FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

A LOS ASISTENTES A LOS CURSOS

Las autoridades de la Facultad de Ingeniería, por conducto del jefe de la División de Educación Continua, otorgan una constancia de asistencia a quienes cumplan con los requisitos establecidos para cada curso.

El control de asistencia se llevará a cabo a través de la persona que le entregó las notas. Las inasistencias serán computadas por las autoridades de la División, con el fin de entregarle constancia solamente a los alumnos que tengan un mínimo de 80% de asistencias.

Pedimos a los asistentes recoger su constancia el día de la clausura. Estas se retendrán por el periodo de un año, pasado este tiempo la DECFI no se hará responsable de este documento.

Se recomienda a los asistentes participar activamente con sus ideas y experiencias, pues los cursos que ofrece la División están planeados para que los profesores expongan una tesis, pero sobre todo, para que coordinen las opiniones de todos los interesados, constituyendo verdaderos seminarios.

Es muy importante que todos los asistentes llenen y entreguen su hoja de inscripción al inicio del curso, información que servirá para integrar un directorio de asistentes, que se entregará oportunamente.

Con el objeto de mejorar los servicios que la División de Educación Continua ofrece, al final del curso deberán entregar la evaluación a través de un cuestionario diseñado para emitir juicios anónimos.

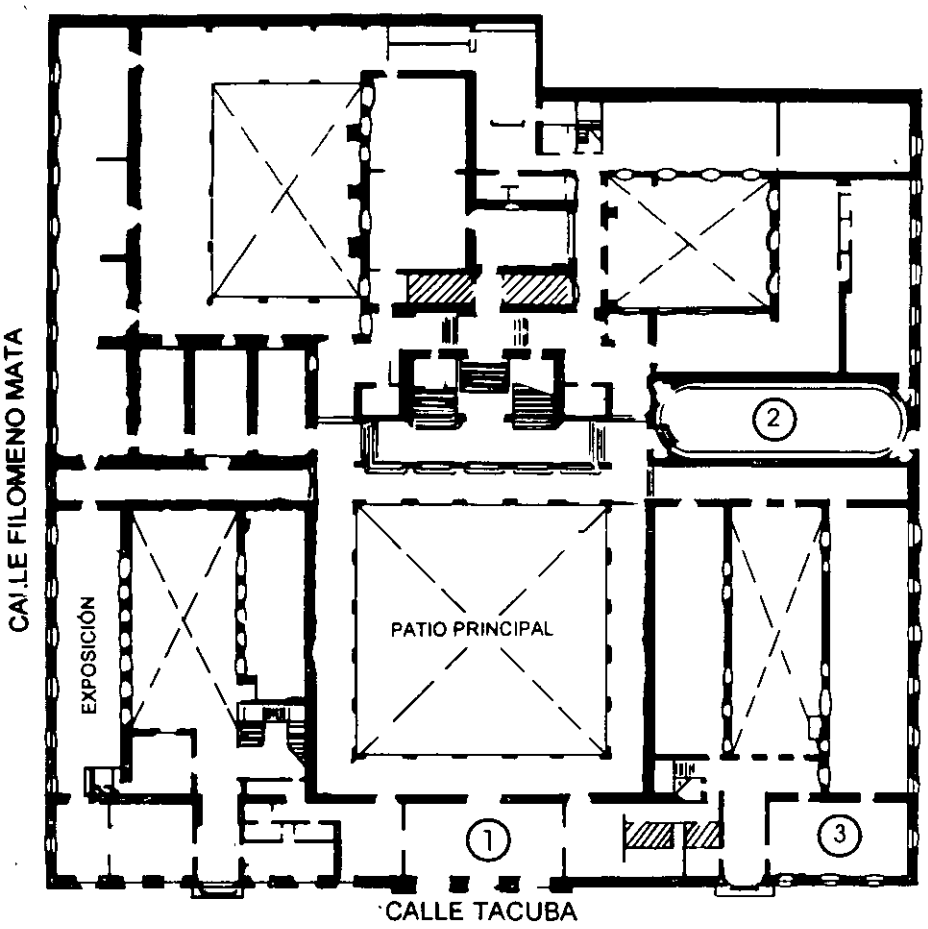
Se recomienda llenar dicha evaluación conforme los profesores impartan sus clases, a efecto de no llenar en la última sesión las evaluaciones y con esto sean más fehacientes sus apreciaciones.

Atentamente

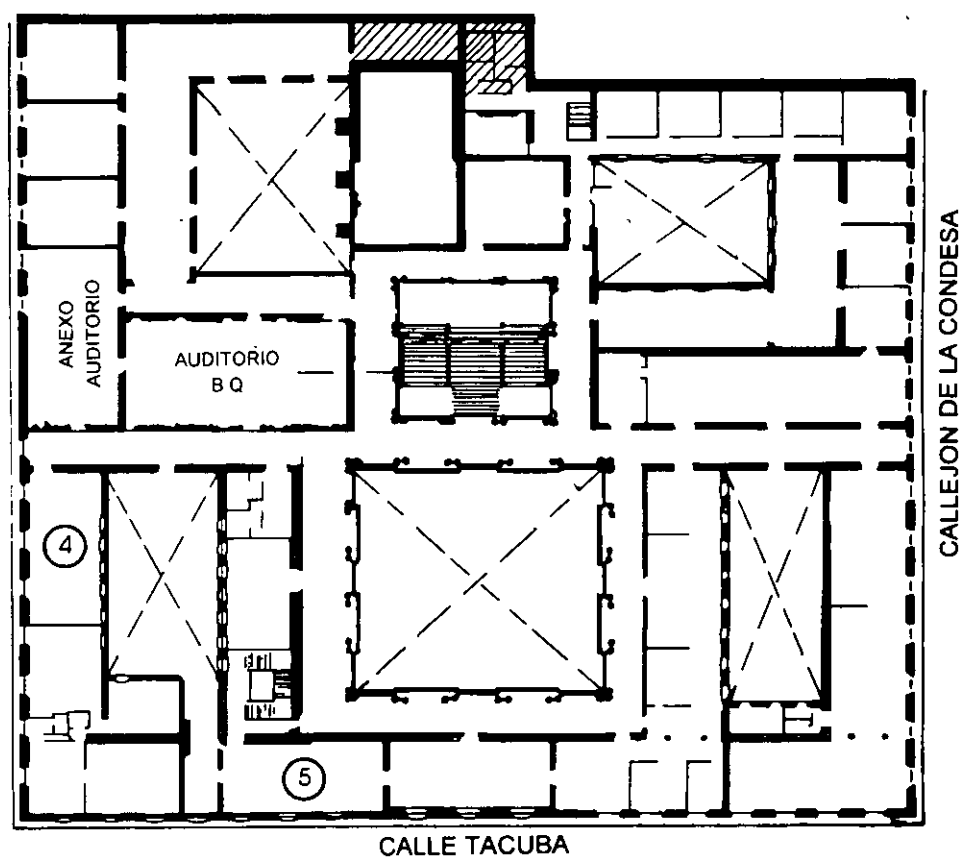
División de Educación Continua.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

PALACIO DE MINERIA

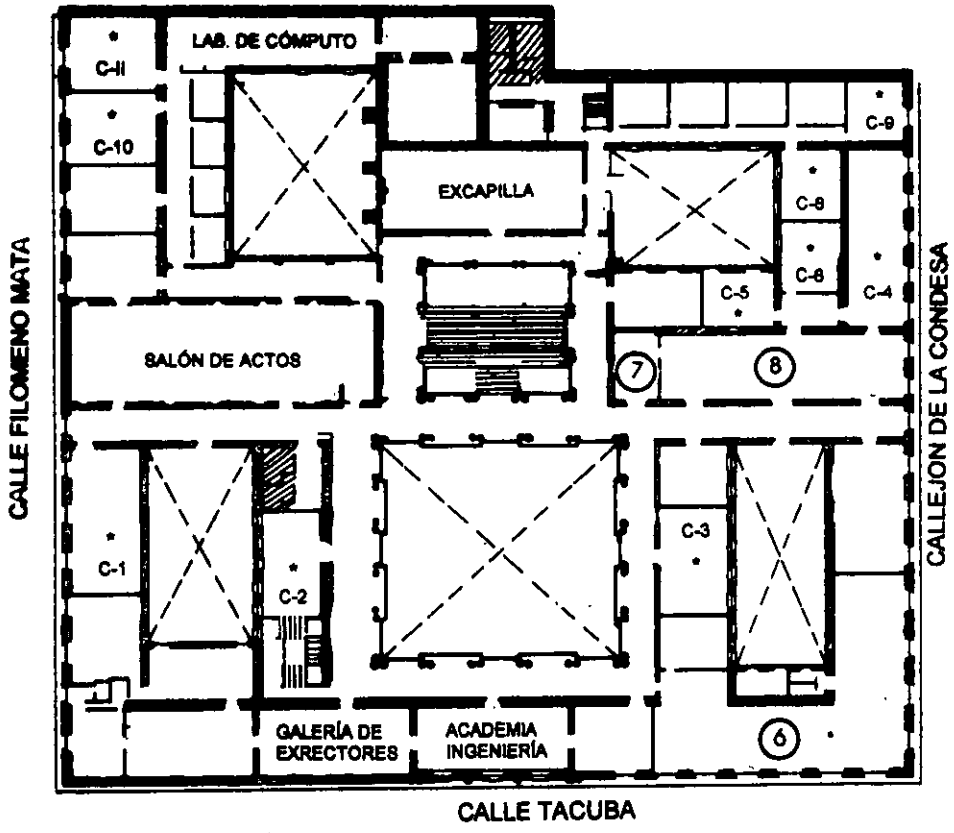


PLANTA BAJA



MEZZANINNE

PALACIO DE MINERIA



1er. PISO

GUÍA DE LOCALIZACIÓN

1. ACCESO
2. BIBLIOTECA HISTÓRICA
3. LIBRERÍA UNAM
4. CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN "ING. BRUNO MASCANZONI"
5. PROGRAMA DE APOYO A LA TITULACIÓN
6. OFICINAS GENERALES
7. ENTREGA DE MATERIAL Y CONTROL DE ASISTENCIA
8. SALA DE DESCANSO

SANITARIOS

* AULAS

DIVISIÓN DE EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA U.N.A.M.
CURSOS ABIERTOS

DIVISIÓN DE EDUCACIÓN CONTINUA
DEC

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

CURSOS ABIERTOS

Diplomado de redes WAN

Diseño de redes y Nuevas tecnologías

Del 19 al 23 de octubre de 1998
Clave del curso (CA144)

Prof: Ing. Federico Vargas

Diseño de Redes y Nuevas Tecnologías
Diplomado en Redes WAN, Palacio de Minería
División de Educación Continua.
Facultad de Ingeniería, UNAM.

