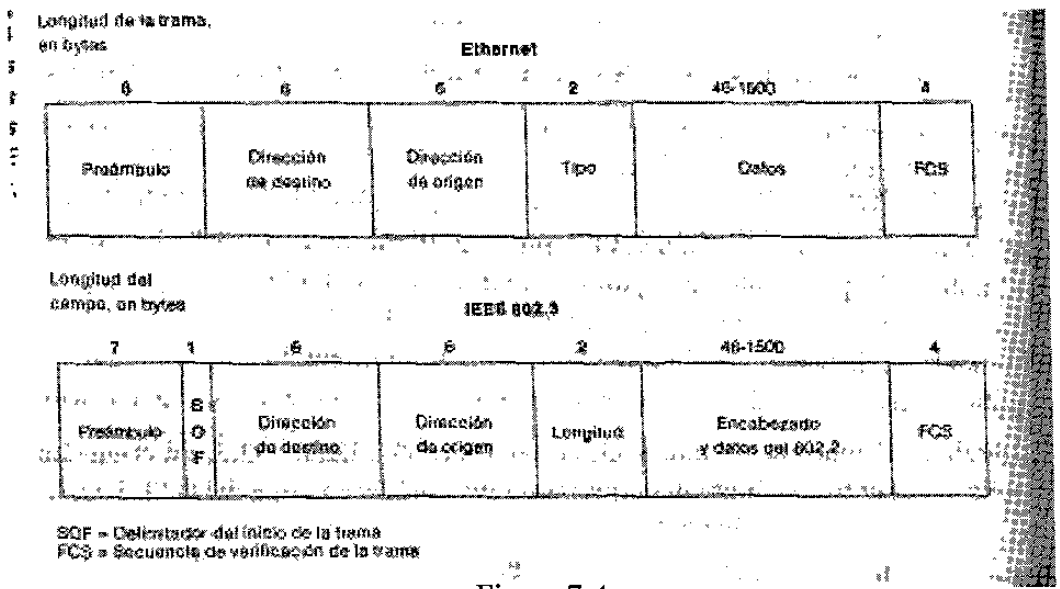



Figura 7-4

Los campos de las tramas de Ethernet y de IEEE 802.3, que se muestran en la figura 7-4, se describen en los puntos siguientes:

- Preámbulo - Es un patrón alternado de unos y ceros que informan a las estaciones de recepción que una trama está por llegar (Ethernet o IEEE 802.3). La trama de Ethernet incluye un byte adicional que es equivalente al campo. Inicio de la trama (SOF) que se especifica en la trama IEEE 802.3.
- SOF (Inicio de la Trama) - El byte delimitador en IEEE 802.3 termina con dos bits 1 consecutivos, que sirven para sincronizar las porciones de recepción de tramas de todas las estaciones de la LAN. El SOF se especifica explícitamente en Ethernet.

- Direcciones de origen y destino - Los primeros 3 bytes de las direcciones están especificados por el IEEE con base en el fabricante. Los 3 últimos bytes son especificados por el fabricante Ethernet o IEEE 802.3. La dirección de origen es siempre una dirección de unidifusión (nodo único). La dirección de destino puede ser de unidifusión, multidifusión (grupo) o difusión (todos los nodos).
- Tipo (Ethernet) - El parámetro especifica el protocolo de la capa superior que recibe los datos una vez terminado el procesamiento de Ethernet.
- Longitud (IEEE 802.3) - La longitud indica el número de bytes de datos que sigen este campo.
- Datos (Ethernet) - Terminado el procesamiento de la capa física y de la capa de enlace de datos, los datos contenidos en la trama se envían hacia un protocolo de las capas superiores, que se identifica en el campo Tipo. A pesar de que la Versión 2 de Ethernet no especifica algún relleno con bytes (en contraste con la red IEEE 802.3), Ethernet espera almenos 46 bytes de datos.
- Datos (IEEE 802.3) - Una vez terminado el procesamiento de la capa física y de la capa de enlace de datos, los datos se envían a un protocolo de las capas superiores, que deben definirse dentro de la porción de datos de la trama, si es que existe. Si los datos que contiene la trama no son suficientes para llenarla a su tamaño mínimo de 64 bytes, se insertan bytes de relleno para asegurar que la longitud de la trama sea de cuando menos 64 bytes.
- FCS (Secuencia de Verificación de Trama) - Esta secuencia tiene un valor de 4 bytes para CRC (verificación de Redundancia Cíclica), creada por el dispositivo emiosr y recalculada por el dispositivo receptor para verificar si hay tramas dañadas.

## ETHERNET A 100 Mbps

Es una tecnología LAN a alta velocidad, que ofrece un ancho de bando adicional a los usuarios de computadora de escritorio en el centro de cableado, así como a

servidores y grupos de servidores ( a los cuales se suele llamar granajas de servidores), en los centros de datos.

El grupo de estudio de la red Ethernet a alta velocidad del IEEE se formó para estudiar la factibilidad de operar Ethernet a velocidades de 100 Mbps. El grupo de estudio estableció varios objetivos para esta nueva red Ethernet de alta velocidad, pero no llegó a un acuerdo en cuanto al método de acceso. Uno de los principales problemas fue determinar si esta nueva red Ethernet, más rápida, soportaría el método CSMA/CD u otro método de acceso.

El grupo dividió esta problemática en dos partes. Por un lado, la Alianza de Fast Ethernet y, por el otro, el Foro 100Vg-AnyLan. Cada grupo generó una especificación para operar Ethernet (y Token Ring para la segunda especificación) a altas velocidades: 100 BaseT y 100VG-AnyLan, respectivamente.

100 BaseT es la especificación del IEEE para la implementación de Ethernet a 100 Mbps con UTP (Cableado de Par Trenzado SinBlindaje) y de STP (Cableado de Par Trenzado Blindado). La capa MAC (Control de Acceso a Medios) es compatible con la capa MAC del IEEE 802.3. La compañía Grand Junction, que en la actualidad es parte de WBU (Unidad de Negocios de Grupos de Trabajo) de Sistemas Cisco, desarrolló Fast Ethernet, la cual fue estandarizada por el IEEE en la especificación 802.3u.

100VG-AnyLAN es una especificación del IEEE para Ethernet y Token Ring a 100 Mbps a través de cableado UTP de par trenzado de 4 pares. La capa MAC no es compatible con la capa MAC del IEEE 802.3. La especificación 100VG-AnyLAN fue desarrollada por Hewlett-Packard (HP) para soportar nuevas aplicaciones sensibles al tiempo, como multimedia. En la especificación IEEE 802.12 está estandarizada una versión de la implementación de HP.

## GENERALIDADES DE 100Base T

La tecnología 100BaseT utiliza la especificación IEEE 802.3 CSMA/CD. Como resultado, 100BaseT conserva el formato, tamaño y mecanismo de detección de errores de la trama IEEE 802.3. Además, soporta todas las aplicaciones y software de red que actualmente corren en las redes 802.3. 100BaseT soporta velocidades de 10 y 100 Mbps utilizando FLPs (Pulsos de Enlace Rápidos) de 100BaseT. Los concentradores 100BaseT deben detectar velocidades dobles al igual que los concentradores Token Ring 4/16, sin embargo, las tarjetas de adaptación pueden soportar 10Mbps, 100Mbps o ambas. La figura 7-5 muestra cómo la subcapa MAC 802.3 y las capas superiores operan con 100BaseT, sin necesidades de modificación alguna.

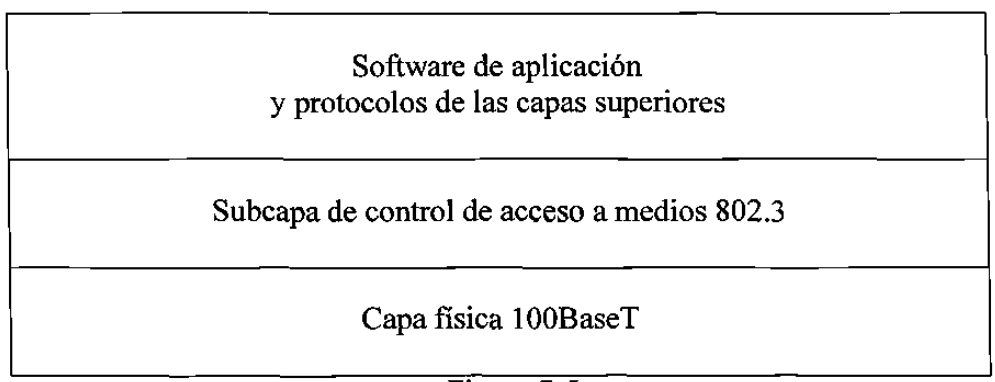



Figura 7-5

## SEÑALIZACIÓN 100Base T

La tecnología 100BaseT soporta dos tipos de señalización:

- 100BaseX
- 4T+

Ambos tipos de señalización pueden trabajar simultáneamente en los niveles de estación y concentrador. Con MII (Interfase Independiente al Medio de Transmisión), que es una interfase parecida al AUI, se obtiene interoperabilidad a nivel estación. El concentrador ofrece interoperabilidad a nivel concentrador.

El esquema de señalización 100BaseX tiene una subcapa de convergencia que adapta el mecanismo de señalización continua dúplex total de la capa PMD (Dependiente del Medio Físico) de FDDI, al tipo de señalización inicio parada, semidúplex de la subcapa MAC (Control de Acceso a Medios [físico]). El uso de 100BaseTX en la especificación FDDI ha permitido la entrega expedita de productos al mercado. 100BaseX es el esquema de señalización que se utiliza con los medios de transmisión tipo 100BaseTX y 100BaseFX. La figura 7-6 muestra cómo la subcapa de convergencia 100BaseX actúa como interfase entre los dos esquemas de señalización.

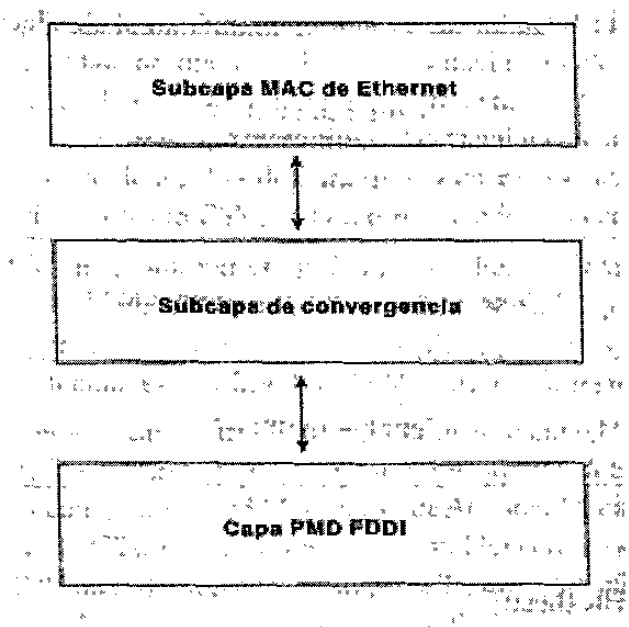



Figura 7-6

El esquema de señalización 4T+ utiliza un par de cables para la detección de colisiones y los otros tres pares para la transmisión de datos. 4T+ permite la operación de 100BaseT a través del cableado Categoría 3 existente, si los cuatro pares se instalan en la computadora de escritorio. El esquema de señalización 4T+ se utiliza con el medio de transmisión 100BaseT4 y soporta solamente operaciones dúplex total. La figura 7-7 muestra la razón de que la señalización 4T+ requiera los cuatro pares de UTP (Cableado de Par Trenzado Sin Blindaje).

# HARDWARE PARA 100Base T

Los componentes que se utilizan para la conexión física de 100BaseT son los siguientes:

- Medio físico - Este dispositivo transporta señales entre computadoras y puede ser cualquiera de los tres tipos de medios de transmisión de 100BaseT:
  - 100 Base TX
  - 100 Base FX
  - 100 Base T4

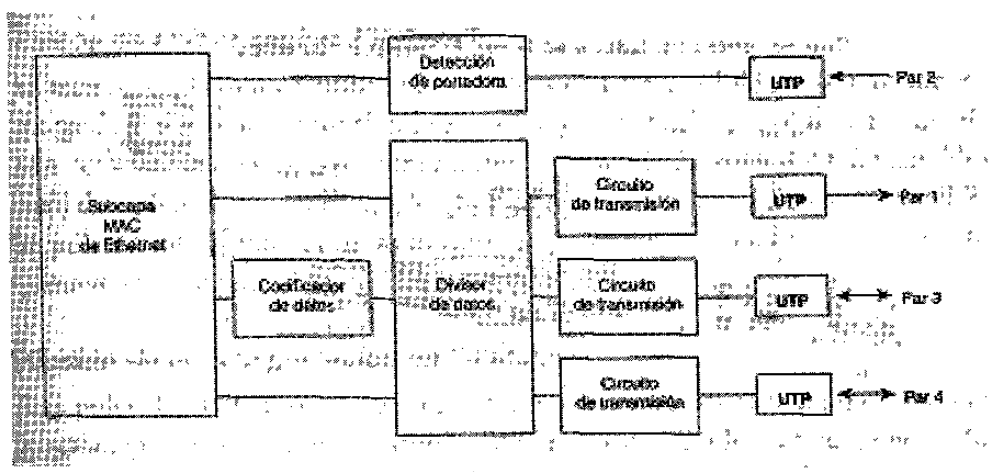



Figura 7-7

- MDI (Interfase Dependiente del Medio de Transmisión) - El MDI es una interfase mecánica y eléctrica entre el medio de transmisión y PHY.
- PHY (Dispositivo de la Capa Física) - El PHY opera a 10 o a 100 Mbps y puede estar compuesto por varios circuitos integrados (o una tarjeta hija) en un puerto Etherneto o un dispositivo externo con un cable de MII (Interfase Independiente al Medio), que se conecta a un puerto MII en un dispositivo 100BaseT (similar a un transceptor Ethernet a 10 Mbps).

- MII (Interfase Independiente al Medio) - El MII se utiliza con un transceptor externo a 100 Mbps para conectar un dispositivo Ethernet a 100 Mbps a cualquiera de los tres tipos de medios de transmisión. El MII tiene un conector de 40 patas y un cable de hasta 0.5 metros de longitud.

La figura 7-8 muestra los componentes de hardware de 100BaseT.