Pre-requisitos:

- Introducción a las comunicaciones de datos
- Redes de Area Local

Temario:

1.- Conceptos básicos del diseño de redes
  Dispositivos para construir redes
    - Hub
    - Bridge
    - Switch
    - Router
  Funcionamiento del switcheo de paquetes
    - Switcheo en capa 2
    - Switcheo en capa 3

2.- Evaluación y selección del esquema de la red
  Modelo de diseño Jerárquico
  Evaluación de los servicios del backbone
  Evaluación de los servicios distribuidos
  Evaluación de los servicios de acceso local
  Selección de las opciones de integridad en la red
    - Enlaces redundantes Vs. topologías "Full-Meshed"
    - Redundancia en los sistemas de potencia
    - Hardware de respaldo

3.- Selección de los dispositivos de red
  Beneficios del switcheo en capa 2
  Beneficios del switcheo en capa 3
  Tipos de switches
  Comparación entre routers y switches

4.- Diseño de redes con frame relay
  Diseño jerárquico
  Topologías regionales
  Desempeño de una red frame relay

5.- Diseño de redes ATM
  Influencia de ATM en las redes
  Funcionamiento de ATM
  Tipos de switches ATM

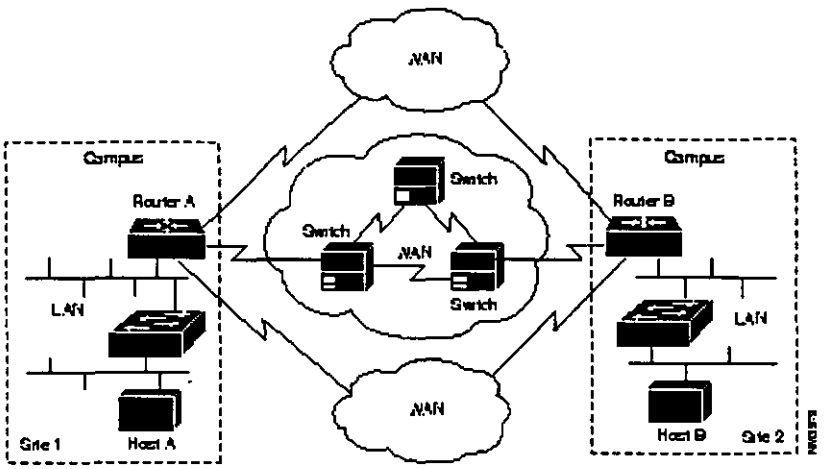
INTRODUCCION

El concepto de *internetworking* hace referencia al hecho establecer la comunicación entre dos o más redes, que para nuestro estudio van a ser únicamente las de datos. Una *internetwork* requiere de muchos protocolos y funciones que le permitan ser escalable y administrable sin que sea necesario una constante intervención manual.

Las grandes internetworks pueden consistir de uno o varios de los siguientes componentes:

- Una red de *Campus*, que está formada por usuarios que se conectan de manera local dentro de un edificio o dentro de un grupo de ellos.
- Redes de Area Amplia (WAN) las cuales conectan a los campus separados geográficamente.
- Conexiones remotas (típicamente dial-up) que permite la conexión de los usuarios móviles con las oficinas centrales o regionales e incluso al Internet.

Figura A-1. Ejemplo de una Internetwork.



El diseño de una Internetwork puede convertirse en una tarea muy delicada. Para diseñar una red confiable y escalable, los diseñadores de redes deben tener en cuenta que los tres distintos componentes de las redes necesitan de requerimientos particulares. Una internetwork que consiste de solo 50 nodos de ruteo, puede convertirse en una fuente de diversos problemas si no se hace una buena planeación de las tecnologías que se van a implementar, de hecho en la medida en que aumentan el número de nodos conectados, las redes se van volviendo más complejas y por lo mismo acarrean problemas cada vez más específicos.

Por lo general, la historia de las redes corporativas puede ser descrita de manera muy sencilla. Al principio, los nodos conectados son pocos y solo en un campus. Posteriormente pueden agregarse algunos usuarios móviles e incluso algunos enlaces WAN. Después de algunos años, lo que antes era una red relativamente sencilla de manejar se ha convertido en una internetwork en donde se manejan diferentes protocolos y arquitecturas de las cuales dependen los usuarios para realizar sus actividades cotidianas. En un principio el uso de la red podría considerarse un lujo, pero después se convierte en una necesidad y por tanto el mantenerla trabajando de manera óptima es una de las tareas diarias del administrador de red que generalmente es también el que realizó el diseño de la misma.

En este documento se pretenden tratar los temas indispensables que debemos conocer como diseñadores de redes de gran escala. Por lo tanto, en las siguientes secciones se hará referencia a la forma en que se puede abordar el diseño de las mismas en cualquiera de sus tres grandes componentes. LAN, WAN y Dial-Up.

CONCEPTOS BASICOS

Dispositivos para construir redes.

Los administradores de redes que están directamente implicados en el diseño de una internetwork cuentan con 4 tipos básicos de dispositivos:

- Hubs (Concentradores)
- Bridges
- Switches
- Routers

Los Hubs se utilizan para conectar a múltiples usuarios hacia un solo dispositivo físico, que los conecta a la red. Estos dispositivos funcionan como repetidores, regenerando la señal en el momento en que se da el flujo de datos.

Los Bridges se utilizan para dividir lógicamente a la red en distintos segmentos. Estos dispositivos operaran a nivel de la capa 2 del modelo de referencia OSI y son independientes de las operaciones que se realizan en capas superiores.

Los Switches son similares a los bridges pero usualmente tienen más puertos. Los switches proporcionan un segmento único en cada puerto, separando así los dominios de colisiones. Hoy en día, los diseñadores de redes están remplazando los hubs por los switches para incrementar el desempeño y el ancho de banda en sus nodos finales, a la vez que están protegiendo la inversión de sus cableados existentes. Se dice que se hace una protección de la inversión en el cableado debido a que el hecho de reemplazar hubs por switches no implica el cambio del cableado existente.

Los ruteadores separan dominios de broadcast y se utilizan para conectar diferentes arquitecturas de red. Los routers direccionan el tráfico basándose en la dirección de la red destino (en capa 3) y no en base a la dirección física o MAC del equipo final. Los ruteadores son dispositivos dependientes de los protocolos.

Es muy marcado el hecho de que los administradores de redes están dejando de utilizar los hubs y bridges en sus implementaciones de internetworks y que los dispositivos más comunes son ahora los switches y los routers. Es por eso que se le va a poner mayor atención al funcionamiento de estos dispositivos y solo en caso de ser necesarió se hará uso de hubs y/o bridges.

Funcionamiento del switcheo de paquetes

Hoy en día en las comunicaciones de datos, todos los equipos de ruteo y de switcheo realizan las siguientes operaciones básicas:

- Switcheo de frames de datos.- Esta es una operación de *store-and-forward* en la cual un frame (o paquete) llega al dispositivo por algún puerto (asociado a una arquitectura de red) y es transmitido hacia otro puerto.

- Mantenimiento de operaciones de switcheo.- En esta operación los switches construyen y mantienen tablas de switcheo. Los ruteadores hacen lo mismo pero con tablas de ruteo y tablas de servicio.

Existen dos métodos para realizar el switcheo de paquetes y se diferencian por la capa del modelo OSI en donde se realizan.

Switcheo en capa 2 y en capa 3

Los routers utilizan el switcheo en capa tres para rutear un paquete y los switches utilizan el switcheo en capa dos para enviar los paquetes por la interfaz adecuada.

La diferencia entre el switcheo en capa 2 y 3 es el tipo de información dentro del frame que se utiliza para determinar cual es la interfaz de salida correcta. En el switcheo en capa 2, los frames son switchados en base a la dirección MAC. En capa 3, los frames son switchados en base a la información de la capa de red que contienen.

El switcheo en capa 2 se realiza observando la dirección MAC destino que viene dentro del paquete. Es decir, el switch observa la dirección destino (MAC) del frame y lo envía hacia el puerto de salida si es que conoce la localidad de la dirección destino. Así pues, el switcheo en capa 2 construye y mantiene una tabla de switcheo en la que se asocian puertos con direcciones MAC.

Si el switch no sabe en que puerto está la dirección MAC destino para cierto paquete, entonces lo envía hacia todas las interfaces para aprender así en que puerto se localiza. Esto se conoce como broadcast. Cuando la respuesta al broadcast es recibida, el switch aprende la dirección de la localidad en donde se encuentra esa nueva MAC y la añade a su tabla de switcheo.

Las direcciones de capa 2 son construidas en base al código del fabricante y un código único de parte. La parte del código del fabricante es asignada a cada empresa por la IEEE. De esta manera las direcciones de capa 2 están asociadas a un espacio plano de direcciones MAC universalmente únicas.

En el siguiente URL ustedes podrán consultar una lista generada por la IEEE de códigos registrados para los fabricantes. Es preciso señalar que no solo existe un solo código para cierto fabricante, por el contrario hay muchas empresas que tienen más de un código registrado por la IEEE para sus productos.

El switcheo de paquetes en capa 3 opera en la capa de red. Este switcheo examina la información que trae consigo el paquete, referente a la red destino y así determina hacia que interfaz de salida debe enviar el paquete.

Las direcciones de capa 3 son determinadas por el administrador de la red quien las distribuye de manera jerárquica en su red. Los protocolos como IP, IPX y AppleTalk utilizan direccionamiento de capa 3. Al crear direcciones de capa 3, el administrador va creando también entidades lógicamente separadas que se encuentran asociadas a localidades geográficas. Así, cuando una estación se cambia de edificio o de ciudad, también se deberá cambiar su dirección de capa 3 asociada, pero la de capa 2 permanecerá constante.

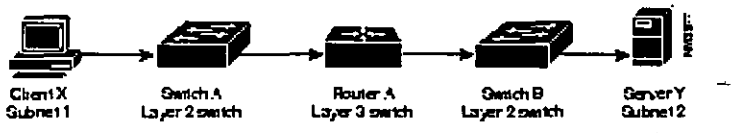
Debido a que los routers operan en la capa 3 del modelo OSI, pueden ser agregados también a la red de manera jerárquica. Así la composición de una red física puede ir íntimamente ligada a la distribución jerárquica de las direcciones de capa 3. Por ejemplo, en una red TCP/IP los segmentos pueden ser distribuidos de manera jerárquica de acuerdo a la composición de las redes físicas que conforman a la internetwork. El flujo de tráfico en ambas composiciones de red es definitivamente diferente. En una red ruteada este flujo puede ser mucho más flexible en el sentido en que se pueden escoger, dentro de la composición jerárquica, una serie de rutas alternativas y además se pueden aislar los dominios de broadcast.

Implicaciones del switcheo en capa 2 y capa 3

El incremento en el poder de procesamiento de escritorio y los requerimientos del ambiente cliente-servidor y las aplicaciones multimedia han despertado la necesidad de anchos de banda más amplios a los que se manejaban en las redes tradicionales de medios compartidos (En donde las estaciones se conectaban a hubs).

Mientras que los switches utilizan la microsegmentación para satisfacer las demandas de mayores anchos de banda, los diseñadores de redes han puesto su atención en la creciente necesidad de comunicación entre subredes. Por ejemplo, cada vez que un usuario accesa a los servidores y otros recursos, que se encuentran en diferentes subredes, el tráfico deberá pasar por un dispositivo de capa 3. En la siguiente figura se muestra como se da este tipo de comunicación.

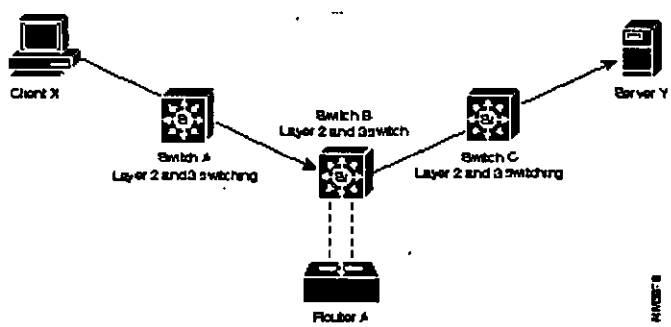
Figura 1-1 Flujo de tráfico entre subredes con switches y routers de por medio.



Como muestra la figura anterior, para que el cliente X pueda comunicarse con el servidor Y, que se encuentra en otra subred, debe pasar a través de la siguiente ruta: Primero por el switch A (switch de capa 2), luego a través del router A (switch de capa 3) y finalmente a través del switch B (switch de capa 2). En este esquema existe un potencial cuello de botella, que puede decrementar el desempeño de la red, y se debe precisamente a que el paquete debe viajar de una red a otra para lograr la comunicación entre subredes.

Para solucionar este cuello de botella, los diseñadores de redes pueden añadir algunas capacidades de capa 3 a sus redes. Actualmente se están implementando el switcheo de capa 3 en los switches tradicionales para aligerar la carga que tenían los routers centrales. En la figura siguiente se ilustra como se pueden utilizar las ventajas del switcheo en capa 3 en la red del ejemplo anterior para lograr que el cliente X se comunique de manera directa con el servidor Y sin tener que pasar por el router A.

Figura 1-2 Flujo de tráfico entre subredes con switches de capa 3.



EVALUACION Y SELECCION DEL ESQUEMA DE RED

Una vez que se han comprendido las necesidades de la red, uno debe identificar y después seleccionar las tecnologías específicas que se amoldan al ambiente de cómputo que se tiene. A lo largo del presente tema discutiremos los siguientes puntos que nos ayudarán a tomar mejor nuestras decisiones:

- Identificar y seleccionar el modelo de red.
- Escoger la mejor opción de integridad.

Identificación y selección del modelo de red.

Los diseños jerárquicos de red nos permiten diseñar redes en capas. Para entender mejor la idea de diseño de capas tomemos en cuenta el siguiente ejemplo. Consideremos al modelo de referencia OSI, el cual es un modelo de capas, para entender e implementar las comunicaciones entre computadoras. Mediante el uso de capas, el modelo OSI simplifica la tarea que dos computadoras tienen que realizar para poder comunicarse. Los modelos jerárquicos de redes también utilizan capas para facilitar la tarea requerida para comunicar a dos o más redes. Cada capa puede desempeñar funciones específicas permitiendo al diseñador de red escoger el mejor sistema y características para cada capa.

Utilizando un modelo jerárquico puede también facilitarnos la tarea de hacer cambios sobre le diseño original. La modularidad nos permite crear modelos elementales que pueden ser replicados en nuevas redes cuando la infraestructura comienza a crecer. Como cada elemento del diseño requiere de ciertos cambios, el costo y complejidad de hacer una actualización puede ser contenido en un pequeño subconjunto de toda la red. Por el contrario, en redes grandes, de diseño plano o de malla, los cambios tienden a tener un mayor impacto sobre los sistemas que la conforman. También el manejo de un correcto aislamiento de fallas es acompañado de un diseño modular creado a partir de pequeños elementos, fáciles de comprender.

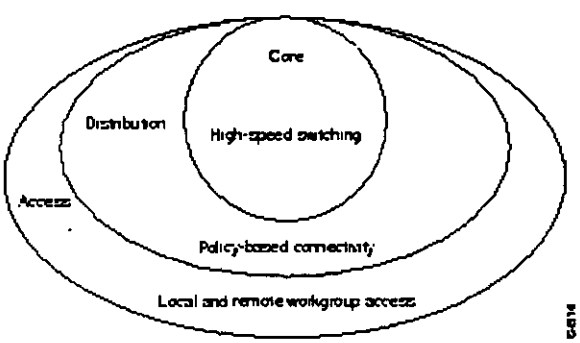
Utilizando un modelo de diseño jerárquico

Un modelo de diseño jerárquico incluye las tres siguientes capas:

- El backbone (core). Capa que provee un óptimo transporte entre los sites.
- La capa de distribución que provee conectividad basada en políticas.
- La capa de acceso local que provee el acceso a la red a los grupos de trabajo y usuarios individuales.

La figura siguiente muestra una vista general de los aspectos que envuelve el diseño de una red jerárquica. Cada capa provee diferentes funcionalidades y en conjunto intentan comunicar a los sistemas de manera óptima y veloz.

Figura 2-1 Modelo jerárquico de diseño de redes.



Función de la capa de backbone

Esta capa está formada por un backbone de switcheo de alta velocidad y debe ser diseñada para switchear paquetes lo más rápido posible. Esta capa no debe hacer ninguna manipulación de paquetes tales como listas de acceso y filtrado de flujos de información que puedan disminuir la velocidad en que se realiza el proceso de store-and-forward.

Función de la capa de distribución.

Esta capa representa la demarcación entre las capas de backbone y de acceso. Ayuda a definir y diferenciar al core de las otras capas. El propósito de esta capa es proveer la definición de borde y es el punto en donde debe suceder la manipulación de los paquetes. En el ambiente de campus, la capa de distribución puede incluir las siguientes funciones:

- Agregación de áreas o direcciones.
- Acceso por departamento o por grupo de trabajo.
- Definición de los dominios de broadcast y multicast.
- Ruteo de redes virtuales (VLAN).
- Cualquier transición de medios que se tenga que realizar.
- Implementación de la seguridad.

En los demás ambientes, la capa de distribución puede ser en donde se lleve a cabo la redistribución de dominios de ruteo o la demarcación entre los protocolos de ruteo estático y dinámico. Este puede ser también el punto en donde los sitios remotos accesan a la red corporativa. La capa de distribución puede ser definida como la capa en que se provee la conectividad a los usuarios, en base a ciertas políticas de acceso.

Función de la capa de acceso

Es precisamente en esta capa en donde los usuarios finales pueden tener acceso a la red. Esta capa puede utilizar listas de acceso o filtros para optimizar las necesidades de acceso a ciertos usuarios. En el ambiente de campus, la capa de acceso puede incluir a las siguientes funciones:

- Ancho de banda compartido.
- Ancho de banda switchado.
- Filtrado a nivel de direcciones MAC.
- Microsegmentación.

En los demás ambientes, la capa de acceso puede dar acceso a los sites remotos por medio de los enlaces WAN.

Algunas veces es mal interpretado que las tres capas deben existir en entidades físicas bien diferenciadas e independientes. Las tres capas son definidas para que en conjunto representen a la robusta funcionalidad que se requiere en las redes de alto desempeño. La Implementación de cada capa se podrá distinguir en cada router o switch, podrá ser representada por un medio físico, puede estar combinada en un mismo dispositivo, o puede incluso ser omitida. La Implementación de las capas depende en gran parte de las necesidades de la red que está siendo diseñada. Sin embargo, hay que notar que para que funcione una red de manera óptima el concepto de jerarquía debe estar presente.

Evaluación de los servicios del backbone

En esta sección abordaremos los temas relacionados a las tecnologías que soportan los servicios del backbone. Los tópicos que serán tratados son:

- Optimización de rutas.

- Prioritización de trafico.
- Balanceo de carga.
- Acceso switchado.
- Encapsulación (tunneling).

Optimización de ruta

Una de las principales ventajas de los ruteadores es que nos ayudan a construir nuestra red de manera lógica en la cual las rutas optimas para llegar a un cierto destino se escogen de manera automática. Los ruteadores realizan esta labor apoyándose en los protocolos de ruteo que van asociados con uno o varios protocolos de red.

Dependiendo de los protocolos de red implementados, los routers nos permiten implementar ambientes de ruteo que respondan a las necesidades especificas de nuestra red. Algunas características de los algoritmos de ruteo pueden promover la optimización en la selección de las rutas. Por ejemplo, el tener como opciones el variar las *métricas* y los *timers* en las tablas de ruteo, o bien el hecho de que nuestros protocolos de ruteo converjan de manera rápida nos van a ayudar en gran medida a cumplir con una de las características que nuestro backbone debe tener, la optimización de rutas.

Prioritización de tráfico

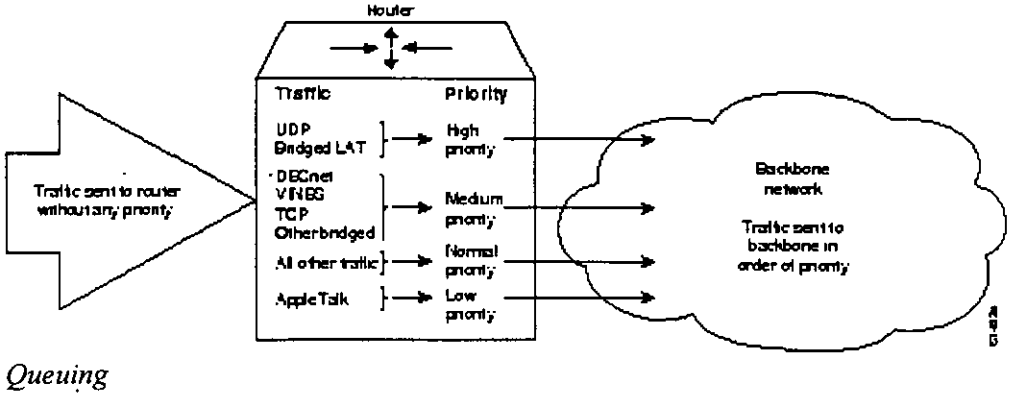
Aunque algunos protocolos de red pueden dar prioridad a cierto tráfico homogéneo, el router puede dar prioridad a los tráficos de flujo heterogéneo. Esta prioritización de tráfico nos permite implementar el ruteo de paquetes en base a políticas (policy-routing) y nos asegura que los protocolos que transporten datos de misión critica puedan tomar precedencia sobre aquellos que transportan trafico menos importante.

Existen varias formas para dar prioridad a los flujos de datos. Enseguida se muestran algunos ejemplos que incluyen algunas tecnologías muy recientes como el Weighted Fair Queuing.

Priority Queuing

Con este método, el trafico puede ser clasificado de acuerdo a varios criterios, incluyendo el tipo de protocolo o subprotocolo, y luego introducido a uno de los cuatro *buffers* de salida; el de alta, media, normal y baja prioridad. En la figura siguiente se muestra como con el Priority Queuing puede ser utilizado para segregar el tráfico de acuerdo a su prioridad.