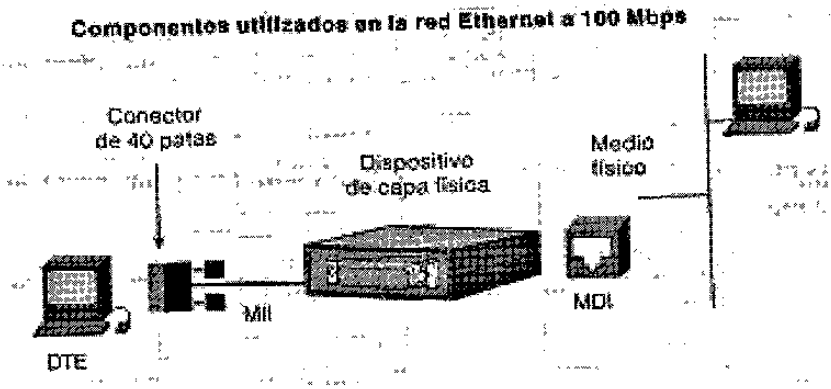



Figura 7-8

## OPERACIÓN 100Base T

Las tecnologías 100BaseT y 10BaseT utilizan los mismos métodos de acceso y detección de colisiones de MAC IEEE 802.3, y tienen también los mismos requerimientos de formato y longitud de la trama. La diferencia principal entre 100BaseT y 10BaseT (además de la diferencia en velocidad) es el diámetro de la red. El diámetro máximo de la red 100BaseT es de 205 metros, aproximadamente 10 veces menor que el de Ethernet a 10 Mbps.

Es necesario reducir el diámetro de la red 100BaseT ya que ésta utiliza el mismo mecanismo para detectar colisiones que 10BaseT. En la red 10 BaseT las limitaciones en distancia se definen para que una estación sepa, en el momento en que está transmitiendo la trama más pequeña permitida (64 bytes), que se ha presentado una colisión con otra estación emisora que está ubicada en el punto más lejano del dominio.

Para que mejore el rendimiento eficiente total de 100BaseT, es necesario reducir el tamaño del dominio de colisión. Esto se debe a que la velocidad de propagación del medio de transmisión no ha cambiado, por lo que una estación que transmite 10 veces más rápido debe estar a una distancia 10veces menor. Como resultado de lo anterior, cualquier estación puede saber si se ha presentado una colisión con cualquier otra estación de la red dentro de los primeros 64 bytes.

## PULSOS DE ENLACE RÁPIDO 110Base T

La tecnología 100BaseT utiliza FLPs (Pulsos de Enlace Rápido), para verificar la integridad del enlace entre el concentrador y el dispositivo 100BaseT. Los FLP son compatibles con las versiones anteriores de NLPs (Pulsos de Enlace Normal) de 10BaseT. Sin embargo, los FLP poseen más información que los NLP y se utilizan en el proceso de autonegociación entre un concentrador y un dispositivo en una red 100BaseT.

## OPCIÓN DE AUTONEGOCIACIÓN EN 100Base T

Las redes 100BseT soportan una característica opcional llamada autonegociación, que permite que un dispositivo y un conecentrador intercambien información (utilizando FLPs 100BaseT) respecto a sus capacidades, y al hacerlo creen un entorno óptimo de comunicaciones.

La autonegociación soporta muchas características, entre ellas la igualación de las velocidades de los dispositivos que soportan la operación a 10 Mbps y a 100 Mbps, el modo de operación full-duplex de los dispositivos que soportan dichas comunicaciones y una configuración automática de señalización para las estaciones 100BaseT4 y 100BaseTX.

# TIPOS DE MEDIOS DE TRANSMISIÓN EN 100Base T

La tecnología 100BaseT soporta tres tipos de medios de transmisión en la capa física del modelo OSI (Capa 1): 100BaseTX, 100BaseFX y 100BaseT4. Los tres tipos de medios de transmisión se pueden poner en interfase con la capa MAC del IEEE 802.3 y se muestran en la figura 7-9. En la tabla 7-2 se comparan las características fundamentales de los tres tipos de medios de transmisión de 100BaseT.

## 100Bae TX

La tecnología 100BaseTX se basa en la especificación TP-PMD (Dependiente del Medio Físico de Par Trenzado) del ANSI (Instituto Nacional de Estándares Americanos). La especificación ANSI TP-PMD soporta UTP(Cableado de Par Trenzado Sin Blindaje) y STP (Cableado de Par Trenzado Blindado). La especificación 100BaseTX utiliza el esquema de señalización 100BaseX a través de cable UTP o STP, Categoría 5 de dos pares.

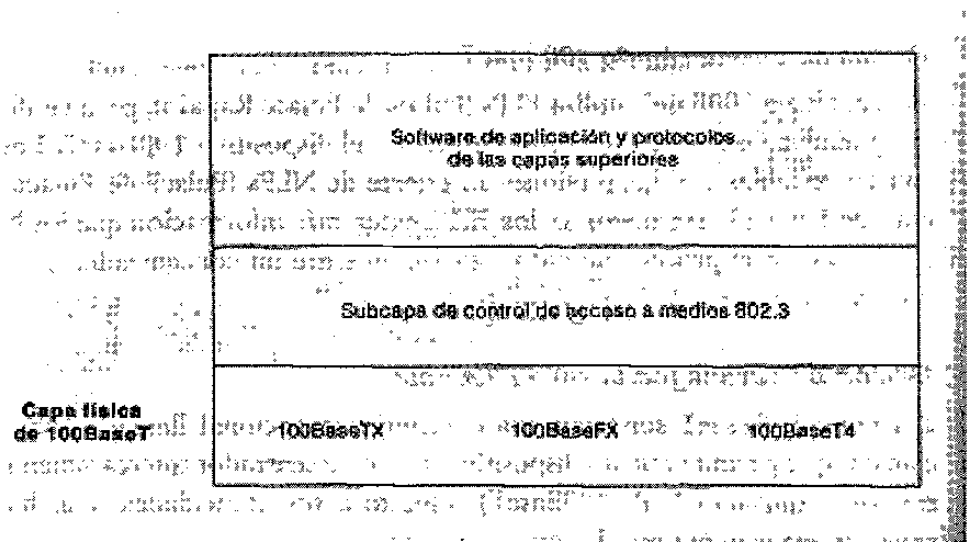



Figura 7-9

| Características | 100BaseTX | 100BaseFX | 100BaseT4 |
|---|---|---|---|
| Cable | UTP Categoría 5 o STP tipo 1 y 2 | fibra multimodo 62,5/125 | UTP categoría 3, 4 o 5 |
| Número de pares o grupos | 2 pares | 2 grupos | 4 pares |
| Conector | Conector ISO 8877 (RJ-45) | Conector (MIC) ST dúplex SC medios interfase | Conector ISO 8877(RJ-45) |
| Longitud máxima de segmento | 100 metros | 400 metros | 100 metros |
| Diámetro máximo de red | 200 metros | 400 metros | 200 metros |

Tabla 7-2

La especificación IEEE 802.3u para las redes 100BaseTX permite un máximo de dos repetidores (concentradores) y un diámetro total de la red de aproximadamente 200 metros. El segmento de enlace, que se define como una conexión punto a punto entre dos dispositivos MII (Interfase Independiente al Medio), puede ser de hasta 100 metros. La figura 7-10 muestra estas reglas de configuración.

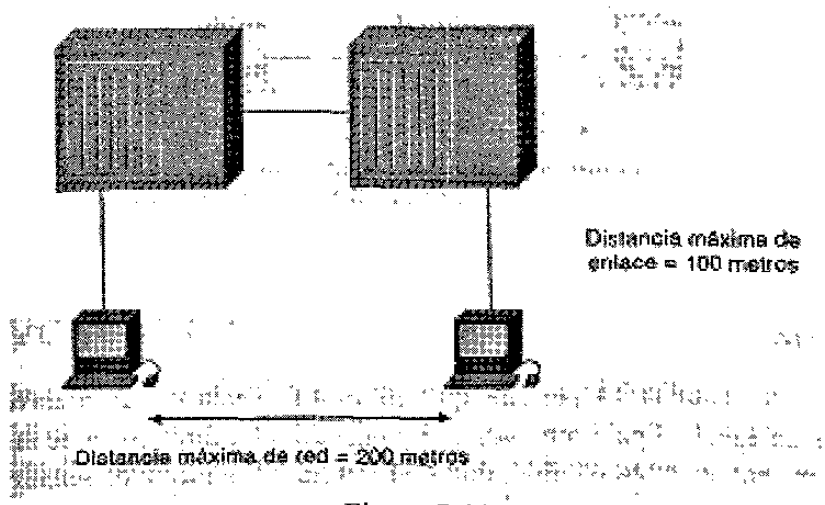



Figura 7-10

## 100Base FX

La tecnología 100BaseFX se basa en la especificación X3T9.5 de la ANSI TP-PMD (Par Trenzado Dependiente del Medio Físico) para las LANs FDDI (Interfase de Datos Distribuida por Fibra óptica). La tecnología 100BaseFX utiliza el esquema de señalización de 100BaseX a través de MMF (Cable de Fibra óptica Tipo Multimodo) de dos hilos. La especificación IEEE 802.3u para redes 100BaseFX permite enlaces DTE (Equipo Terminal de Datos) a DTE de hasta aproximadamente 400 metros o una red con base en repetidores de aproximadamente 300 metros de longitud. La figura 7-11 muestra estas reglas de configuración.

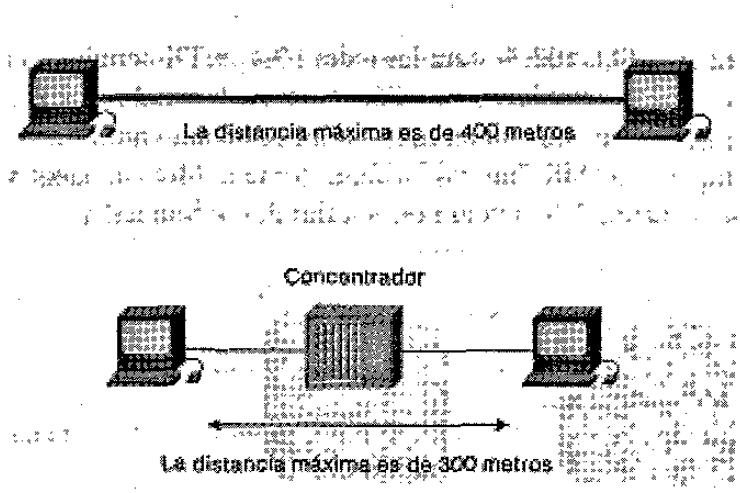



Figura 7-11

## 100Base T4

La tecnología 100BaseT4 permite que 100BaseT pueda correr a través del cableado Categoría 3 existente, siempre y cuando los cuatro pares se instalen en la computadora de escritorio. 100BaseT4 utiliza el esquema de señalización 4T+ semidúplex. La especificación IEEE 802.3u para redes 100BaseT4 permite que haya redes con un máximo de dos repetidores (concentradores) y un diámetro total de la red de aproximadamente 200 metros. Un segmento de enlace, que se define como una conexión

punto a punto entre dos dispositivos MII (Interfase Independiente al Medio), puede tener hasta 100 metros de longitud. La figura 7-12 muestra estas reglas de configuración.

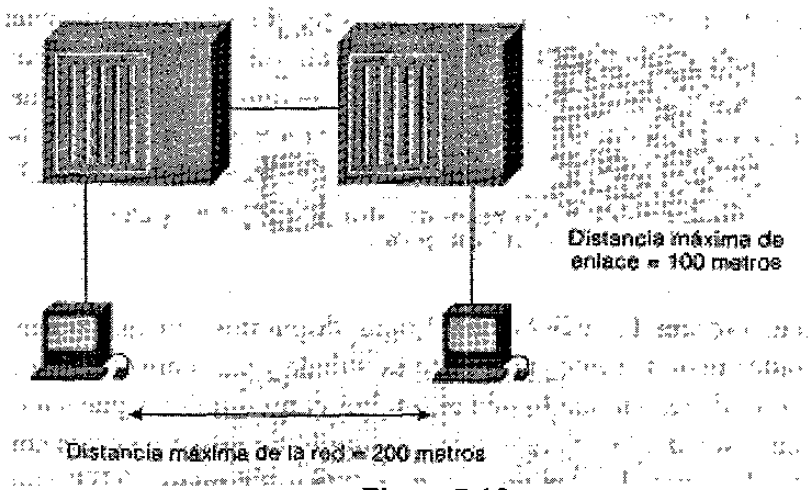



Figura 7-12

## 100VG-Any Lan

La tecnología 100VG-AnyLan fue desarrollada por Hewlett Packard (HP) como alternativa de CSMA/CD para aplicaciones novedosas sensibles al tiempo, como multimedia. El método de acceso se basa en la demanda de las estaciones y se diseñó como un método mejorado para redes Ethernet y Token Ring a 16 Mbps. La tecnología 100VG-AnyLAN funciona con los siguientes tipos de cable:

- UTP (Cableado de Par Trenzado Sin Blindaje) categoría 3 de 4 pares
- UTP categoría 4 o 5 de 2 pares
- STP (Cableado de Par Trenzado Blindado)
- Fibra óptica

El estándar del IEEE 802.12 100VG-ANyLAN especifica limitaciones en cuanto a longitud del enlace, configuraciones del concentrador y distancia máxima de la red. Las longitudes de enlace del nodo al concentrador son de 100 metros (UTP categoría 3) o de

150metros (UTP categoría 5). La figura 7-13 muestra las limitaciones de 100VG-AnyLAN en cuanto a la longitud del enlace.

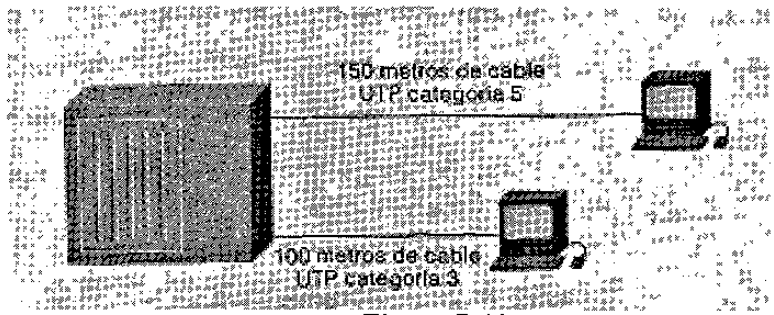



Figura 7-13

Los concentradores 100VG-AnyLAN están dispuestos jerárquicamente. Cada concentrador tiene al menos un puerto de subida y un puerto cada dos (uno sí y uno no) puede ser un puerto de bajada. Los concentradores pueden estar dispuestos en cascada de tres si están vinculados hacia arriba de otros concentradores y pueden estar alejados entre sí en cascada a 100 metros (UTP categoría 3) o a 150 metros (categoría 5). La figura 7-14 muestra la configuración de concentradores en 100VG-AnyLAN.

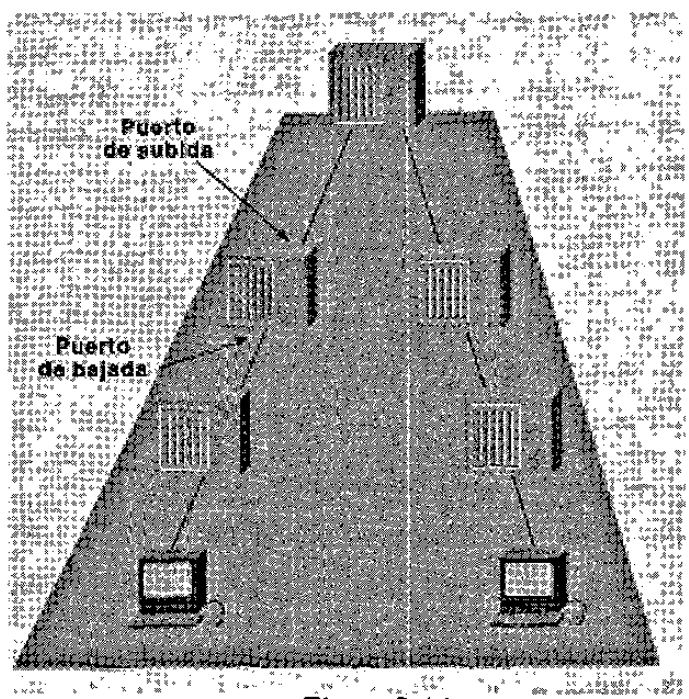



Figura 7-14

Las limitaciones en cuanto a la longitud de extremo a extremo de la red son de 600 metros (UTP categoría 3) o de 900 metros (UTP categoría 5). Si los concentradores se ubican en el mismo gabinete de cableado, las distancias de terminal a terminal se reducen a 200 metros (UTP categoría 3) y 300 metros (UTP categoría 5). La figura 7-15 muestra las limitaciones en cuanto a longitud máxima de la red 100VG-AnyLAN.

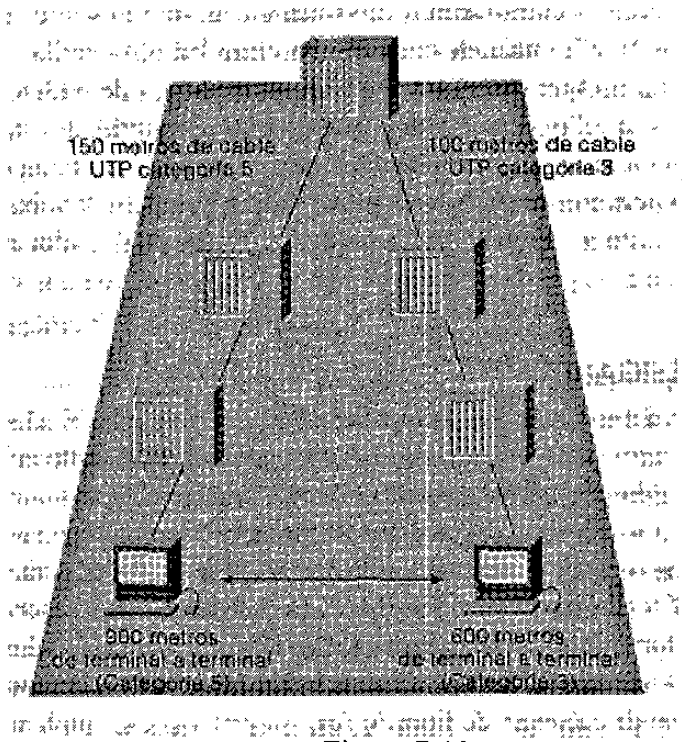



Figura 7-15

## OPERACIÓN DE 100VG-Any Lan

La tecnología 100VG-AnyLAN utiliza el método de acceso de prioridad por demanda con el que se eliminan las colisiones y permite tener una carga de tráfico mayor que 100BaseT. El método de acceso de prioridad por demanda es más determinista que CSMA/CED, debido a que el concentrador controla el acceso a la red.

El estándar 100VG-AnyLAN es un concentrador de primer nivel o repetidor, que actúa como la raíz. Este repetidor raíz controla la operación del dominio de prioridad.

Los concentradores pueden disponerse en cascada de tres en una topología en estrella. Los concentradores interconectados actúan como un solo repetidor de gran tamaño, en el que el repetidor raíz sondea cada puerto ordenadamente.

En general, en el modo de operación de prioridad por demanda de 100VG-AnyLAN, un nodo que desea transmitir solicita permiso al concentrador (o switch). Si la red está libre, el concentrador inmediatamente confirma la solicitud y el nodo comienza a transmitir un paquete hacia el concentrador. Si se recibe más de una solicitud al mismo tiempo, el concentrador utiliza la técnica de sondeo ordenado, para confirar cada solicitud que se le presente. A las solicitudes de alta prioridad, como las aplicaciones de videoconferencia, que son sensibles al tiempo, se les de prioridad de servicio con respecto a las solicitudes de prioridad normal. Para asegurar un acceso justo a todas las estaciones de la red, el concentrador no otorgará permiso de acceso a un puerto ubicado en una misma fila más de dos veces.

## ETHERNET GIGABIT

Es una extensión del estándar de Ethernet IEEE 802.3. Opera a 1000 Mbps netos de ancho de banda para datos, a la vez que conserva la compatibilidad con los dispositivos de red de Ethernet y Fast Ethernet. La red Ethernet Gigabit ofrece nuevos modos de operación dúñex total para conexiones switch a switch y switch a estación terminal. Asimismo, permite modos de operación semidúplex para conexiones compartidas utiliando repetidores y CSM/CD. Además, la red Ethernet Gigabti que se utilizan en las redes IEEE 802.3 existentes. En general, se espera que opere inicialmente a través de cableado de fibra óptica, sin embargo, se implementará con cable UTP (Par Trenzado Sin Bilindaje) categoría 5 y también con cable coaxial.

La Alianza Ethernet Gigabit es un foro abierto formado por varios fabricantes, que promueve la cooperación de la industria en el desarrollo de Ethernet Gigabit. La Alianza financia actividades encaminadas a la estandarización de Ethernet Gigabit, mismsa que están dirigidas por el grupo de trabajo IEEE 802.3, y también constribuye con recursos

técnicos para facilitar la convergencia y el consenso respecto a las especificaciones técnicas. Además, la alianza proporciona recursos para el establecimiento y demostración de la interoperabilidad de productos, así como la promoción de la comunicación mutua entre fabricantes y consumidores potenciales de productos Ethernet Gigabit.

El Grupo de Trabajo IEEE 802.3 ha formado la Fuerza de Trabajo Ethernet Gigabit 802.3z, que desarrollará un estándar Ethernet Gigabit y se adherirá a un gran número de requerimientos. Dicho estándar debe permitir la operación half-duplex y full-duplex a 1000 Mbps. Las implementaciones que sign este estándar utilizarán el formato de trama del IEEE 802.3/Ethernet, así como el método CSMA/CED para accesar el medio de transmisión. Asimismo, las implementaciones de Ethernet Gigabit serán compatibles con las versiones anteriores de 10BaseT y 100BaseT. Además, el estándar del IEEE especificará el soporte para un enlace por fibra óptica multimodo con una longitud máxima de 500 metros; un enlace por fibra óptica monomodo con una longitud máxima de 2 km; un enlace basado en cobre con una longitud máxima de al menos 25 metros. El estándar Ethernet Gigabit actuará como un complemento a los estándares 802.3 Ethernet/Fas Ethernet existentes.

## ESPECIFICACIÓN ETHERNET GIGABIT

Los esfuerzos que se están realizando en materia de estándares, se basan en la especificación de Canal de Fibra (Fibre Channel) y otros componentes de conectividad a alta velocidad. Las implementaciones iniciales de Ethernet Gigabit utilizará componentes ópticos de Canal de Fibra a 780 nm (pequeña longitud de onda) de alta velocidad para efectuar la señalización a través de fibra óptica. Los esquemas de codificación y decodificación 8B/10B se utilizarán para convertir y quitar los datos seriales. La tecnología de Canal de Fibra actualmente opera a 1.063 Gbps, pero se le está mejorando para que pueda funcionar a 1.250 Gbps y de esta manera se aposible ofrecer una velocidad total de transmisión de dtos de 1000 Mbps. Para distancias de enlace mayores, se especificarán componentes ópticos a 1300 nm (grandes longitudes de onda).

Para dar cabida a futuros avances en la tecnología del silencio y el pensamiento de señales digitales, se especificará una interfase lógica independiente del medio de transmisión entre las capas MAC y PHY que permitirá que la red Ethernet Gigabit pueda operar utilizando cable UTP (Par Trenzado Sin Blindaje). Esta interfase lógica permitirá la utilización de esquemas de codificación más adecuados para su uso con cableado UTP que se implementará de manera independiente a la codificación del Canal de Fibra. La figura 7-16 muestra los elementos funcionales de Ethernet Gigabit.

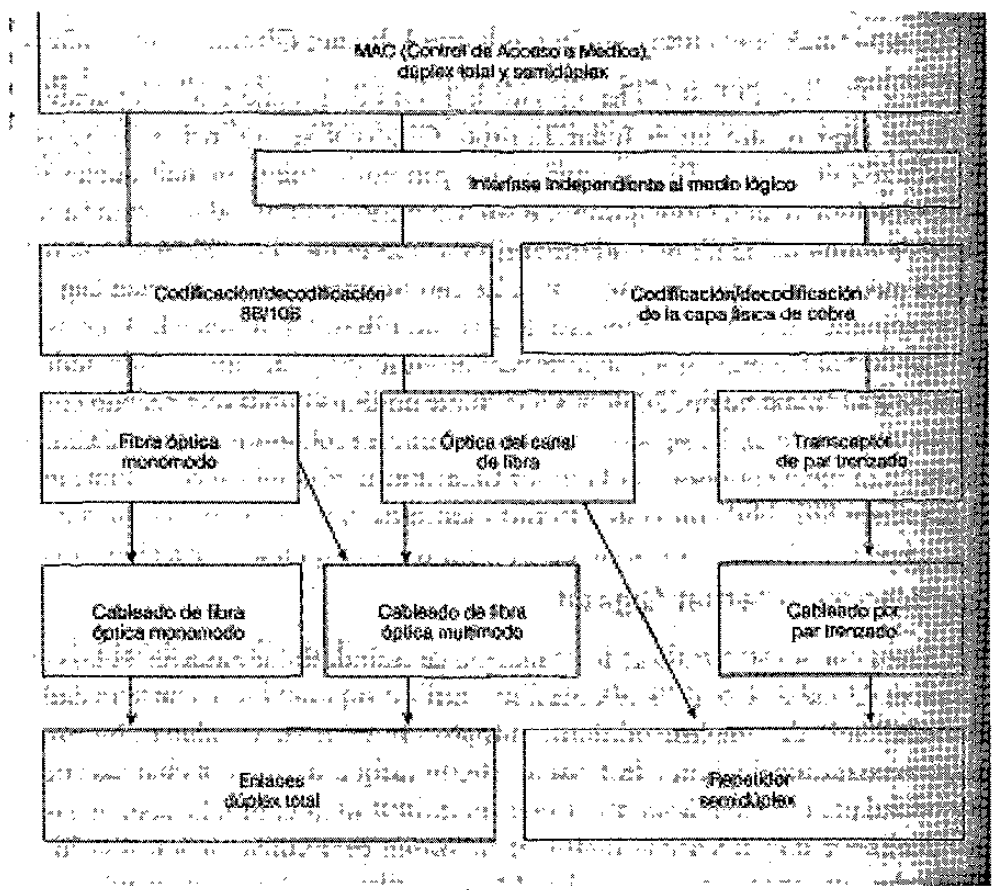



Figura 7-16

## LA MIGRACIÓN HACIA ETHERNET GIGABIT

La migración hacia Ethernet Gigabit ocurrirá gradualmente y su implementación inicial se hará en la parte troncal de las redes Ethernet existentes. Posteriormente, se actualizarán las conexiones entre los servidores de la red y, con el tiempo, las mejoras

también llegarán hasta la computadora de escritorio. Éstas son algunas acciones que probablemente se tomen para implementar la tecnología Ethernet Gigabit:

- Actualización de los enlaces de switch a switch - Los enlaces a 100 Mbps entre los switches o repetidores de Fast Ethernet pueden reemplazarse por enlaces a 1000 Mbps; con ellos se hará más veloz la comunicación entre los switches de la troncal y se permitirá que éstos soporten un número mayor de segmentos Fast Ethernet conmutados y compartidos.
- Actualización de los enlaces switch a servidor - Se pueden implementar conexiones a 1000 Mbps entre los switches y los servidores de alto desempeño. Esta actualización requerirá que a los servidores se les instalen NICs Ethernet Gigabit.
- Actualización de una Troncal Fast Ethernet - Se puede actualizar un switch de troncal de Fast Ethernet con switches 10/100 conectados para convertirse en un switch Ethernet Gigabit que soporte múltiples switches 100/1000, así como ruteadores y concentradores con interfases Ethernet Gigabit y repetidores Gigabit.

Esta medida permitiría que los servidores se conectan directamente a la troncal a través de las NICs Ethernet Gigabit; así se incrementaría el rendimiento eficiente total de los servidores de los usuarios con aplicaciones de gran ancho de banda. Una red Ethernet Gigabit podría soportar una gran cantidad de segmentos, un mayor ancho de banda por segmento y, por tanto, un mayor número de nodos por segmento.

- Actualización de una troncal de FDDI compartida - Se puede actualizar una troncal de FDDI reemplazando el concentrador FDDI, el punto de conexión o el ruteador Ethernet de FDDI a Ethernet con un switch o repetidor Ethernet Gigabit. La única actualización que se requiere es la instalación de nuevas interfases Ethernet Gigabit en los ruteadores, switches o repetidores.