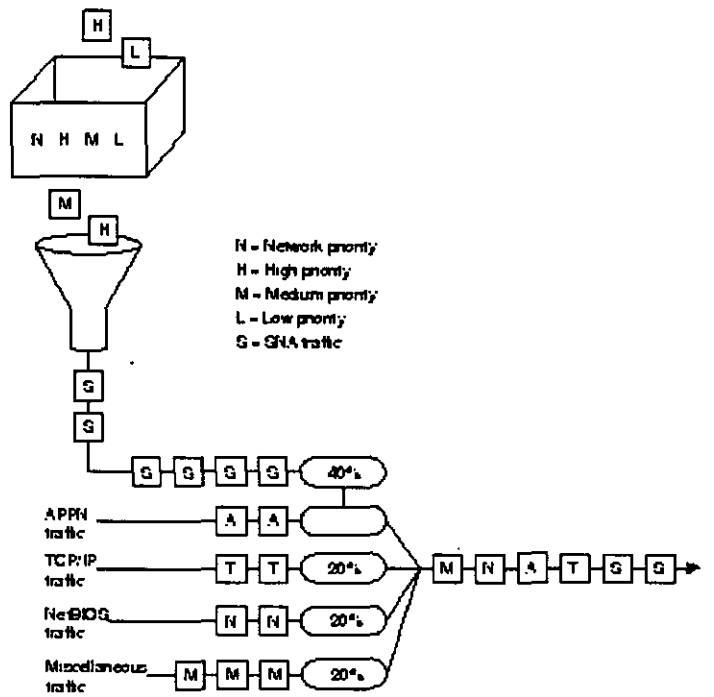
Figura 2-2 Priority Queuing



Custom Queuing

La desventaja principal del método anterior se debe a que muchas veces se teme que los paquetes clasificados como de baja prioridad, por lo mismo no lleguen a su destino final y se descarten en algún punto intermedio. Para eliminar ese tipo de situaciones, existe otro método llamado *Custom Queuing* que lo que hace es reservar ancho de banda para un protocolo en particular, permitiendo así que el trafico de misión critica siempre tenga un ancho de banda mínimo para su transporte. Si por alguna razón el trafico de cierto protocolo no ocupa todo el ancho de banda que se le tiene reservado, entonces ese remanente puede ser utilizado por algún otro protocolo.

Figura 2-3 Custom Queuing

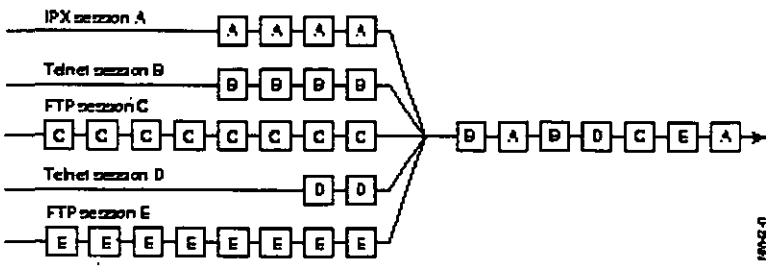


Weighted Fair Queuing

Este método es un algoritmo de administración de prioridades de tráfico que utiliza el modelo TDM (Time Division Multiplexing) para dividir el ancho de banda disponible entre los clientes de una misma interfaz. En TDM cada cliente es alojado en un tiempo utilizando el método round-robin. En WFQ (Weighted Fair Queuing), el ancho de banda es distribuido sobre todos los clientes de tal manera que todos utilizan de manera justa el total del ancho de banda.
Aquí se pueden asignar diferentes conjuntos de pesos, por instancia a través del tipo-de-servico (Type-Of-Service), para que más ancho de banda sea asignado.

Si cada cliente es asignado al mismo ancho de banda independientemente de la tasa de llegada, el volumen de menor tráfico tiene prioridad efectiva sobre el tráfico de mayor volumen. El uso de pesos permite a las aplicaciones sensibles al retraso obtener mayor ancho de banda, así se garantiza una respuesta consistente bajo flujos de trafico intenso. Existen varios tipos de flujos de datos sobre el mismo medio, como se muestra en la figura que a continuación se muestra.

Figura 2-4 Weighted Fair Queuing



C y E representan sesiones de FTP que son flujos de alto volumen de tráfico. A, B y D son sesiones interactivas y son de bajo volumen de tráfico. Cada sesión en este caso la referiremos como conversación. Cada conversación es servida de manera cíclica y obtiene un slot dependiendo de la tasa de llegada, entonces el FTP no monopoliza el ancho de banda. Los retardos de ida y vuelta (round trip delays) para tráfico interactivo, se vuelven, entonces, predecibles.

WFQ provee un algoritmo para identificar flujos de datos dinámicamente utilizando una interfaz, y los ordena en colas separadas. El algoritmo utiliza varias formas de discriminación basadas en cualquier información del protocolo de red que esté disponible y realiza así su ordenamiento. Por ejemplo, para el trafico de IP, los discriminadores son las direcciones de fuente y destino, tipo de protocolo, numero de socket. y TOS (Type Of Service). Así es como las sesiones de Telnet (sesiones B y D) son asignadas a diferentes colas lógicas, tal cual se muestra en la figura anterior.

Balanceo de cargas

La manera más fácil de agregar ancho de banda al backbone es instalando nuevos enlaces. Los routers proveen el balanceo de cargas para múltiples enlaces así como para múltiples rutas.

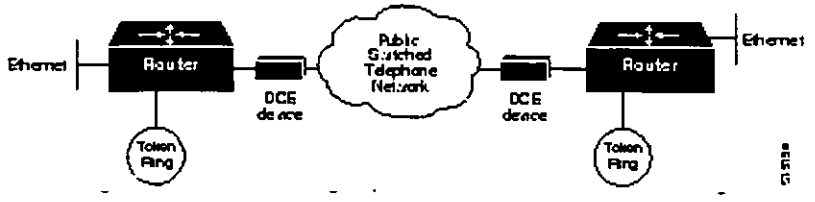
Para IP por ejemplo, los routers proveen de balanceo de cargas en base a paquetes o en base a destinatario. Para el balanceo en base a destinatario, cada router utiliza su memoria cache de ruteo para determinar la interfaz de salida. Para algunos protocolos como IGRP o EIGRP de Cisco Systems, el balanceo con pesos diferentes es posible.

Acceso Switchado

El acceso switchado nos permite habilitar un enlace WAN solo cuando lo necesitamos vía comandos automatizados en el ruteador. Un modelo de red confiable consiste de conexiones dedicadas duales y una línea swhitcheada. Bajo condiciones normales de operación se pueden balancear las líneas dedicadas, pero la conexión switcheada no se activa hasta que una de las dos líneas falla.

Tradicionalmente, las conexiones WAN sobre las redes publicas de telefonía switcheada (PSTN Public Switched Telephone Networks) han utilizado conexiones dedicadas. Esto puede ser muy caro cuando alguna aplicación requiere transmitir un bajo volumen de información sobre conexiones periódicas. Para reducir la necesidad de circuitos dedicados, existe una tecnología llamada Dial-on-Demand Routing (DDS). La figura 2-8 ilustra la típica conexión DDR.

Figura 2-5 Ambiente de Dial-on-Demand Routing (DDR)



Utilizando DDR, bajo volumen de transferencia, y conexiones periódicas pueden ser implementadas a través de la PSTN. Un router activa el DDR cuando recibe un paquete destinado a una localidad que se encuentra del otro lado de la línea dial-up. Después de que el router marca el número destino y establece la conexión, los paquetes de cualquier protocolo soportado pueden ser transmitidos. Cuando la transferencia se completa, la línea automáticamente se desconecta. Así desconectando las líneas no utilizadas, DDR puede reducir los costos de propiedad de las mismas.

Encapsulación (Tunneling)

La encapsulación toma frames o paquetes de cierta arquitectura de red y los coloca dentro de otra arquitectura de red distinta. Este método algunas veces es referido como tunneling. El tunneling provee los medios para la encapsulación de paquetes dentro de un protocolo ruteable utilizando las interfaces virtuales.

Evaluando los servicios de distribución

En esta sección discutiremos las tareas que soportan los servicios de distribución en una internetwork. Dichas tareas son:

- Administración del ancho de banda en el backbone.
- Filtrado de áreas y servicios.
- Distribución basada en políticas.
- Servicio de gateway.
- Redistribución de rutas entre protocolos de ruteo.
- Transformación de medios.

Administración del ancho de banda

Para optimizar el ancho de banda en la red, los switches proveen medios por los cuales mediante el incremento de enlaces entre ellos se puede utilizar la tecnología de "trunking". Con ella cada nuevo enlace se ve como un incremento en el ancho de banda del enlace anterior. La conexión se hace de manera paralela entre los switches y la mayoría de las marcas nos puede proporcionar este tipo de facilidades.
Por otro lado, en los routers contamos con muchos *features* que nos permiten incrementar el desempeño del flujo de paquetes, no así el desempeño mismo del hardware utilizado.

Filtrado de áreas y servicios

Los filtros basados en áreas y servicios son los primeros servicios de distribución utilizados por la implementación de políticas de acceso. En ambas ocasiones, la implementación se realiza a través de ACLs.(Access Control Lists). Las listas de acceso son secuencias de lineamientos que permiten o niegan el acceso a ciertas direcciones o bajo ciertas condiciones.

Estas listas de acceso pueden ser implementadas sobre los paquetes de entrada o de salida sobre las interfaces del router. Los filtros relacionados con los servicios, se implementan sobre protocolos de capas superiores, por ejemplo SNMP o FTP si hacemos referencia al stack de TCP/IP.

Por ejemplo, supongamos que estamos conectados a Internet y que solo queremos que los paquetes que lleguen por el puerto 25 de una estación con TCP/IP sean del tipo SMTP (Correo Electrónico). En este sentido tendríamos que programar una lista de acceso de "entrada" sobre el puerto que conecta al servidor de e-mail diciendo que solo vamos a recibir conexiones dirigidas a dicho servidor por el puerto 25 y por SMTP. Todos los demás intentos de conexión por tal puerto deberán ser rechazados por el router (ej. Conexiones por telnet).

Distribución basada en políticas

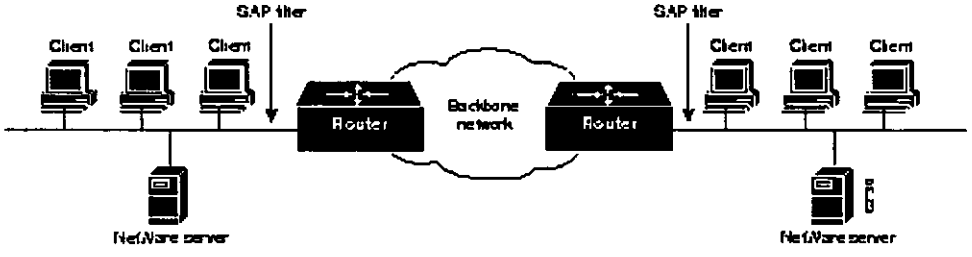
La distribución basada en políticas se apoya en la premisa de que diferentes departamentos dentro de una misma organización pueden tener diferentes políticas de acuerdo a la dispersión de tráfico a través de la internetwork de la corporación. Estas políticas buscan satisfacer ciertos requerimientos sin comprometer el desempeño y la integridad de la información.