- Actualización de las computadoras de escritorio de alto desempeño - Las NICs de Ethernet Gigabit se pueden utilizar para actualizar a Ethernet Gigabit las computadoras de escritorio de alto desempeño. Estas computadoras de escritorio podrían estar conectadas a switches o repetidores Ethernet Gigabit.

# CAPÍTULO 8.

# INTERFASE F.D.D.I.

## ANTECEDENTES

La FDDI (Interfase de Datos Distribuidos por Fibra óptica) especifica una LAN con topología de anillo doble, método de acceso de estafeta circulante a 100 Mbps que utiliza cable de fibra óptica. La red FDDI se suele utilizar como una tecnología de troncal a alta velocidad, ya que soporta un gran ancho de banda y distancias mayores en comparación con las tecnologías que se basan en cobre. Se debe hacer notar que en fechas relativamente recientes se liberó una especificación llamada CDDI (Interfase de Datos Distribuidos por Cobre) que se basa en cobre y ofrece servicios a 100 Mbps a través de cobre. La tecnología CDDI implementa protocolos de FDDI a través de par trenzado de cobre.

La tecnología FDDI utiliza un arquitectura de anillo doble a través del cual fluye tráfico en direcciones opuestas (llamada de giro contrario). Los anillos dobles consisten en un anillo principal y otro secundario. Durante la operación normal, el anillo principal se utiliza para la transmisión de datos, y el anillo secundario permanece libre. El propósito principal de los anillos dobles, es ofrecer una confiabilidad y robustez superiores. La figura 8-1 muestra los anillos principal y secundario de giro contrario de FDDI.

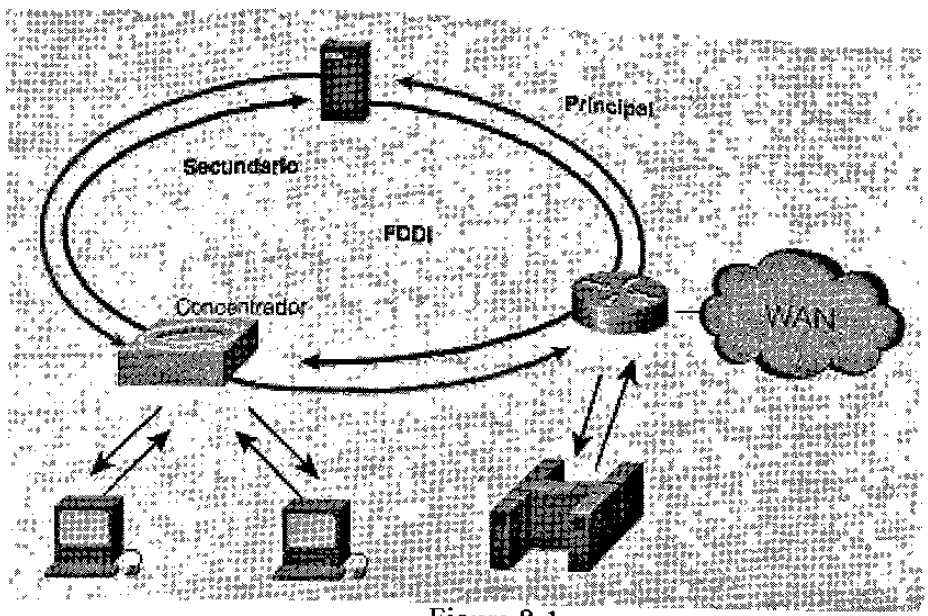



Figura 8-1

## ESTÁNDARES

La tecnología FDDI fue desarrollada por el comité estadounidense de estándares X3T9.5, ANSI (Instituto Nacional de Estándares Americanos) a mediados de los años 80. Entonces, las estaciones de trabajo de ingeniería de alta velocidad empezaban a saturar el ancho de banda de las LANs (Redes de Área Local) existentes, las cuales se basaban en Ethernet y Token Ring. Se necesitaba un nuevo medio de transmisión en las LANs que pudiera soportar fácilmente estas estaciones de trabajo y sus aplicaciones distribuidas. Al mismo tiempo, la confiabilidad de la red se había convertido en un problema de gran importancia ya que los administradores de sistemas migraron las aplicaciones críticas de computadoras grandes hacia las redes. FDDI se desarrolló con la idea de satisfacer estas necesidades. Una vez terminada la especificación FDDI, la ANSI la propuso ante la ISO (Organización Internacional de Estándares), que creó una versión internacional de FDDI totalmente compatible con la versión estándar de la ANSI.

# LOS MEDIOS DE TRANSMISIÓN DE FDDI

La tecnología FDDI utiliza la fibra óptica como medio de transmisión principal pero también puede funcionar con cable de cobre. Como se mencionó anteriormente, a la red FDDI que utiliza cobre se le conoce como CDDI (Interfase de Datos Distribuida por Cobre). La fibra óptica tiene varias ventajas sobre el medio de transmisión por cobre. En particular, seguridad, confiabilidad y desempeño, se mejoran con la fibra óptica, ya que ésta no emite señales eléctricas. Un medio de transmisión que emite señales eléctricas (por cobre) puede ser intervenido y, por lo tanto, podría permitir el acceso no autorizado a los datos que circulan por él. Además, la fibra óptica es inmune a la interferencia eléctrica causada por la RFI (Interferencia de Frecuencias de Radio) y la EMI (Interferencia Electromagnética). Históricamente, la fibra óptica ha soportado un ancho de banda (rendimiento eficiente total) mucho mayor que el cobre, aunque los avances tecnológicos recientes han hecho posible que el cobre pueda transmitir a 100 Mbps. Por último, FDDI permite una distancia de 2 kilómetros entre las estaciones si se utiliza fibra óptica multimodo, y distancias aún mayores si se utiliza fibra óptica monomodo.

FDDI define dos tipos de fibras: monomodo y multimodo. Un modo es un rayo de luz que ingresa a la fibra formando un determinado ángulo. Las fibras ópticas multimodo utilizan al LED (Diodo Emisor de Luz) como dispositivo para la generación de luz, en tanto que la fibra óptica monomodo por lo general utiliza láseres.

Las fibras ópticas mulimodo permiten la propagación de varios modos de luz a través de la fibra óptica. Como estos modos de luz ingresan a la fibra formando diferentes ángulos, llegarán al extremo de la fibra en diferentes instantes de tiempo. A esta característica se le conoce con el nombre de dispersión modal. La dispersión modal limita el ancho de banda y las distancias alcanzables utilizando fibras ópticas multimodo. Por esta razón, la fibra óptica multimodo, en general, se utiliza para efectuar conexiones dentro de un edificio o en un área geográfica limitada.

Las fibras ópticas monomodo permiten la propagación de sólo un modo de luz a través de la fibra, de modo que no hay dispersión modal en este tipo de fibra; por lo tanto, las fibras ópticas monomodo ofrecen conectividad con un desempeño considerablemente mayor a lo largo de distancias mucho más grandes, razón por la cual, en general, se utilizan para hacer conexiones entre edificios y en ambientes geográficamente dispersos.

La figura 8-2 muestra una fibra óptica monomodo que utiliza un láser como fuente de luz y una fibra óptica mulimodo que utiliza un LED como fuente de luz.

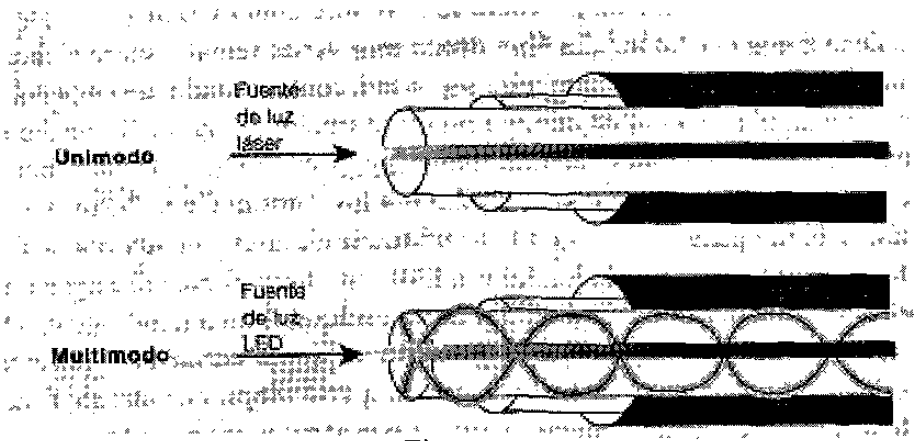



Figura 8-2

## ESPECIFICACIONES DE FDDI

FDDI especifica las partes de la capa física y la de enlace de datos del modelo de referencia de OSI. En realidad, FDDI no es una sola especificación, sino que es un grupo formado por cuatro especificaciones diferentes, cada una de las cuales cubre una determinada función. La combinación de estas especificaciones permite ofrecer conectividad a alta velocidad entre los protocolos de las capas superiores como TCP/IP e IPX, y los medios de transmisión como la fibra óptica.

Las cuatro especificaciones de FDDI son MAC (Control de Acceso a Medios), PHY (Protocolo de la Capa Física), PMD (Protocolo Dependiente del Medio Físico) y SMT

(Administración de las Estaciones). La especificación MAC define cómo se accesa el medio de transmisión, incluyendo el formato de trama, el manejo de la estafeta, el direccionamiento, los algoritmos para el cálculo del valor de CRC (Verificación de la Redundancia Cíclica) y el mecanismo de recuperación de errores. La especificación PHY define los procedimientos de codificación/decodificación, los requerimientos de temporización y el entramado, entre otras funciones. La especificación PMD define las características del medio de transmisión, incluyendo los enlaces por fibra óptica, los niveles de potencia, las tasas de error, los componentes ópticos y los conectores. La especificación SMT define la configuración de las estaciones de FDDI, la configuración del anillo y las características de control del anillo, incluyendo la inserción y remoción de la estación, la inicialización, el aislamiento y la recuperación de fallas, la programación y la reunión de estadísticas.

FDDI es similar a los estándares IEEE 802.3 Ethernet y a IEEE 802.5 Token Ring en cuanto a su relación con el modelo OSI. Su propósito principal es ofrecer conectividad entre los protocolos comunes de las capas superiores de OSI y el medio de transmisión utilizado para conectar los diferentes dispositivos de la red. La figura 8-3 muestra las cuatro especificaciones de FDDI y su relación entre sí y con la subcapa LLC (Control de Enlace Lógico) definido por el IEEE. La subcapa LLC es un componente de la Capa 2, la capa MAC, del modelo de referencia OSI.

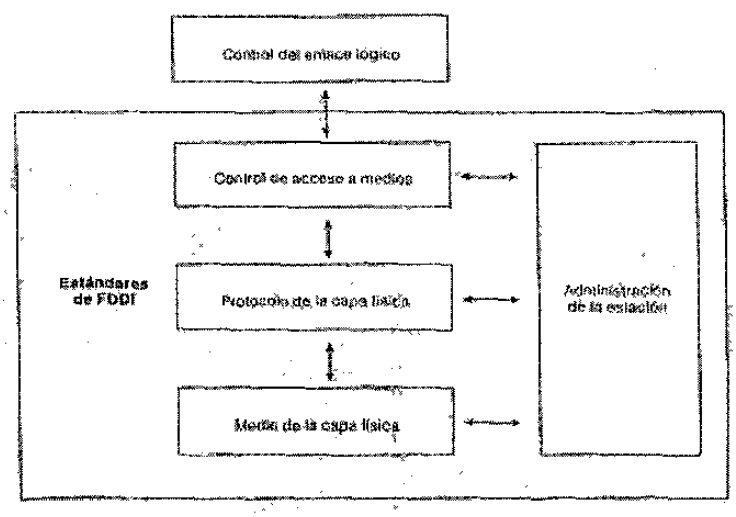



Figura 8-3

# TIPOS DE CONEXIÓN A LAS ESTACIONES DE FDDI

Una de las características inherentes del estándar FDDI es la gran variedad de modos de conectar los dispositivos a la red FDDI. El estándar FDDI define tres tipos de dispositivos: SAS (Estaciones de Una Conexión), DAS (Estaciones de Doble Conexión) y un concentrador:

Una estación SAS se conecta solamente a un anillo (el principal) por medio de un concentrador. Una de las ventajas principales de conectar dispositivos por medio de conexiones SAS es que los dispositivos no afectan de ninguna forma al anillo FDDI en caso de que sean desconectados o apagados. Los concentradores se estudiarán con más detalle en el análisis siguiente:

Cada una de las estaciones DAS en la red FDDI tiene dos puertos que se designan como A y B. Estos puertos conectan el DAS con el anillo doble de FDDI; por lo tanto, cada puerto ofrece una conexión tanto al anillo principal como al secundario. Como usted verá en la siguiente sección, los dispositivos que utilizan conexiones DAS afectarán el anillo si se desconectan o apagan. La figura 8-4 muestra los puertos A y B de la estación DAS de FDDI con conexiones hacia los anillos principal y secundario.

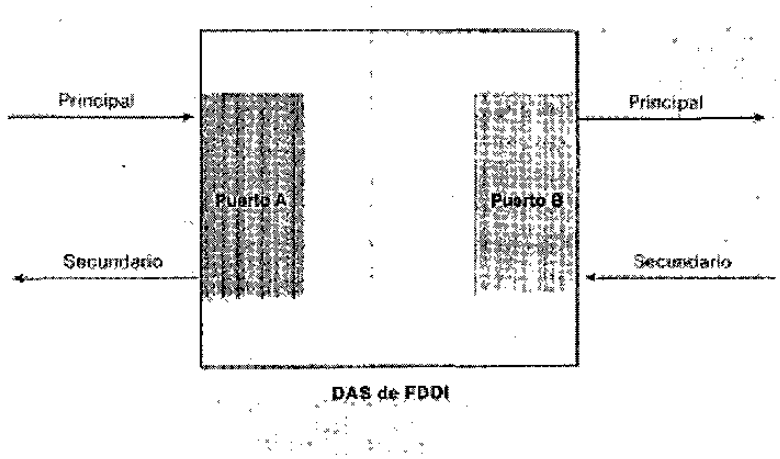


Figura 8-4

El concentrador de FDDI (también llamado DAC [Concentrador de Doble Conexión]) es el bloque principal de una red FDDI. Se conecta directamente a ambos anillos y asegura que, si cualquier SAS se encuentra en estado de falla o apagado, no afectará el anillo. Esta característica es particularmente importante cuando las PCs o dispositivos similares que se apagan y enciendan con frecuencia, se conectan al anillo. La figura 8-5 muestra las conexiones al anillo de un SAS, DAS y un concentrador de FDDI.