Una política dentro de una internetwork puede ser definida como una regla o serie de reglas que gobiernan la distribución de tráfico entre los dispositivos finales. Un departamento puede enviar tráfico de tres diferentes tipos de protocolos al backbone, pero tal vez deseen que alguno de ellos atraviese el backbone con cierta prioridad dado que el tráfico que transporta es de importancia vital. Para minimizar el tráfico excesivo, otro departamento querrá excluir de su LAN todo el tráfico exceptuando el correo electrónico.

Estas políticas reflejan políticas específicas a un departamento. Sin embargo, las políticas pueden reflejar los objetivos de toda la empresa.

Diferentes políticas frecuentemente deben ser implementadas sobre diferentes grupos de trabajo. Considere la situación que se muestra en la figura siguiente.

Figura 2-6 Distribución basada en políticas: Filtrado de SAP



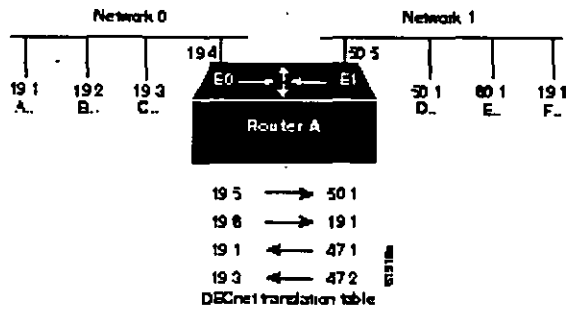
Asumamos que la política del corporativo limita el tráfico innecesario en el backbone. Una forma para hacerlo es restringir la transmisión de los SAP (Service Advertisements Protocol) de IPX. Los mensajes de SAP permiten a los servidores de novell anunciar sus servicios a los clientes. La organización puede tener otra política implementada que indica que los servicios de IPX deben ser locales. En este caso, este tipo de anuncios no tienen porque ser anunciados a las localidades remotas. Los filtros de SAP previenen que el tráfico abandone la interfaz del router previniendo así la propagación de los anuncios más allá de las interfaces locales.

Servicios de gateway

Una de las capacidades que traen consigo los routers es el de gateway. Por ejemplo, DECnet actualmente se encuentra en su V fase de desarrollo. Las direcciones de DECnet de la fase V y las de la fase IV son diferentes y por tanto si necesitamos que en una red convivan estaciones de las dos fases, necesitamos hacer una traducción de direcciones y de esto precisamente se puede hacer a través de la facilidad de gateway que traen los routers como parte de su sistema operativo.

La implementación de lo anterior se ilustra en la figura siguiente:

Figura 2-7 Implementación del ATG (Address Translation Gateways) para DECnet.



Redistribución de protocolos de ruteo

En la sección anterior se describió la forma de cómo hacer las funciones de gateway para protocolos ruteables, pero éstos también pueden hacer una redistribución de protocolos de ruteo diferentes.

En muchas ocasiones es necesario manejar distintos protocolos de ruteo en el mismo router, esto es muy común en los ISPs ya que tienen que conectar a sus clientes con el protocolo que ellos estén manejando. Para poder propagar la información que están recibiendo hacia sus demás localidades necesariamente lo deberán hacer a través de su protocolo de backbone. Muchas veces este protocolo no es el mismo y por tanto se tiene que hacer una traducción de métricas para que se rescate mucha de la información sobre las rutas óptimas para llegar a las localidades remotas. Para hacer esto tenemos que asignar métricas de redistribución sobre todos los protocolos que estén involucrados. También es usual que se redistribuyan rutas estáticas a protocolos de ruteo dinámicos.

Transformación de medios

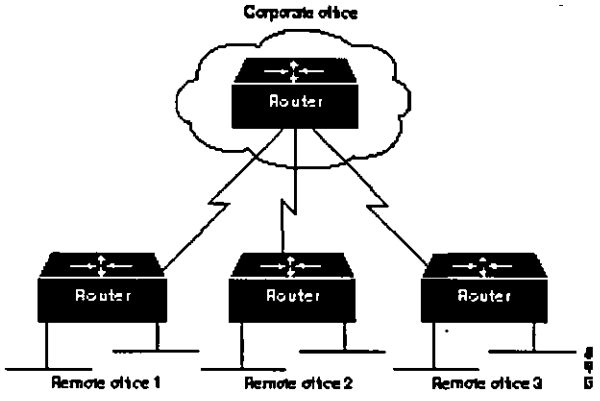
Como último servicio de la capa de distribución, debemos mencionar que todos los cambios de tecnologías se tienen que dar en este nivel para propiciar un ambiente homogéneo de medios y paquetes sobre el backbone. Cada trama que necesite ser transformada en alguna otra, deberá ser realizada aquí y los equipos que nos permiten realizar la tarea pueden ser switches o routers.

Selección de las opciones de integridad en la red.

Uno de las principales preocupaciones de los diseñadores de redes se refiere a determinar el nivel de disponibilidad de las aplicaciones que corren sobre ella. Generalmente, la respuesta está influenciada por los costos de implementación y operación que implica. Para algunas organizaciones es simplemente imposible mantener un sistema completamente redundante en sus redes, por los costos asociados. Sin embargo, siempre es posible llegar a un balance entre lo que se quiere implementar y lo que se puede hacer con los recursos disponibles.

El diseño NO redundante de la figura 2-18 muestra las consideraciones involucradas con el incremento de los niveles de tolerancia ante fallas en una internetwork.

Figura 2-8 Diseño típico de una red no redundante



Esta internetwork tiene dos niveles jerárquicos; el primero se refiere a la red corporativa y la segunda es representada por las oficinas remotas. Si asumimos que la red corporativa alberga a varias redes locales, cada una con muchos usuarios, podemos fácilmente visualizar el hecho de que muchos hosts se quedarán incomunicados parcial o totalmente en caso de que los enlaces o los mismos routers fallen.

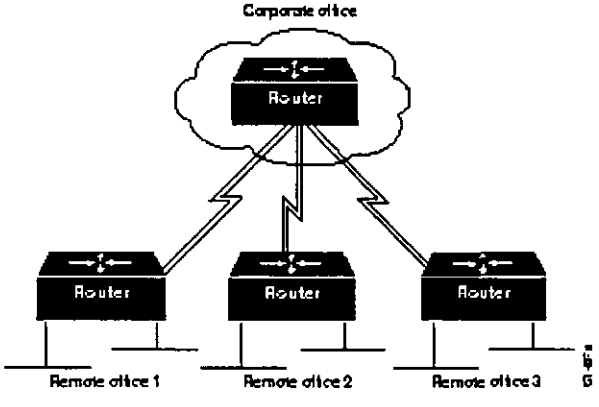
En las secciones siguientes se analizarán algunas opciones de redundancia que se pueden implementar a nuestro ejemplo.

Enlaces redundantes Vs. Topologías full-meshed

Típicamente los enlaces WAN en una internetwork son los que presentan más problemas en una internetwork, generalmente ocasionados por distintos factores: El loop local (enlace de la última milla), los CSU/DSU, etc. Sin embargo, son indispensables para la interconexión de oficinas remotas.

Como primera opción de redundancia podríamos pensar en la configuración de la figura 2-19.

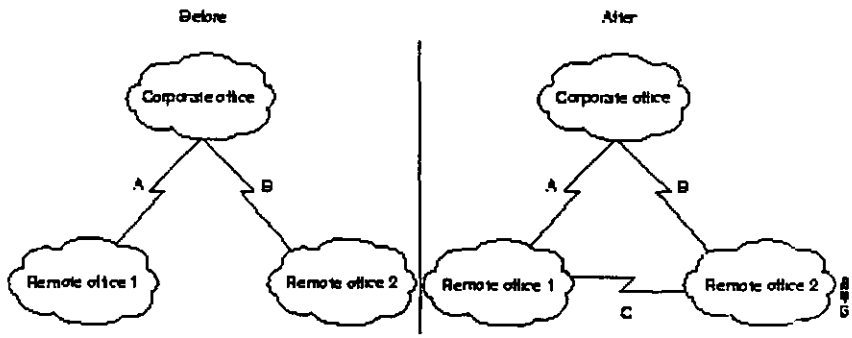
Figura 2-9 Internetwork con enlaces duales hacia las oficinas remotas



Con esto de manera natural podríamos incrementar el ancho de banda para las oficinas remotas y además contaríamos con un enlace de backup en caso de que alguno fallara. Sin embargo, esto puede representar un costo elevado, ya que se tendrían que pagar tres enlaces adicionales y si por alguna razón, el router de la oficina corporativa fallara, toda la empresa quedaría virtualmente aislada.

Existe otra alternativa para añadir redundancia al esquema ejemplo de este estudio. La figura 2-20 muestra lo que sería una evolución de topologías en una red WAN.

Figura 2-10 Evolución de una topología de estrella a una topología full-meshed



En la porción del "antes" de la figura 2-20 cualquier falla asociada a los enlaces A y B dejará sin comunicación a una oficina remota. Añadiendo el enlace C en la porción del "después" de la misma figura estaremos creando un esquema mucho más robusto al que teníamos anteriormente. El costo es bajo pero no siempre se puede implementar, ya que esto dependerá de la disposición de enlaces de nuestro *carrier* de una oficina remota a la otra.

Una topología full-meshed tiene tres ventajas distintas sobre la topología de estrella redundante y son las siguientes:

- Una topología full-meshed usualmente es menos costosa.
- Esta topología provee comunicaciones más directas entre las oficinas remotas, lo cual puede ser muy importante para el caso de intercambio de datos entre las oficinas remotas.
- Una topología full-meshed promueve una operación distribuida, previniendo los cuellos de botella en el router del corporativo, agregando así la disponibilidad de la comunicación entre los usuarios de la internetwork.

Sin embargo, la topología de estrella puede ser una solución alternativa para los siguientes casos.

- Existe un intercambio de tráfico muy pequeño entre las oficinas remotas.
- Los datos que se transfieren de la oficina central hacia las remotas son susceptibles al retraso, así que entre más ancho de banda mejor.

Redundancia en los sistemas de potencia

Las fallas en los sistemas de potencia son muy comunes en grandes internetworks. Debido a que ellos pueden ser muy difíciles de predecir y que son problemas que pueden ser diferentes de acuerdo al site o local en donde se encuentran los equipos, existen solo algunas recomendaciones generales que expondremos en el presente trabajo.

Desde el punto de vista de los equipos como tal, algo que se debe cuidar es que cuenten con fuentes de poder redundantes. Esto implica que la fuente primaria esté funcionando mientras que la segunda se mantiene en stand-by. Si por alguna razón llegase a fallar la fuente primaria o el sistema que la alimenta, la segunda fuente de poder deberá soportar toda la carga del equipo y evitar que el equipo se apague. Es importante mencionar que para tener una configuración correcta de las fuentes de poder, ambas deben estar conectadas a circuitos diferentes de alimentación, si es que se cuenta con ellos.