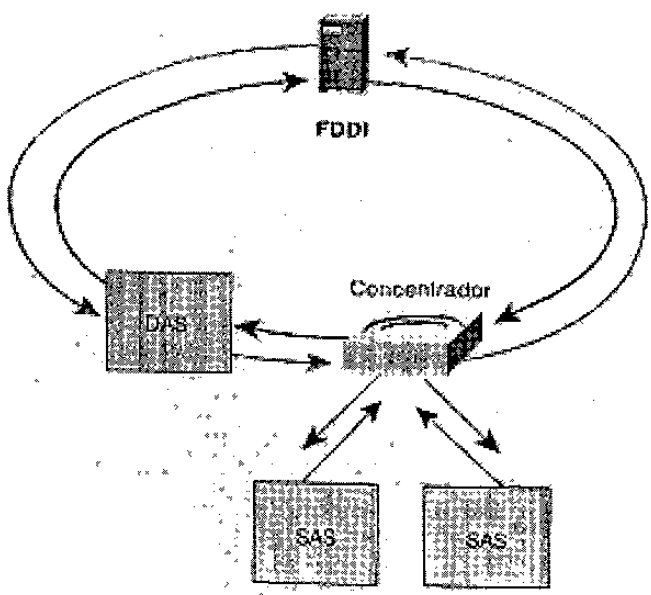



Figura 8-5

## TOLERANCIA A FALLAS EN FDDI

La red FDDI tiene varias características en cuanto a su tolerancia a las fallas. En particular, en la configuración de anillo doble de FDDI, la implementación de un interruptor óptico de desvío y el soporte de doble origen, hacen de FDDI una tecnología muy elástica en cuanto al uso de medios de transmisión se refiere.

# ANILLO DOBLE

La característica principal en cuanto a la tolerancia a las fallas de FDDI es su anillo doble. Si una estación conectada al anillo doble llega a fallar o se apaga o si se daña el cable, el anillo doble se envuelve automáticamente (en sí mismo) en un solo anillo. Al envolverse el anillo, la topología de anillo doble se convierte en una topología de un solo anillo. Los datos continúan circulando por el anillo FDDI sin que se afecte el desempeño de la red mientras se realiza la función de envoltura. Las figuras 8-6 y 8-7 muestran el efecto de la función de envoltura en FDDI.

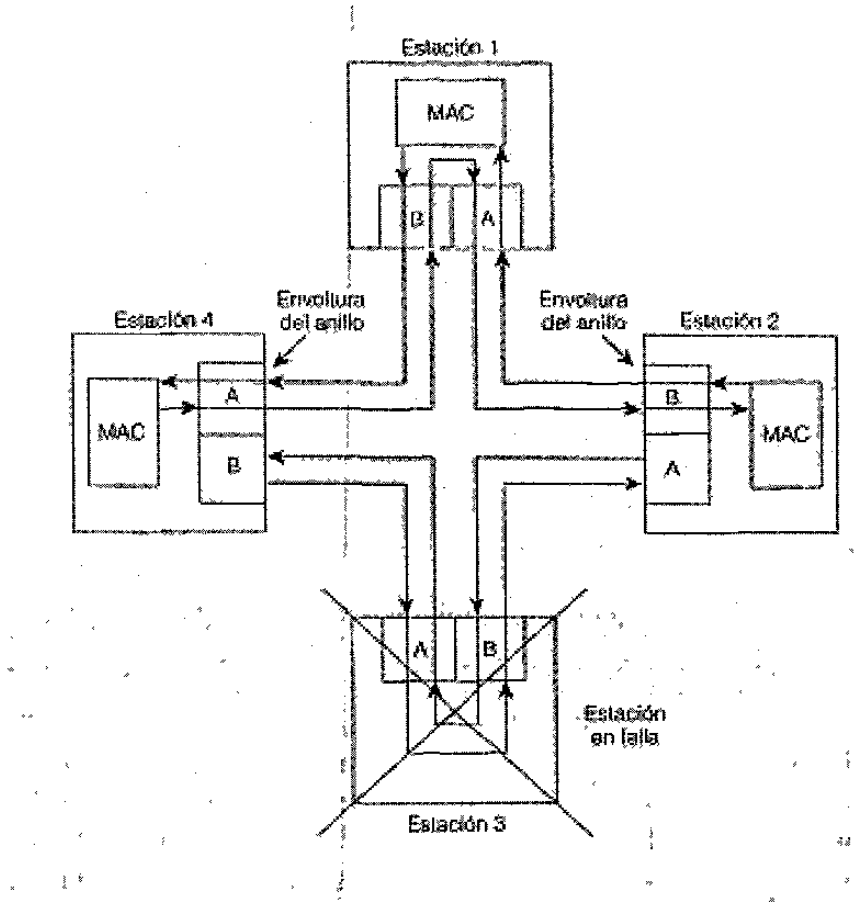



Figura 8-6

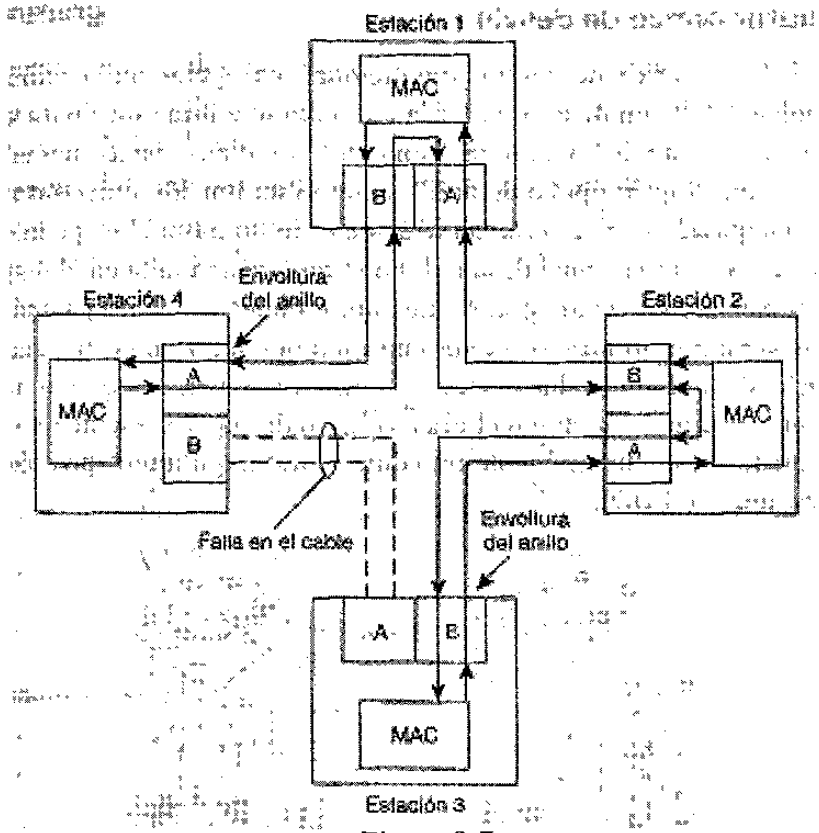



Figura 8-7

Cuando una sola estación llega a fallar, como se muestra en la figura 8-6, los dispositivos ubicados a ambos lados de la estación en estado de falla (o apagada) se envuelven, formando así un anillo doble. La operación de la red continúa con las estaciones restantes en el anillo. Cuando se presenta una falla en el cable, como se muestra en la figura 8-7, los dispositivos que están a ambos lados de la falla se envuelven. La operación de la red continúa en todas las estaciones.

Obsérvese que la red FDDI ofrece la función de tolerancia a fallas en caso de una sola falla. Cuando se presentan dos o más, el anillo FDDI se segmenta en dos o más anillos independientes, que no se pueden comunicar entre sí.

# INTERRUPTOR ÓPTICO DE DESVÍO

Un interruptor óptico de desvío proporciona una operación continua en el anillo doble si falla un dispositivo de la red. Esto se utiliza tanto para evitar la segmentación del anillo como para eliminar de la red a las estaciones en estado de falla. El interruptor óptico de desvío realiza esta función utilizando espejos ópticos que pasan la luz directamente desde el anillo hasta el dispositivo DAS durante la operación normal de la red. En el caso de una falla en el dispositivo DAS, por ejemplo que se apague, el interruptor óptico de desvío pasará la luz a través de sí mismo utilizando espejos en su interior y, por lo tanto, mantendrá la integridad en el anillo. La ventaja de esta característica es que el anillo no entrará en una condición de envoltura en el caso de que se presente una falla en un dispositivo. La figura 8-8 muestra cómo funciona un interruptor óptico de desvío en una red FDDI.

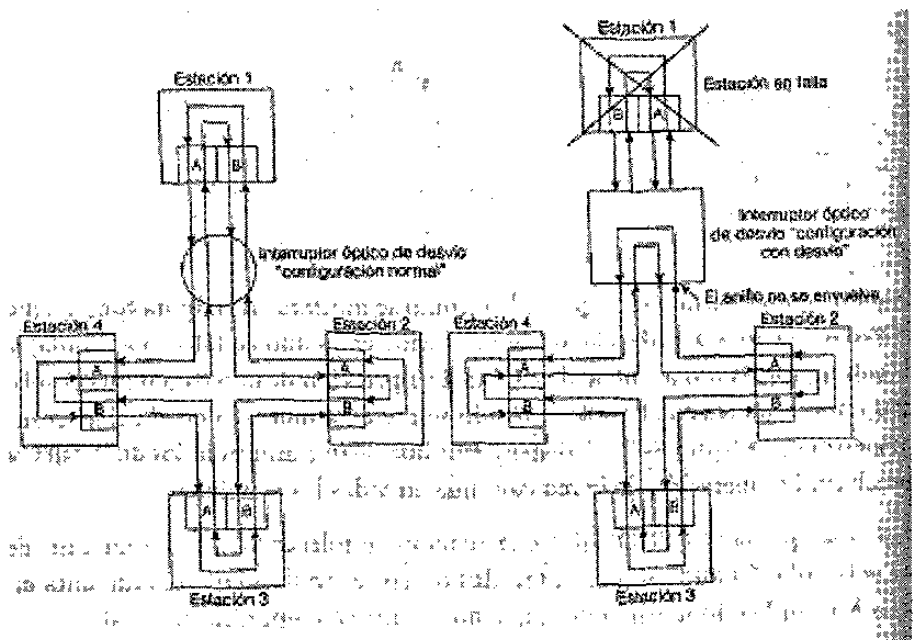



Figura 8-8

# DUAL HOMING

Los dispositivos cruciales como ruteadores o hosts de maninframes, pueden utilizar una técnica de tolerancia a fallas que se llama dual homing para ofrecer redundancia

adicional y garantizar la operación de la red. En situaciones de dual homing, el dispositivo crucial se conecta a dos concentradores. La figura 8-9 muestra una configuración de dual homing para dispositivos como servidores de archivos y ruteadores.

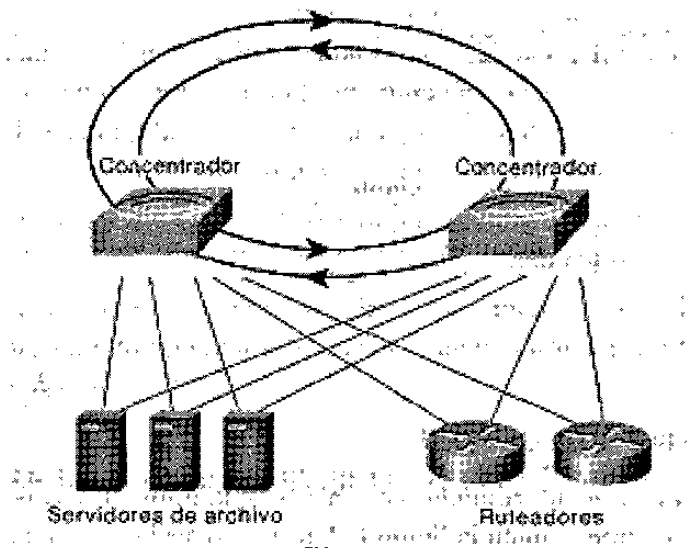



Figura 8-9

A un par de enlaces del concentrador se declara enlace activo; el otro par se declara pasivo. El enlace pasivo permanece en modo de respaldo hasta que se determina que el enlace principal (o el concentrador al que está conectado) ha fallado. Cuando se presenta esta situación, el enlace pasivo se activa automáticamente.

## FORMATO DE TRAMA FDDI

El formato es semejante al de Token Ring. Ésta es una de las áreas donde FDDI aprovecha mucho la experiencia con las tecnologías anteriores de LAN, como Token Ring. Las tramas en FDDI pueden llegar a incluir hasta 4,500 bytes. La figura 8-10 muestra el formato de trama de una trama de datos de FDDI y de una estafeta.

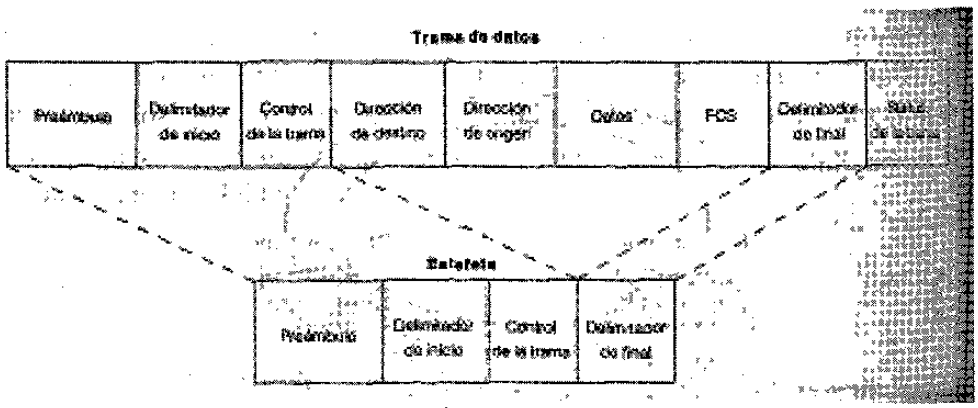



Figura 8-10

## CAMPOS DE LA TRAMA DE FDDI

Las definiciones siguientes resumen los campos de la trama de datos y la estafeta en FDDI, que se muestran en la figura 8-10.