En algunos sistemas conocidos como los "backbone-in-a-box" en donde todo el tráfico del backbone se concentre en un solo equipo, sea este router o switch, se debe tener especial cuidado en mantener la mayor redundancia posible.

Existen también las situaciones en las que la falla de potencia ocurre a nivel de edificio o de corporativo inclusive, en estos casos la perdida de energía puede representar también perdidas monetarias considerables para la empresa. Para evitar este tipo de incidentes, algunas empresas mantienen un "espejo" de los servidores más importantes en localidades geográficamente separadas. De hecho muchos ISPs grandes cuentan con redundancia hasta en sus centros de monitoreo. Con esto pueden garantizar a sus clientes una gran disponibilidad del servicio. Obviamente cada NOC (Netowork Operation Center) cuenta con la misma información y continuamente se actualiza en ambos sites.

Otras empresas solo deciden mantener imágenes de los servidores ya que aunque su NOC quedase aislado, las operaciones criticas de negocio podrían seguir funcionando.

Las compañías más grandes y con muchos recursos pueden incluso establecer convenios con las compañías de luz para poder alimentar a sus sitios críticos con dos sistemas de potencia completamente independientes y redundantes a la vez.

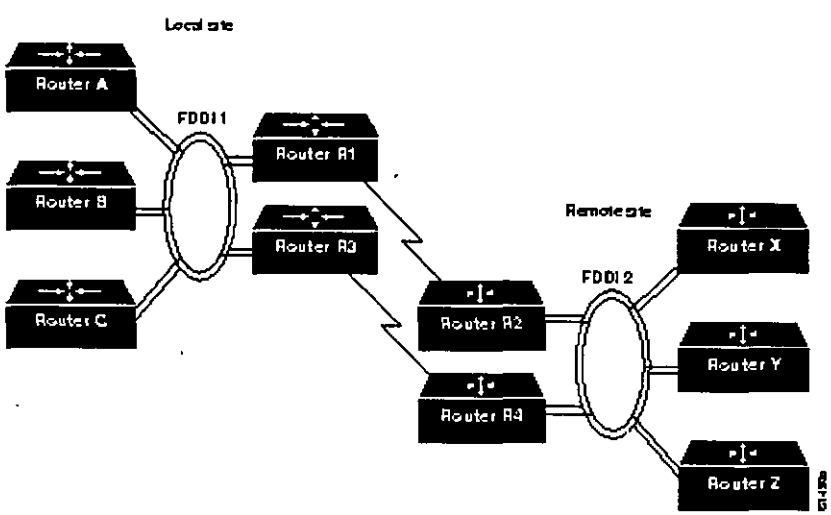
La gran desventaja de este tipo de implementaciones tiene la desventaja de representar un costo elevado, sin embargo, es tarea del diseñador de redes identificar las partes de su red que necesariamente deberán estar protegidas contra este tipo de incidentes.

Hardware de Respaldo

Como todos los dispositivos complejos, los switches, routers, etc. Están propensos a tener problemas de hardware. Es importante tener en cuenta el hecho de que algunos equipos pueden presentar repentinamente fallas en su funcionamiento y por tanto se recomienda manejar estas situaciones desde varios puntos de vista. Existen equipos que soportan una configuración de redundancia activa. Esto se puede ejemplificar fácilmente haciendo referencia al protocolo HSRP (Hot Standby Router Protocol), el cual nos permite tener funcionando dos routers a la vez con la misma información de ruteo. Cuando llega a fallar el que está activo, inmediatamente el de backup toma las operaciones de ruteo y switcheo de paquetes, manteniendo así a la internetwork funcionando de manera ininterrumpida.

En la figura siguiente se muestra una configuración típica en donde se podría manejar en HSRP.

Figura 2-11 Configuración de routers redundantes



Otro tipo de respaldo puede ser abordado con un stock de equipos y tarjetas para los mismos. Esto es importante para cuando se tienen fallas parciales en los equipos. En México, la espera de una reposición de tarjeta, fabricada de origen en otros países puede ser muy tardada y las consecuencias pueden ser catastróficas. Es cierto también que mantener un stock en nuestros sites puede resultar muy caro, pero existe la alternativa de los contratos de mantenimiento que incluso pueden establecer una responsabilidad de respuesta por parte del proveedor de hasta máximo 24 hrs.

SELECCION DE LOS DISPOSITIVOS DE RED

Hasta el momento, hemos hablado del funcionamiento de los equipos que podemos utilizar en nuestras internetworks y hemos mencionado de manera dispersa los beneficios que cada uno de ellos y las tecnologías que están disponibles nos puede brindar. En este capitulo haremos un breve resumen de los beneficios que nos representan y haremos algunas distinciones y comparaciones finales entre ellos.

Beneficios del switcheo en capa 2

Un switch de capa nos puede ofrecer de manera individual los siguientes beneficios.

- Ancho de banda.- Los switches LAN proveen un excelente desempeño a los usuarios ofreciéndoles ancho de banda dedicado por puerto. Cada puerto del switch representa un segmento diferente. A esta técnica se le conoce como *microsegmentación.* Recordemos también que por el hecho de hacer "trunking" podemos aumentar el ancho de banda en las conexiones que existen entre ellos.
- VLANs.- Los switches de LAN pueden agrupar puertos individuales en segmentos lógicos diferentes llamados Virtual LANs. Muchos de ellos reducen el broadcast a solo el segmento que representan las VLAN. Las VLANs también se conocen como dominios de switcheo o dominios autónomos de switcheo. Algunos switches pueden incluso switchear paquetes VLANs distintas; otros necesitan de un router.
- Reconocimiento automático de paquetes y traducción de frames.- Esto permite al switch transformar formatos de frames de manera automática. De Ethernet MAC a FDDI SNAP por ejemplo.

Beneficios del switcheo en capa 3

Debido a que los routers utilizan direcciones de la capa 3, que generalmente vienen asociados a cierta distribución jerárquica de las mismas; la conexión de los mismos nos pueden dar la evidencia de la forma en que la red está construida. Será fácilmente identificar las capas de la jerarquía y los diferentes módulos que se planearon en el diseño de la red.

Los beneficios que nos pueden ofrecer son los siguientes:

- Control de broadcast y multicast
- Segmentación de los dominios de broadcast
- Seguridad
- Calidad de servicio (Dependiendo del protocolo utilizado en la red)
- Prioritización de tráfico
- Definición de políticas de comunicación entre hosts.

Tipos de switches

Los switches los podríamos categorizar de la siguiente manera:

- LAN switches
- ATM Switches

Actualmente los diseñadores de redes están migrando sus tecnologías de acceso compartido por el acceso dedicado que les pueden proporcionar los switches de LAN. Los switches de esta categoría pueden ser aquellos que ofrecen acceso a redes Ethernet, Fast Ethernet, Token Ring y FDDI. Todos ellos ofreciendo los servicios de microsegmentación, VLANs, Trunking, etc.

Los switches de ATM, a diferencia de todos los demás, realizan un transporte de datos a través de celdas y nos pueden ofrecer las siguientes ventajas:

- Variedad en servicios e interfaces soportadas
- Redundancia
- Sofisticado mecanismo para la administración del flujo de tráfico.

Estos equipos, pueden ser también clasificados de manera más específica de acuerdo a su nivel de funcionalidad y los usos que se les puede dar. Con respecto a esto tendríamos la siguiente clasificación.

- Switches ATM para grupos de trabajo.
- Switches ATM para Campus.
- Switches ATM para Corporativo.
- Switches de acceso a multiservicios.

Comparación entre routers y switches

Para remarcar las diferencias entre estos dos tipos de dispositivos, las secciones siguientes se enfocarán a describir el papel que ocupan cada uno de ellos en las siguientes categorías:

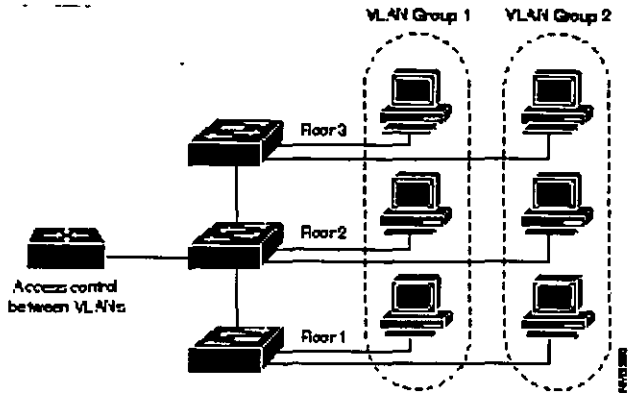
- Implementaciones de VLANs.
- Implementación de internetworks switcheadas.

Papel de los switches y los routers en la implementación de VLANs

Una VLAN consiste de un solo dominio de broadcast y resuelve los problemas de escalabilidad de las grandes redes planas en donde un solo dominio de broadcast es dividido en pequeños segmentos conocidos como VLANs. Las VLANs ofrecen una gran flexibilidad en cuanto a los cambios que se le puedan hacer al diseño original de la red, dado que el cambio en la configuración de las mismas solo implica una reprogramación de las mismas y no movimientos de conexiones o introducción de nuevos dispositivos.

El papel de los switches en este tipo de diseño es el de transportar los datos de manera veloz en el backbone y el de los routers es precisamente el de proveer comunicación entre las diferentes VLANs generadas y proveer de seguridad a la red. En la siguiente figura se muestra este tipo de implementaciones.

Figura 3- 1 Papel de los Routers y Switches en la VLANs

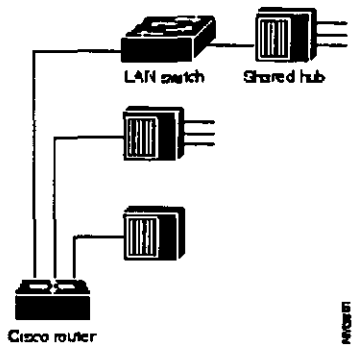


Papel de los routers y switches en el diseño de una internetwork tipo campus

En este tipo de diseños, la implementación de las redes va a variar mucho con respecto a las facilidades que se quieran tener, pero lo importante es que la combinación de los servicios de cada equipo van a proveer la modularidad de la red y la van a mantener en un estado de escalabilidad a cualquier nivel.

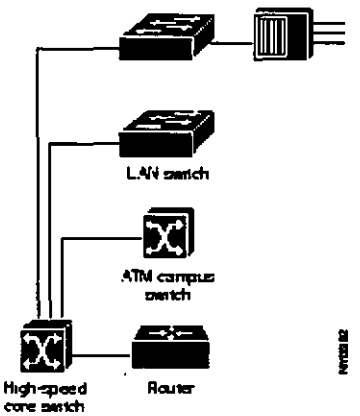
Por ejemplo, en la siguiente figura se muestra la primera fase de implementación de una red en crecimiento: La microsegmentación.