- Preámbulo - Es una secuencia única que prepara a cada estación para recibir una trama entrante.
- Delimitador de inicio - Indica el comienzo de una trama a través de un patrón de señalización que lo diferencia del resto de la trama.
- Control de la trama - Indica el tamaño de los campos de dirección y si la trama contiene datos síncronos o asíncronos, entre otra información de control.
- Dirección de destino - Contiene una dirección de unidifusión (singular), una dirección de multidifusión (grupo) o una dirección de difusión (a todas las estaciones). Igual que con las direcciones en las redes Ethernet y Token Ring, las direcciones de destino en FDDI tienen una longitud de 6 bytes.
- Dirección de origen - Identifica a la estación que envió la trama. Tal como sucede con las direcciones Ethernet y Token Ring, las direcciones de origen de FDDI tienen una longitud de 6 bytes.
- Datos - Contienen información destinada a un protocolo de las capas superiores o información de control.

- FCS (Secuencia de Verificación de Trama) - Este campo es llenado por la estación de origen con un valor de la verificación de redundancia cíclica que se calcula en función del contenido de la trama (igual que en Ethernet y Token Ring). La dirección de destino recalcula el valor para determinar si la trama se dañó en su tránsito por la red. Si fue así, se elimina la trama.
- Delimitador del final - Este campo contiene símbolos únicos, que no pueden ser de datos, y que indican el final de la trama.
- Status de la trama - Permite que la estación de origen determine si se ha presentado un error y si la trama fue confirmada y copiada por una estación receptora.

## INTERFASE DE DATOS DISTRIBUIDA POR COBRE

La CDDI (Interfase de Datos Distribuida por Cobre) es la implementación de los protocolos de FDDI a través de par trenzado de cobre. Igual que FDDI, CDDI ofrece una tasa de transferencia de datos de 100 Mbps y utiliza una arquitectura de anillo doble para dar redundancia. La tecnología CDDI soporta distancias de aproximadamente 100 metros desde el escritorio hasta el concentrador.

La tecnología CDDI está definida por el Comité ANSI X3T9.5. El nombre oficial del estándar CDDI es TP-PMD (Dependiente del Medio Físico por Par Trenzado). También se le conoce como TP-DDI (Interfase de Datos Distribuida por Par Trenzado), que es compatible con el término FDDI (Interfase de Datos Distribuida por Fibra óptica).

La tecnología CDDI es compatible con la capa física y la capa de control de acceso a medios definido por el estándar ANSI.

El estándar ANSI especifica solamente dos tipos de cable para CDDI: el STP (Par Trenzado Blindado) y el UTP (Par Trenzado Sin Blindaje). El cableado STP tiene una impedancia de 150 ohms y se adhiere a las especificaciones de la EIA/TIA 568 (IBM Tipo 1). El cable UTP para datos (Categoría 5) consta de cuatro pares sin blindaje, con

vueltas apretadas y fue desarrollado especialmente con polímeros de aislamiento cubiertos de plástico que cumplen con las especificaciones del EIA/TIA 568B.

La figura 8-11 muestra la especificación TP-PMD de CDDI en relación con las especificaciones restantes de FDDI.

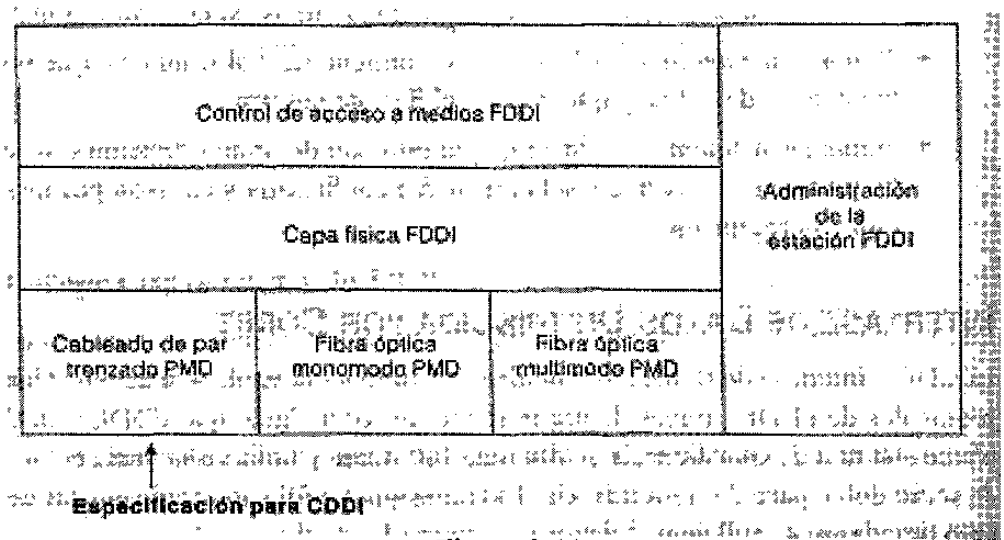



Figura 8-11

# CAPÍTULO 9.

# TOKEN RING/IEEE 802.5

## ANTECEDENTES

La red Token Ring fue desarrollada originalmente por IBM en los años 70. Aún es la principal tecnología LAN (Red de Área Local) de IBM y está sólo en segundo lugar, después de Ethernet/IEEE 802.3, entre las tecnologías de red más generalizadas. La especificación asociada IEEE 802.5 es casi idéntica y compatible totalmente con la red Token Ring de IBM. De hecho, la especificación IEEE 802.5 se constituyó después de Token Ring de IBM y continúa compitiendo con este desarrollo. En general, el término Token Ring se utiliza para referirse a la red Token Ring de IBM y a las redes IEEE 802.5. Este capítulo se ocupa de las redes Token Ring e IEEE 802.5.

Estas redes son básicamente compatibles, aunque sus especificaciones difieren sólo en detalles pequeños. La red Token Ring de IBM especifica una topología en estrella, donde todas las estaciones terminales se conectan a un dispositivo llamado MSAU (Unidad de Acceso a la Multiestación). En cambio, la especificación IEEE 802.5 no especifica ninguna topología, aunque virtualmente toda implementación de IEEE 802.5 se basa en la topología en estrella. Hay otras diferencias, entre ellas el tipo de medios (el IEEE 802.5 no los especifica, aunque las redes Token Ring de IBM utilizan cable de par

trenzado) y el tamaño del campo de información de ruteo. La figura 9-1 muestra las especificaciones de la red Token Ring de IBM y las del IEEE 802.5.

| | Red Token Ring de IBM | IEEE 802.5 |
|---|---|---|
| Tasa de datos | 4.16 Mbps | 4.16 Mbps |
| Estaciones/ segmentos | 260 (par trenzado blindado) 72 (par trenzado sin blindaje) | 250 |
| Topología | Estrella | No especificada |
| Medios | Par trenzado | No especificada |
| Señalización | Banda base | Banda base |
| Método de acceso | Estafeta circulante | Estafeta circulante |
| Codificación | Manchester diferencial | Manchester diferencial |

Figura 9-1

# CONEXIONES FÍSICAS

Las estaciones en la red Token Ring de IBM se conectan directamente a los MSAUs, los cuales pueden estar conectados por cable para constituir un anillo grande (ver figura 9-2). Los cables de conexión conectan a los MSAUs con MSAUs adyacentes, en tanto que los cables de lóbulo los conectan a las estaciones. Los MSAUs incluyen conmutadores de desviación para eliminar estaciones del anillo.

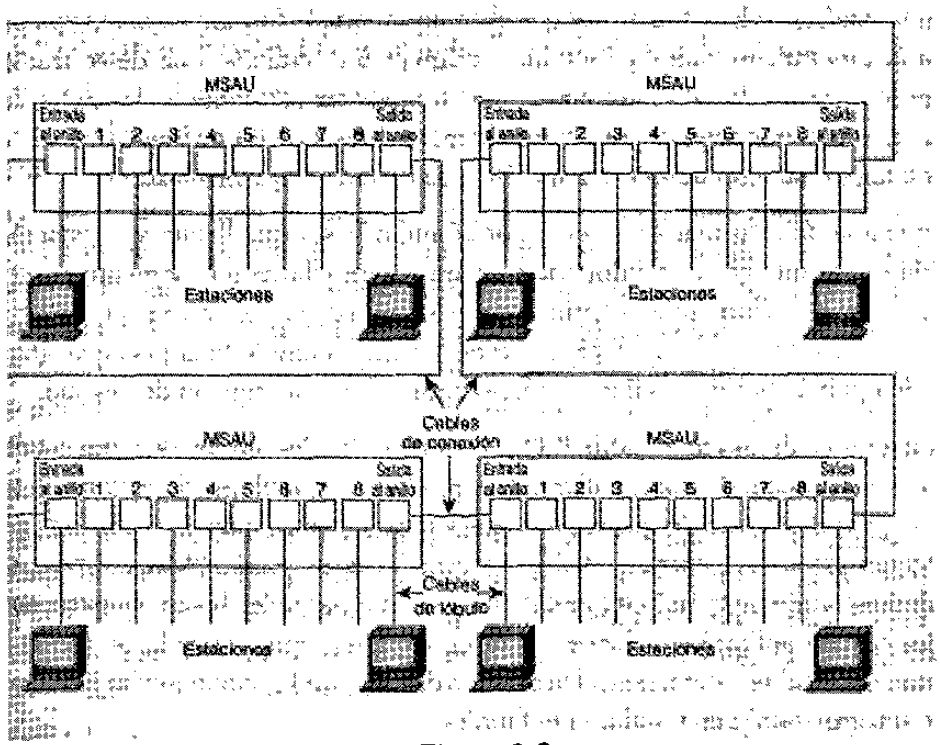



Figura 9-2

# OPERACIÓN DE TOKEN RING

Las redes Token Ring e IEEE 802.5 son dos ejemplos básicos de redes de estafeta circulante (otro ejemplo es FDDI). Las redes de estafeta circulante circulan alrededor del anillo, una trama pequeña llamada estafeta. La posesión de dicha estafeta otorga el derecho para comenzar a transmitir. Si un nodo recibe la estafeta sin información que transmitir, transfiere la estafeta a la estación siguiente. Cada estación puede tener la estafeta solamente por un período limitado de tiempo.

Cuando una estación tiene información que transmitir, toma la estafeta, cambia un bit en ella (lo cual cambia la estafeta a un estado de secuencia de inicio de trama), agrega la información que desea transmitir y la envía a la siguiente estación en el anillo. Mientras la trama de información está circulando por el anillo, no hay ninguna estafeta en la red (a menos que el anillo soporte la función de liberación previa de la estafeta), lo cual

significa que cualquier otra estación que desee transmitir deberá esperar. Por lo tanto, no se pueden presentar colisiones en las redes Token Ring. Si la red soporta la función de liberación previa de la estafeta, puede liberarse una nueva estafeta cuando la transmisión de la trama haya terminado.

La trama de información circula por el anillo hasta que llegue a la estación de destino, la que copia la información para procesarla en un momento posterior. La trama de información continúa circulando por el anillo hasta que es retirada en el momento en el que llega a la estación que la envió. Ésta puede verificar la trama para saber si fue vista y después copiada por la estación de destino.

A diferencia de las redes CSMA/CD (como Ehternet), las redes de estafeta circulante son deterministas, lo que significa que es posible calcular el tiempo máximo que tendrá que pasar antes de que alguna estación pueda transmitir. Esta característica y algunos aspectos de confiabilidad, hacen de las redes Token Ring tecnologías ideales para aplicaciones donde el retardo deba ser predecible y la operación continua de la red sea importante. Un ejemplo de dichas aplicaciones serían los entornos de automatización en instalaciones fabriles.

## SISTEMA DE PRIORIDAD

Las redes Token Ring utilizan un sofisticado sistema de prioridades que permite el uso más frecuente de la red a determinadas estaciones de alta prioridad designadas por el usuario. Las tramas Token Ring tienen dos campos que controlan la prioridad: el campo prioridad y el campo reservación.

Solamente las estaciones con una prioridad igual o mayor que el valor de prioridad contenido en la estafeta, pueden usar esa estafeta. Una vez tomada la estafeta y convertida en una trama de información, solamente las estaciones con un valor de prioridad mayor al de la estación transmisora pueden reservarla para poder hacer uso de ella la siguiente vez que la estafeta pase por dichas estaciones. Cuando se genera la

siguiente estafeta, ésta incluye la prioridad más alta de la estación que la reservó. Las estaciones que aumenten un nivel de prioridad de la estafeta deben reintegrar la prioridad anterior una vez terminada su transmisión.

## MECANISMOS PARA LA ADMINISTRACIÓN DE FALLAS

Las redes Token Ring emplean varios mecanismos para la detección y recuperación de fallas de la red; por ejemplo, se selecciona cualquier estación de la red Token Ring para que sea el supervisor activo. Esta estación, que potencialmente puede ser cualquiera en la red, actúa como una fuente centralizada de información de temporización para otras estaciones del anillo y desempeña una gran variedad de funciones de mantenimiento del anillo. Una de estas funciones es el retiro de las tramas que se quedan circulando continuamente por el anillo. Cuando un dispositivo emisor llega a fallar, su trama puede seguir circulando por el anillo. Esto puede evitar que otras estaciones transmitan sus propias tramas y, en esencia, puede llegar a trabar la red. El supervisor activo puede detectar dichas tramas, quitarlas del anillo y generar una nueva estafeta.

La topología en estrella de la red Token Ring de IBM también contribuye a mantener la confiabilidad general de la red. Como toda la información en la red Token Ring puede ser vista por los MSAU activos, éstos pueden ser programados para que verifiquen los problemas y retiren estaciones del anillo de manera selectiva si fuera necesario.

Por medio de un algoritmo de la red Token Ring llamado señalamiento se detectan y se trata de reparar ciertas fallas en la red. Siempre que una estación detecte un problema serio en la red (como una ruptura en el cable), ésta manda una trama de señalamiento, que define un dominio de falla. Este dominio incluye a la estación que está reportando la falla, su NAUN (Estación Vecina Activa más Cercana) y todo lo que se encuentre entre ambas. El señalamiento inicia un proceso llamado autorreconfiguración, donde los nodos en un dominio de falla diagnostican automáticamente, en un intento de reconfigurar la red en trono a las áreas en falla. Físicamente, el MSAU puede hacerlo por medio de la reconfiguración eléctrica.

# FORMATO DE TRAMA

Las redes Token Ring e IEEE 802.5 soportan dos tipos básicos de trama: estafetas y tramas de datos/comandos. Las estafetas son de una longitud de 3 bytes y constan de un delimitador de inicio, un byte para el control de acceso y un delimitador de final. Las tramas de datos/comandos varían en tamaño, dependiendo del tamaño del campo Información. Las tramas de datos transportan información destinada a los protocolos de las capas superiores, mientras que las tramas de comandos contienen información de control y no tienen datos destinados a los protocolos de las capas superiores. En la figura 9-3 muestran ambos formatos.

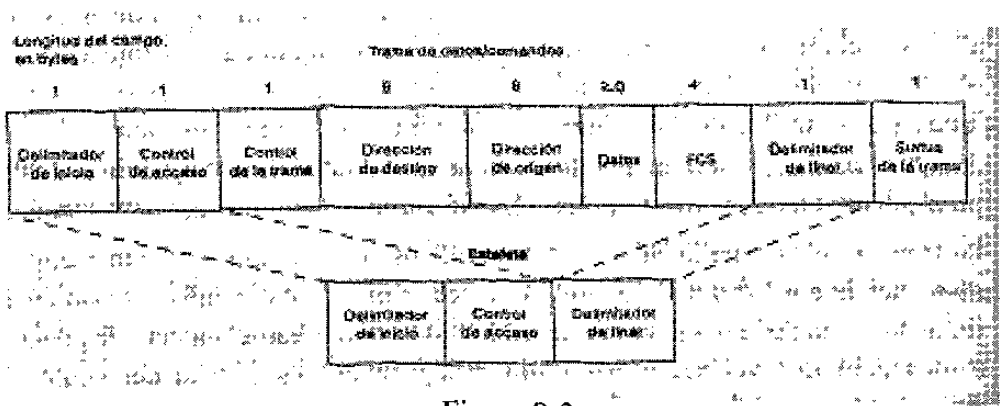



Figura 9-3

# CAMPOS DE LA TRAMA DE ESTAFETA

Los tres campos de la trama de estafeta que se muestran en la figura 9-3, se resumen en las descripciones siguientes:

- Delimitador de inicio - Avisa a cada una de las estaciones la llegada de una estafeta (o trama de datos/comandos). Este campo incluye señales que distinguen el byte del resto de la trama, violando el esquema de codificación que se utiliza en las demás partes de la trama.

- Byte de control de acceso - Contiene el campo Prioridad (los 3 bits más significativos) y el campo Reservación (al menos 3 bits significativos), así como 1 bit de estafeta (que se utiliza para diferenciar una estafeta de una trama de datos/comandos) y 1 bit de supervisión (que utiliza el supervisor activo para determinar si una trama está circulando indefinidamente por el anillo).
- Delimitador de final - Este campo indica el final de la trama de datos/comandos. Asimismo, contiene bits para señalar una trama dañada e identifica la trama ubicada al final dentro de una secuencia lógica.

## CAMPOS DE LA TRAMA DE DATOS/COMANDOS

Las tramas de datos/comandos tienen los mismos tres campos que las tramas de estafeta, más algunos otros. Los campos de la trama de datos/comandos se muestran en la figura 9-3 y se describen en los puntos siguientes:

- Delimitador de inicio - Indica a cada estación la llegada de una estafeta (o trama de datos/comandos). Este campo incluye señales que distinguen al byte del resto de la trama, violando el esquema de codificación que se utiliza en cualquier otra parte de la trama.
- Byte para el control de acceso - Este byte incluye al campo Prioridad (los 3 bits más significativos) y el campo Reservación, así como 1 bit de estafeta (utilizado para diferenciar una estafeta de una trama de datos/comandos) y 1 bit de supervisión (utilizado por el supervisor activo para determinar si una trama está circulando indefinidamente).
- Byte de control de la trama - Indica si la trama contiene datos o información de control. En las tramas de control, este byte se utiliza para especificar el tipo de información de control.
- Direcciones de origen y destino - Dos campos de dirección de 6 bytes identifican las direcciones de origen y destino de la estación.

- Datos - La longitud de este campo está limitada por el tiempo de conservación de la estafeta en el anillo, que define el máximo tiempo que una estación puede conservar la estafeta en su poder.
- FCS (Secuencia de Verificación de Trama) - Este campo es llenado por la estación origen con un valor calculado en función del contenido de la trama. La estación de destino recalcula este valor para determinar si se dañó la trama en su tránsito por el anillo. Si así fue, la trama es eliminada.
- Delimitador del final - Este campo indica el final de una estafeta o trama de datos/comandos. El delimitador del final también contiene bits para señalar una trama dañada e identificar que esta trama se ala última en una secuencia lógica.
- Status de la trama - Es un campo de 1 byte que se utiliza para terminar una trama de comandos/datos. Este campo incluye el indicador de confirmación de dirección y el indicador del copiado de la trama.

# CAPÍTULO 10.

# FRAME RELAY

## ANTECEDENTES

Frame Relay es un protocolo WAN de alto desempeño que opera en las capas física y de enlace de datos del modelo de referencia de OSI. Originalmente, la tecnología Frame Relay fue diseñada para ser utilizada a través de las ISDN (Interfases de la Red Digital de Servicios Integrados). Hoy en día, se utiliza también a través de una gran variedad de interfases de otras redes.

Frame Relay es un ejemplo de tecnología de conmutación de paquetes. En las redes que utilizan esta tecnología, las estaciones terminales comparten el medio de transmisión de la red de manera dinámica, así como el ancho de banda disponible. Los paquetes de longitud variable se utilizan en transferencias más eficientes y flexibles. Posteriormente, estos paquetes se conmutan entre los diferentes segmentos de la red hasta que llegan a su destino. Las técnicas de multiplexaje estadístico controlan el acceso a la red en una red de conmutación de paquetes. La ventaja de esta técnica es que permite un uso más flexible y eficiente del ancho de banda. La mayoría de las LAN más aceptadas en la actualidad, como Ethernet y Token Ring, son redes de conmutación de paquetes.

A veces se describe a Frame Relay como una versión compacta de X.25 con menos características a cuanto a robustez, como el ventaneo y la retransmisión de los datos más recientes, que se ofrecen en X.25. Esto se debe a que Frame Relay normalmente opera a través de instalaciones WAN que ofrecen servicios de conexión más confiables y un mayor grado de confiabilidad que los disponibles a finales de los años 70 e inicios de los 80, las cuales servían como plataformas habituales para las WANs X.25. Como se dijo anteriormente, Frame Relay es estrictamente una arquitectura de protocolos de la Capa 2, en tanto que X.25 también proporciona servicios de la Capa 3 (la capa de red). Por lo anterior , Frame Relay supera en desempeño y eficiencia en la transmisión a X.25, y la tecnología Frame Relay resulta apropiada para las aplicaciones WAN actuales, como la interconexión LAN.

## ESTANDARIZACIÓN DE FRAME RELAY

La propuesta inicial para la estandarización de Frame Relay se presentó al CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) en 1984. Sin embargo, por su falta de interoperabilidad y estandarización, Frame Relay no tuvo gran aceptación a fines de los años 80.

En 1990 ocurrió un gran desarrollo en la historia de Frame Relay cuando las compañías Cisco, Digital Equipment, Northern Telecom y StrataCom formaron un fconsorcio para aplicarse al desarrollo de la tecnología Frame Relay. Dicho consorcio desarrolló una especificación que conformó el protocolo básico de Frame Relay que se estaba analizando en el CCITT, pero ampliaba el protocolo con características que ofrecían facilidades adicionales en entornos complejos de interconectividad de redes. A estas extensiones e Frame Relay se les conoce en conjunto como LMI (Interfase de Administración Local).

Desde que la especificación del consorcio se desarrolló y publicó, muchos proveedores han anunciado su apoyo a esta definición extendida de Frame Relay. La ANSI y el CCITT estandarizaron, posteriormente, sus propias variaciones a la

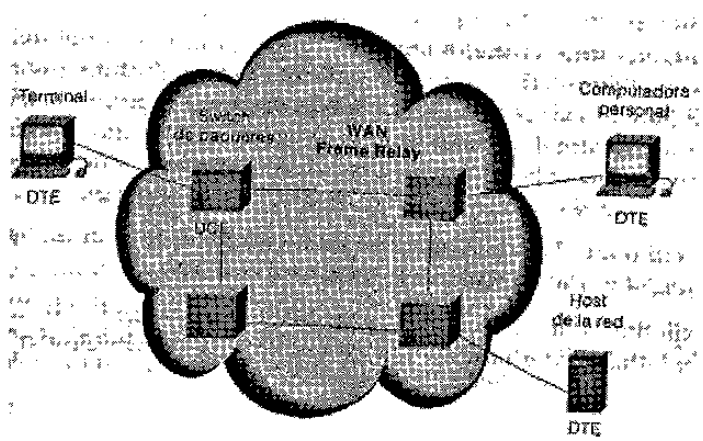
especificación LMI original, y actualmente se utilizan dichas especificaciones estandarizadas con mayor frecuencia que la versión original.

A nivel internacional, la tecnología Frame Relay fue estandarizada por la ITU-T (Unión Internacional de Telecomunicaciones, Sector Telecomunicaciones). En Estados Unidos, Frame Relay es un estándar del SIN (Instituto Nacional Americano de Estándares).

## DISPOSITIVOS DE FRAME RELAY

Los dispositivos conectados a una WAN Frame Relay caen dentro de dos categorías generales: DTE (Equipo Terminal de Datos) y DCE (Equipo de Comunicación de Datos). Los DTEs, en general, se consideran equipo de terminal para una red específica y, por lo general, se localizan en las instalaciones de un cliente. De hecho, pueden ser propiedad del cliente. Algunos ejemplos de dispositivos DTE son las terminales, computadoras personales, ruteadores y puentes.

Los DCE son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en una red, que son en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos, éstos son switches de paquetes. La figura 10-1 muestra la relación entre las dos categorías de dispositivos.



La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas, funcionales y de procedimiento para la conexión entre dispositivos. Una de las especificaciones de interfase de la capa física que más se utiliza es la especificación del RS-232 (Estándar Recomendado 232). El componente de la capa de enlace de datos define el protocolo que establece la conexión entre el dispositivo DTE, que puede ser un ruteador y el dispositivo DCE, que puede ser un switch. En esta sección se analiza una especificación de protocolo de uso común en las interredes WAN, el protocolo Frame Relay.

## CIRCUITOS VIRTUALES FRAME RELAY

Frame Relay ofrece comunicación de la capa de enlace de datos orientada a la conexión. Esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador de conexión. Este servicio se impelementa por medio de un circuito virtual Frame Relay, que es una conexión lógica creada entre dos DTE (Equipos Terminales de Datos) a través de una PSN (Red de Conmutación de Paquetes) de Frame Relay.

Los circuitos virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del DLCI (Identificador de Conexión del Enlace de datos). Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red menos compleja.

Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (switches) ubicados en la red Frame Relay PSN.

Los circuitos virtuales Frame Relay caen dentro de dos categorías: SVCs (Circuitos Virtuales Conmutados) y PVCs (Circuitos Virtuales Permanentes).

## CIRCUITOS VIRTUALES CONMUTADOS

Los SVCs son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

- Establecimiento de la llamada - Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
- Transferencia de datos - Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- Ocioso - la conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.
- Terminación de la llamada - Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual, los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Se espera que los SVC se establezcan, conserven y finalicen utilizando los mismos protocolos de señalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipo DCE Frame Relay soportan SVCs; por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

## CIRCUITOS VIRTUALES PERMANENTES

Los PVCs son conexiones establecidas en forma permanente, que se utilizan en transferencias de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de

establecimiento de llamada y finalización que se utilizan con los SVCs. Los PVC siempre operan en alguno de los estados siguientes:

- Transferencia de datos - Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- Ocioso - Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVCs, los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en un estado ocioso.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

## IDENTIFICADOR DE CONEXIÓN DEL ENLACE DE DATOS

Los circuitos virtuales Frame Relay se identifican a través de los DLCIs (Identificadores de Conexión del Enlace de Datos). Normalmente los valores de DLCI son asignados por el proveedor del servicio Frame Relay (en su caso, la compañía telefónica). Los DLCIs Frame Relay tienen un significado local, lo que significa que los valores en sí mismos no son únicos en la WAN Frame Relay; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión. La figura 10-2 muestra cómo se puede asignar a un solo circuito virtual un valor DLCI diferente en cada extremo de la conexión.

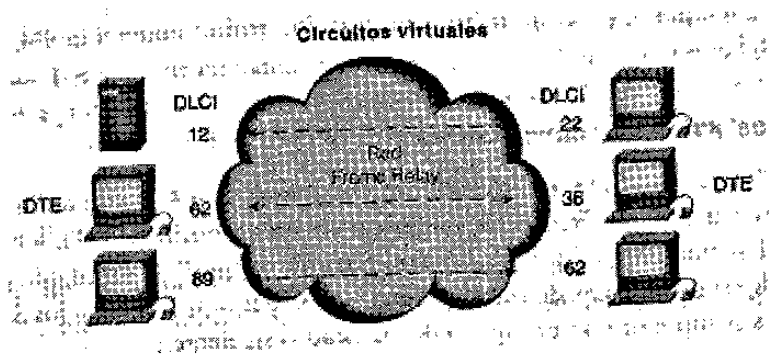



Figura 10-2

# MECANISMOS DE CONTROL DE LA SATURACIÓN

Frame Relay reduce el gasto indirecto de la red, al implementar mecanismos simples de notificación de la saturación, más que un control de flujo explícito por cada circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores. La tecnología Frame Relay implementa dos mecanismos de notificación de la saturación:

- FECN (Notificación de la Saturación Explícita Hacia Adelante)
- BECN (Notificación de la Saturación Explícita Hacia Atrás)

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de la trama Frame Relay. Éste también contiene un bit DE (Elegibilidad para Descarte), que se utiliza para identificar el tráfico menos importante que se puede eliminar durante períodos de saturación.