Figura 3-2 Utilizando switches para la microsegmentación



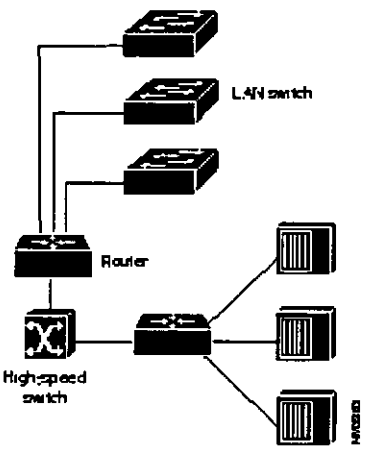
La segunda fase consta de un incremento en el ancho de banda del backbone y el comienzo de la distribución de los switches en la internetwork.

Figura 3-3 Añadiendo velocidad al backbone y ruteando entre switches



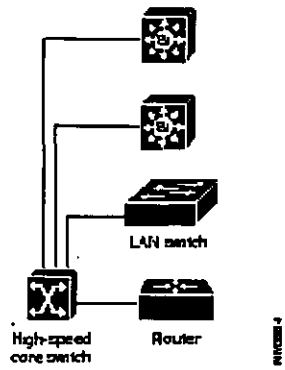
En la fase 3 los routers son distribuidos entre los LAN switches y entre el switch central. Ahora la red está protegida contra las tormentas de broadcast y se sigue dando acceso a gran velocidad a los usuarios finales.

Figura 3-4 Distribución de routers entre los switches del backbone y los de la periferia



En la cuarta fase, que es la última, se provee a los usuarios switcheo de capa 2 y tres a través de toda la infraestructura de la internetwork y por tanto todos los servicios mencionados en los capítulos anteriores se estarían manejando en el diseño final. La figura siguiente muestra la implementación de esta ultima fase.

Figura 3-5 Switcheo end-to-end con VLANs y beneficios de capa 3



DISEÑO DE REDES CON FRAME RELAY

Hasta el momento hemos visto la forma de operar a los equipos y las opciones de colocación a lo largo de nuestra internetwork. En estos dos últimos capítulos abordaremos los casos especiales de dos tipos de redes de alto desempeño. Una en el ambiente WAN y otra en el ambiente de campus.

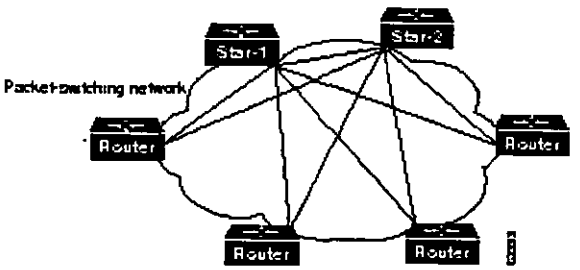
Cuando se esta construyendo una internetwork que enlaza a la red corporativa con oficinas remotas mediante el uso de una PSDN (Packet-Switched Data Network) los dos puntos más importantes a considerar son los costos y el desempeño. Un diseño que cumpla con las características anteriores deberá seguir las siguientes reglas:

- Cuando se implementen redes de switcheo de paquetes, debemos balancear la reducción de costos con el desempeño de la misma.
- Construir un ambiente manejable y que se pueda escalar fácilmente según los requerimientos de nuevos enlaces WAN.

Diseño Jerárquico

El objetivo de diseñar redes de manera jerárquica es modularizar los elementos en capas más pequeñas y manejables. La esencia de este tipo de diseños consiste en hacer subredes para que el tráfico entre nodos se pueda manejar de una manera más dinámica. Este tipo de diseños permiten a los administradores de redes añadir más módulos al esquema global sin tener que reconfigurar sus topologías o hacer grandes inversiones.

Figura 4-1 Interconexión jerárquica en una red de switcheo de paquetes



Tres ventajas básicas podemos mencionar para apoyar la decisión del diseño de redes jerárquicas:

- Escalabilidad.
- Manejabilidad.
- Optimización en el control de broadcast y multicast.

Todo lo que mencionamos en capítulos anteriores sobre el diseño jerárquico de internetwors aplica a las redes de switcheo de paquetes en redes frame relay.

El método por el cual muchos distribuidores de servicios de frame relay tarifican sus servicios es mediante el DLCI (Data Link Connection Identifier) que identifica a una conexión virtual permanente. El DLCI define la conexión entre elementos de frame relay. Para una red de este tipo el número de DLCIs es altamente dependiente de los protocolos transportados y de los flujos de paquetes que los vayan a ocupar. En general, el número máximo de DLCIs por interfaz está entre los 10 y 50. Este número depende de los siguientes factores:

- Protocolos a ser ruteados. Dado que los broadcast que se reciben por cada interfaz tienen que ser propagados por cada DLCI, los protocolos como AppleTalk o IPX pueden disminuir el desempeño de una interfaz a medida que se van añadiendo más DLCIs a ella. Recordemos que este proceso implica la generación de interfaces virtuales en los routers.
- Tráfico de broadcast.
- Velocidad de las líneas. Si se predice un alto número de broadcast sobre los enlaces, entonces debemos considerar el hecho de tener unos límites superiores de CIR (Commited Information Rate) y de Be (Burst Excess). Además debemos implementar sobre los enlaces pocos DLCIs.
- Rutas estáticas. En caso de que se implementen rutas estáticas el uso de DLCIs se puede incrementar dado que los broadcast de anuncios de ruteo estarán erradicados.

El diseño jerárquico de redes frame relay puede ser implementado de dos formas diferentes:

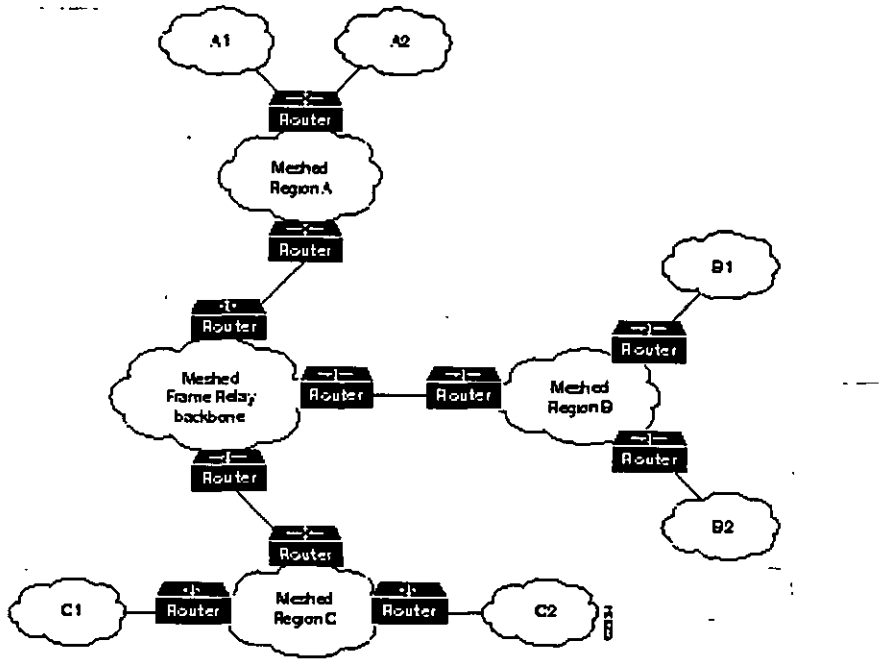
- Topologías full-meshed.
- Topologías híbridas.

Ambos diseños tienen sus ventajas y sus desventajas. Enseguida discutiremos ambos tipos de implementación.

Topologías full-meshed

El diseño jerárquico de redes full-meshed nos permite disminuir el número de DLCIs en la internetwok y nos hace más manejable la red en el sentido de que es una topología segmentada.

Figura 4-2 Ambiente ful-meshed en redes frame relay



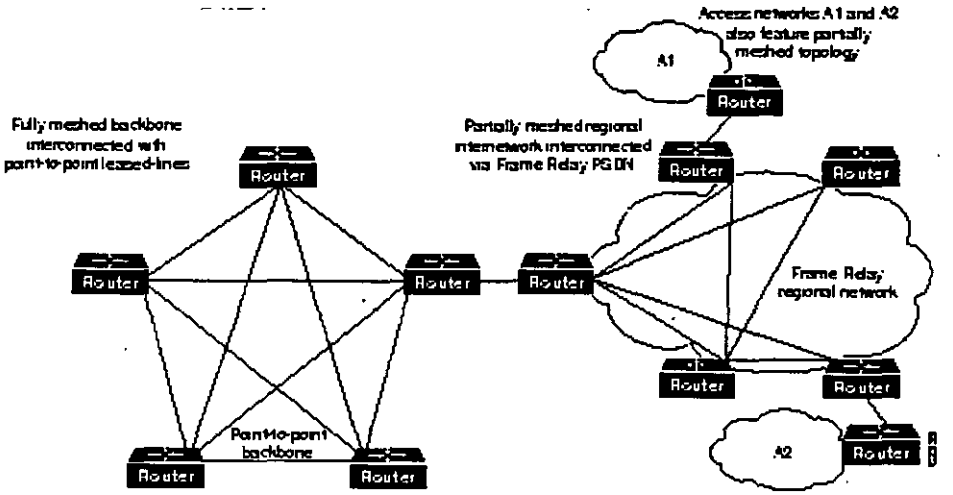
La imagen anterior nos muestra una topología full-meshed en el backbone y en los enlaces regionales. Las principales ventajas de este tipo de construcciones se debe a que tenemos un buen nivel de escalación en nuestra red y al mismo tiempo podemos mantener localizado el tráfico con regiones. Colocando routers entre las topologías full-meshed podremos limitar el número de DLCIs por interfaz física, permitiéndonos tener un mejor control sobre la replicación de paquetes sobre las interfaces virtuales. Es de vital importancia tener en cuenta que hay que manejar de manera muy delicada la replicación de paquetes en el backbone ya que generalmente se requiere de una gran rapidez de switcheo de paquetes y el salvar ancho de banda nos permitirá terne un mejor desempeño a lo largo de la internetwork.

Hay que considerar también el alto costo asociado con las interfaces físicas de los equipos y de los mismos enlaces WAN. En este tipo de topologías los routers nos ayudan a separar las mallas existentes entre cada una de las capas y nos da una muy buena pauta para hacer escalable la red.

Topologías híbridas

La importancia económica y estratégica en los backbones forzan a los diseñadores de redes a implementar topologías híbridas para resolver sus problemas de enlaces WAN. Estas topologías se construyen a partir de mallas entre los routers de backbone WAN y mallas completas o parciales en la periferia. La figura siguiente muestra un ejemplo de este tipo de implementaciones

Figura 4-3 Internetwork de frame relay híbrida



Estas construcciones tienen la ventaja de proveer un alto desempeño en el backbone, localizar tráfico y la simplificación de la escalación de la red. Además las redes híbridas en frame relay son atractivas porque proporcionan un mejor control y permiten crear en el backbone enlaces dedicados que dan como resultado una gran estabilidad.

Las desventajas están asociadas con los costos de los enlaces dedicados así como la propagación de broadcast que pueden ser significativos a nivel de las internetworks de la capa de acceso.