El bit FECN es parte del campo Direcciones en el encabezado de la trama Frame Relay. El mecanismo FECN inicia en el momento en que un dispositivo DTE envía tramas Frame Relay a la red. Si la red está saturada, los dispositivos DCE (switches) fijan el valor de los bit FECN de las tramas en 1. Cuando las tramas llegan al dispositivo DTE de destino, el campo Direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación se puede ignorar.

El bit BECN es parte del campo Direcciones en el encabezado de trama Frame Relay. Los dispositivos del DCE fijan el valor del bit BECN en 1 en las tramas que viajan en sentido opuesto a las tramas con bit FECN igual a 1. Esto permite al dispositivo DTE

receptor saber que una trayectoria específica en la red está saturada. Posteriormente, el dispositivo DTE envía esta información a un protocolo de las capas superiores para que sea procesada. Dependiendo de la implementación, el control del flujo puede iniciarse o bien se puede ignorar la indicación.

## Bit DE

El bit DE (Elegibilidad para Descarte) se utiliza para indicar que una trama tiene una importancia menor que otras. El bit DE es parte del campo Direcciones en el encabezado de la trama Frame Relay.

Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que ésta tiene una importancia menor respecto a las demás tramas. Al saturarse la red, los dispositivos DCE descartarán las tramas con el bit DE fijado en 1 antes de descartar aquellas que no la tienen. Por lo anterior disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante blindaje de saturación.

# VERIFICACIÓN DE ERRORES EN FRAME RELAY

Frame Relay utiliza un mecanismo para la verificación de errores conocido como CRC (Verificación de Redundancia Cíclica). El CRC compara dos valores calculados para determinar si se han presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores más que su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por lo que la integridad de los datos no se sacrifica si la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte más alta de Frame Relay.

# INTERFASE LMI

LMI (Interfase de la Administración Local) es un conjunto de avances en la especificación básica de Frame Relay. LMI fue desarrollada en 1990 por Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation. Presenta varias características (llamadas exstensiones) para la administración de interredes complejas. Entre las extensiones LMI más importantes de Frame Relay están el direccionamiento global, los mensajes de status de los circuitos virtuales y la multidifusión.

La extensión de direccionamiento global LMI otorga a los valores del DLCI (Identificador de la Conexión de Enlace de Datos) Frame Relay un significado global más que local. Los valores DLCI se convierten en direcciones DTE únicas en la WAN Frame Relay. La extensión global de direccionamiento agrega funcionalidad y buena administración a las interredes Frame Relay; por ejemplo, las interfases de red individuales y los nodos terminales conectados a ellos se pueden identificar por medio de técnicas estándar de descubrimiento y resolución de direcciones. Además, para los ruteadores ubicados en su periferia, toda la red Frmae Relay aparece como una típica LAN.

Los mensajes de status de los circuitos virtuales LMI permiten la comunicación y sincronización entre los dispositivos DTE y DCE Frame Relay. Estos mensajes se utilizan para reportar, de manera periódica, el status de los PVCs; así se previene el envío de datos a agujeros negros (esto es, a través de PVCs inexistentes).

La extensión de LMI para multidifusión permite que se asignen grupos de multidifusión. Con la multidifusión se ahorra ancho de banda , ya que permite que los mensajes sobre la resolución de direcciones y de actualizaciones de ruteo sean enviados solamente a grupos específicos de ruteadores. La extensión también transmite reportes sobre el status de los grupos de multidifusión en los mensajes de actualización.

# IMPLEMENTACIÓN DE LA RED FRAME RELAY

Una implementación habitual y privada de red Frame Relay consiste en equipar un multiplexor T1 con interfases Frame Relay e interfases que no sean Frame Relay. El tráfico de Frame Relay es enviado fuera de la interfase Frame Relay y hacia la red de datos. El tráfico que no es de Frame Relay se direcciona hacia la aplicación o servicio adecuados, como una PBX (Central Privada de Intercambio) de servicio telefónico o una aplicación de video teleconferencia.

Una red Frame Relay típica consta de varios dispositivos DTE, que pueden ser ruteadores, conectados hacia puertos remotos de un equipo multiplexor vía servicios tradicionales punto a punto, como T1, T1 fraccional o circuitos de 56K. En la figura 10-3 se muestra un ejemplo de una red simple Frame Relay.

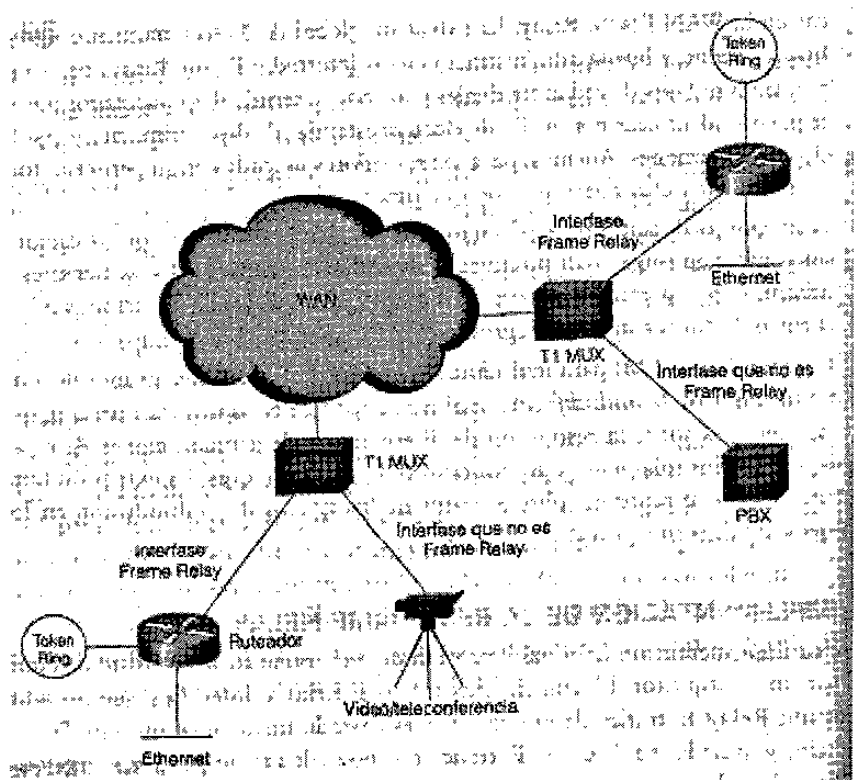



Figura 10-3

La mayoría de las redes Frame Relay que se utilizan en la actualidad son equipadas por los proveedores de servicios que ofrecen servicios de transmisión a clientes. A esto se le conoce como un servicio público de Frame Relay, pues también Frame Relay se implementa tanto en las redes públicas ofrecidas por las compañías de larga distancia, como en las redes privadas empresariales.

Se analizarán las dos metodologías para el uso de Frame Relay.

## REDES PÚBLICAS DE LARGA DISTANCIA

En las redes públicas Frame Relay de larga distancia, el equipo de conmutación Frame Relay se ubica en las centrales telefónicas de compañías de larga distancia. A los suscriptores se les cobra determinada cantidad según el uso que hagan de la red. Sin embargo, los clientes no se encargan de administrar y mantener el equipo y el servicio de la red Frame Relay.

En general, el proveedor del servicio de telecomunicaciones también es propietario del equipo DCE. El equipo DCE puede ser propiedad del cliente, o bien del proveedor del servicio de telecomunicaciones como un servicio para el usuario.

Actualmente la mayoría de las redes Frame Relay son redes públicas que suministran servicios de larga distancia.

## REDES PRIVADAS EMPRESARIALES

Las organizaciones a nivel mundial están utilizando cada vez más redes privadas Frame Relay. En las redes privadas Frame Relay, la administración y el mantenimiento de la red son responsabilidad de una empresa (o compañía privada). El cliente es el dueño de todo el equipo, incluyendo el de conmutación.

# FORMATOS DE TRAMA FRAME RELAY

Para entender mejor la funcionalidad de Frame Relay, ayuda mucho conocer la estructura de la trama de la tecnología Frame Relay. La figura 10-4 muestra el formato básico de la trama de Frame Relay y la figura 10-5 muestra la versión LMI de la misma.

Los indicadores señalan el principio y el final de la trama. La trama Frame Relay está formada por tres componentes principales: el área del encabezado y de las direcciones, la porción de los datos de usuario y la FCS (Secuencia de Verificación de Trama). El área de direcciones, que tiene una longitud de 2 bytes, se compone de 10 bits que representan al identificador del circuitos y 6 bits de los campos asociados a la administración de la saturación. Comúnmente, a este identificador se le conoce como DLCI (Identificador de la Conexión del Enlace de Datos). En las descripciones siguientes se analiza cada uno de estos elementos.

# TRAMA ESTÁNDAR FRAME RELAY

Estas tramas constan de los campos que se muestran en la figura 10-4.

Las descripciones siguientes resumen los campos básicos de la trama Frame Relay que se ilustran en la figura 10-4.

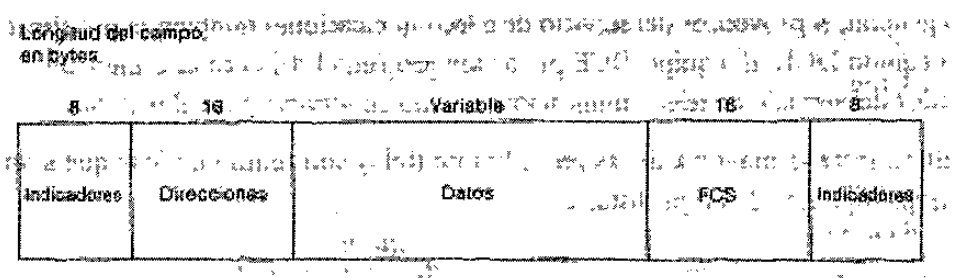



Figura 10-4

- Indicadores - Delimitan el comienzo y la terminación de la trama. El valor de este campo es siempre el mismo y se representa como el número decimal 7E o el número binario 01111110.
- Direcciones - Contiene la información siguiente:
  - DLCI: El DLCI de 10 bits es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el disposit5ivo DTE y el switch. Cada conexión virtual que se multiplexe en el canal físico será representada por un DLCI único. Los valores de DLCI tienen significado local solamente, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual.
  - EA(Dirección Extendida): La EA se utiliza para indicar si el byte cuyo valor EA es 1, es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte sea el último octeto DLCI. Aunque todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCIs más largos. El octavo bit de cada byte del campo Direcciones se utiliza para indicar el EA.
  - C/R: El C/R es el bit que sigue después del byte DLCI más significativo en el campo Direcciones. El bit C/R no está definido hasta el momento.
  - Control de la saturación: Este campo consta de 3 bits que controlan los mecanismos de notificación de la saturación en Frame Relay. Éstos son los bits FECN, BECN y DE, que son los últimos 3 bits en el campo Direcciones.

FECN (Notificación de la Saturación Explícita Hacia delante) es un campo de un solo bit que puede fijarse en un valor de 1 por medio de un interruptor para indicar a un dispositivo DTE terminal, como un ruteador, que ha habido saturación en la dirección de la transmisión de la trama del origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de

reaccionar de manera inteligente ante estos indicadores de saturación. Hoy en día, los protocolos DECnet y OSI son los únicos protocolos de las capas superiores que implementan estas características.

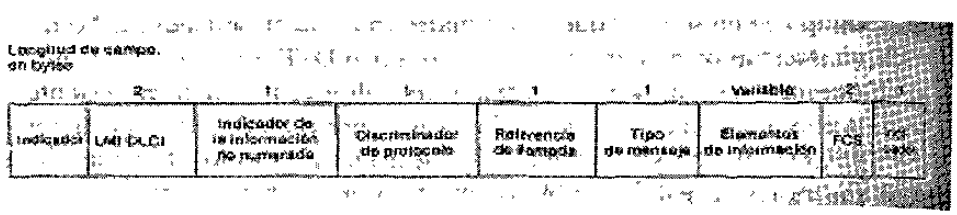
BECN (Notificación de Saturación Explícita Hacia Atrás) es un campo de un solo bit que, al ser establecido en 1 valor por un switch, indica que ha habido saturación en la red en la dirección opuesta a la de la transmisión de la trama desde el origen al destino.

El bit DE (Elegibilidad para Descarte) es fijado por el dispositivo DTE, un ruteador por ejemplo, para indicar que la trama marcada es de menor importancia en relación con otras tramas que se estén transmitiendo. En una red saturada las tramas que se marcan como "elegible para descarte" deben ser descartadas antes que cualquier otra. Lo anterior representa un mecanismo justo de establecimiento de prioridad en las redes Frame Relay.

- Datos - Los datos contienen información encapsulada de las capas superiores. Cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil que variará en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar el PDU (Paquete de Protocolos de las Capas Superiores) a través de una red Frame Relay.
- Secuencia de verificación de tramas - Asegura la integridad de los datos transmitidos. Este valor es calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión.

## FORMATO DE LA TRAMA LMI

Las tramas Frame Relay que siguen las especificaciones LMI contienen los campos



que se muestran en la figura 10-5.

Las descripciones siguientes se refieren a los campos que se ilustran en la figura 10-5:

- Indicador - Delimita el comienzo y el final de la trama.
- LMI DLCI - Identifica la trama como una trama LMI en vez de una trama básica Frame Relay. El valor DLCI específico del LMI definido por la especificación del consorcio LMI es DLCI = 1023.
- Indicador de la información no numerada - Fija el bit sondeo/final en cero.
- Discriminador de protocolos - Siempre contiene un valor que indica que es una trama LMI.
- Referencia de llamada - Siempre contiene ceros. En la actualidad este campo no se usa ni tiene ningún propósito.
- Tipo de mensaje - Etiqueta la trama con uno de los siguientes tipos de mensajes:
  - Mensaje de solicitud de status: Permite que un dispositivo de usuario solicite el status de la red.
  - Mensaje de status: Responde a los mensajes de solicitud de status. Los mensajes de status incluyen mensajes de sobrevivencia y de status del PVC.
- Elementos de información - Contiene una cantidad variable de IEs (Elementos Individuales de Información). Los IE constan de los campos siguientes:
  - Identificador IE: Identifica de manera única el IE.
  - Longitud del IE: Indica la longitud del IE.
  - Datos: Constan de uno o más bytes que contienen datos encapsulados de las capas superiores.
- FCS (Secuencia de la Verificación de Tramas) - Asegura la integridad de los datos transmitidos.