Topologías regionales en redes frame relay

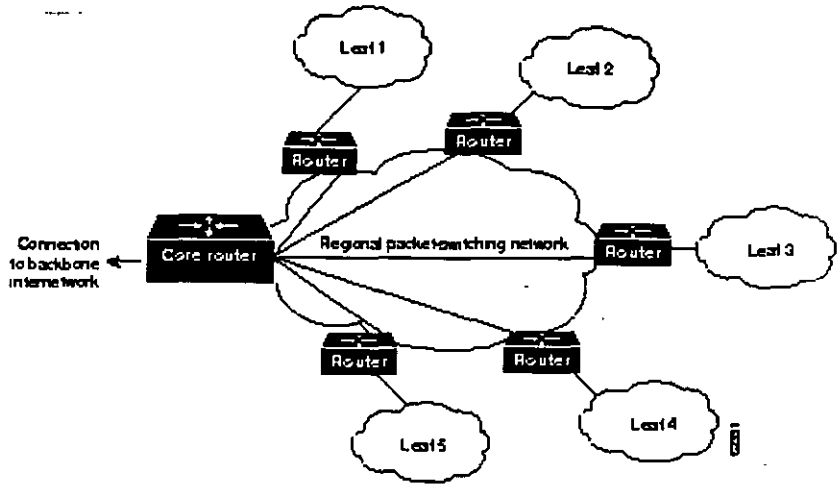
Existen tres tipos de topologías para las redes regionales de frame relay y uno puede escoger la que mejor se adapte a sus necesidades.

- Estrella
- Full-meshed
- Partially-meshed

Estrella

Estas topologías son atractivas porque minimizan el número de DLCIs requeridos lo cual minimiza el costo de la implementación. Sin embargo, una topología en estrella presenta de manera inherente ciertas limitaciones de ancho de banda. Consideremos como ejemplo un ambiente en donde el router del backbone está conectado a una nube de frame relay a 256 Kbps y que las oficinas remotas se conectan a 56 Kbps. Al irse incrementando el número de sitios remotos, el acceso al backbone se irá reduciendo de manera considerable. Por otro lado, en caso de que se implemente una estrella de manera estricta, en caso de que un enlace presente alguna falla, la oficina remota quedará incomunicada tanto del backbone como de los demás sitios remotos.

Figura 4-4 Topología de estrella

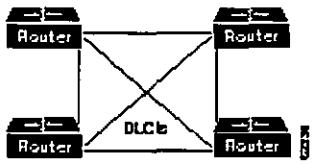


Topología full-meshed

Una topología de este tipo requiere de una conexión via DLCIs de cada router de la nube con todos los demás. Este tipo de diseños no son muy propicios para redes grandes de frame relay y las razones son las siguientes.

Estas redes requieren de muchos DLCIs. Uno para cada enlace lógico entre los nodos. Como se muestra en la figura siguiente, la asignación de DLCIs está regida por la formula [n(n-1)]/2 donde n es el número de routers que están directamente conectados.

Figura 4-5 Topología full-meshed

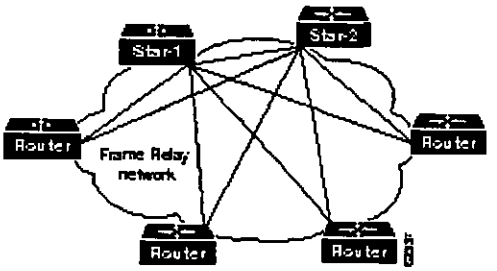


La replicación de broadcast disminuirá el desempeño de manera considerable en la red. Esto se debe a que en frame relay, los routers tratan a la nube de frame relay como un solo medio multiacceso. Cada vez que un router envía un multicast (como una actualización de tablas de ruteo, mensajes de spanning tree, SAP, etc.) ese paquete deberá copiar el frame a cada DLCI para cada interfaz frame relay.

Topología patially- meshed

Combinando los conceptos de una topología de estrella con la de full-meshed el resultado que obtendremos es una topología parcial. Estas topologías son las que generalmente se recomiendan para ambientes regionales porque ofrecen una mejor tolerancia a fallas (que en topologías de estrellas) y son menos caras que ambientes en full-meshed. La idea es implementar el menor número de mallas y eliminar los puntos de falla individuales.

Figura 4-6 Internetwork partially-meshed en estrella gemela



Desempeño de una red frame relay

Existen dos cosas son las cuales se debe tener cuidado al implementar una redes de frame relay.

- Métricas de la tarifa del proveedor de PSDN.
- Requerimientos de administraciónón de tráfico.

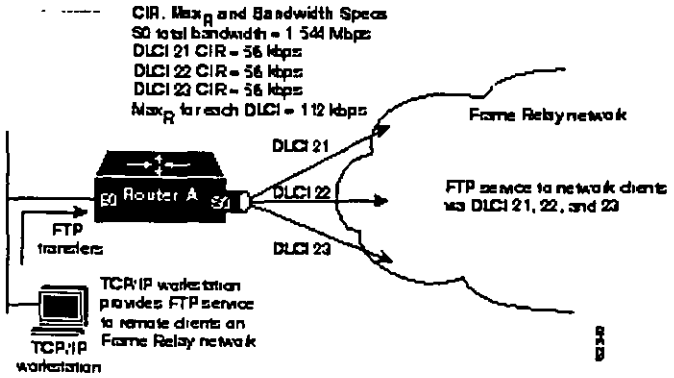
Métricas de la tarifa del proveedor de PSDN

Cuando se contrata un servicio con algún proveedor de frame relay, el CIR –medido en bps- es una de las métricas a considerar. CIR es la medida máxima de tráfico permitido que el carrier permitirá en un específico DLCI. El CIR puede ser cualquier valor hasta la capacidad máxima del canal con el cual se conecta el cliente con el proveedor.

Otra métrica es el Bc (Commited Burst) y el Be (Excess burst). Bc es el número de bits que la internetwork de frame relay permite transmitir en el CIR. Be representa el limite máximo de bits para un DLCI. Este es el número de bits que la internetwork de frame relay intentará transmitir después de que el Bc es acomodado. Be representa un pico en la tasa máxima de transferencia de datos (MAXr) en frame relay, donde MAXr = (Bc + Be)/Bc * CIR medido en bps.

Considere la situación ilustrada en la figura siguiente. Los DLCI 21, 22 y 23 son asignados a CIRs de 56Kbps. Asumamos que el MAXr para cada línea es de 112Kbps (el doble). La línea serial que conecta al router con la nube de frame relay tiene una capacidad máxima de 1.544 Mbps. Dado el tipo de tráfico que será enviado a la nube, tenemos una situación en la cual el potencial de sobrepasar el límite de MAXr es sumamente alto. Esto se debe a que el tráfico consiste de FTPs sobre la red. Si esto ocurre, los datos pueden ser descartados sin notificación alguna si los buffers de Be (Que se encuentran en el switch de frame relay) se exceden.

Figura 4-7 Ejemplo de una situación limitante en los CIRs provistos



Requerimientos de administración de tráfico

Cuando se transmiten por una misma interfaz fisica diferentes tipos de tráfico, algunas veces es conveniente hacer una separación del mismo mediante el uso de los DLCIs. Esto puede hacerse de dos formas. La primera consiste en hacer un mapeo estático entre los DLCIs y las interfaces virtuales de la conexión o bien definiendo la encapsulación que va a manejar cada una de ellas.

A manera de ejemplo, vamos a listar una configuración para un router cisco de la implementación de cada una de las opciones presentadas.

Listado 4-8.a Mapeo de DLCIs a las interfaces virtuales

```
Interface Serial0
No ip address
Encapsulation frame-relay

Interface Serial0.1 point-to-point
Ip address 131.108.3.12 255.255.255.0
Frame-relay interface-dlci 21 broadcast
No frame-relay inverse-arp ip 21
No frame-relay inverse-arp novell 21

Interface Serial0.2 point-to-point
No ip address
Ipx network A3
Frame-relay interface-dlci 22 broadcast
No frame-relay inverse-arp ip 22
No frame-relay inverse-arp novell 22
```

Listado 4-8.b Mapeo de DLCIs sobre la misma interfaz

```
Interface Serial0
Ip address 131.108.3.12 255.255.255.0
Ipx network A3
Frame-relay map IP 131.108.3.62 21 broadcast
Frame-relay map novell C09845 22 broadcast
```

Influencia de ATM en las redes

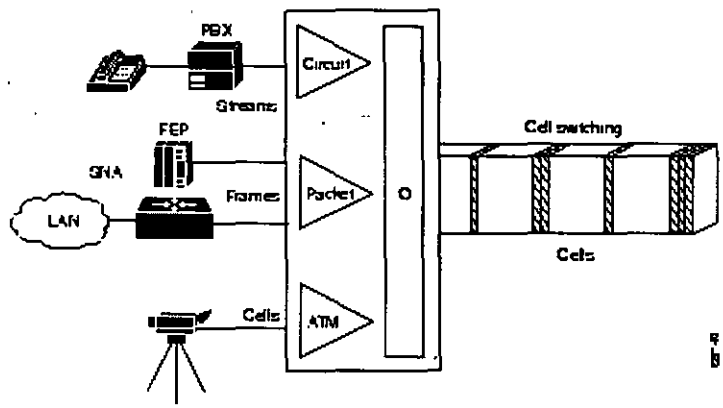
Hoy en día, 90% del cómputo se realiza en el escritorio y ese porcentaje cada vez se incrementa más y más. Las aplicaciones distribuidas día a día dependen de ancho de banda más amplio y la aparición de Internet ha elevado en gran medida los requerimientos de conexión a alta velocidad tanto en la LAN como en la red WAN. Las comunicaciones de voz se han incrementado de manera considerable y se han implementado sistemas de correo de voz cada vez más confiables ya sea centralizados o distribuidos alrededor del planeta. La internetwork es una herramienta crucial para el desarrollo de las tareas cotidianas en cualquier tipo de empleo.

Hasta estos días, las redes locales estaban lógicamente separadas de las redes WAN. En las LAN el ancho de banda cuesta de acuerdo a la implementación de hardware que se tenga y la conectividad está limitada por los mismos equipos. En la LAN solo se transmiten datos. En la WAN el ancho de banda es muy caro debido a las tarifas de larga distancia y las aplicaciones sensibles al retraso en el tiempo, como la voz, típicamente se mantienen separadas. Es decir, se envían los datos por ciertos circuitos y los datos por otros. Sin embargo, las nuevas aplicaciones que demandan cada vez más mejores calidades de servicio están forzando a que estos usos comunes estén cambiando. Ejemplo de ello es la implementación de voz sobre redes publicas y privadas de frame relay.

ATM ha surgido como una de las tecnologías que integran a LANs y WANs. ATM puede soportar cualquier tipo de tráfico de manera separada o mezclado en flujos de información, sea o no sensible al retraso en tiempo.

En la figura siguiente se muestra la forma en que ATM puede soportar lo que se comentó anteriormente.

Figura 5-1 Soporte de ATM para múltiples tipos de tráfico



ATM también es una tecnología escalable que puede soportar capacidades de transmisión bajas (E1) asi como manejar los flujos de información a velocidades que hoy nos parecen extremadamente grandes (OC-48).

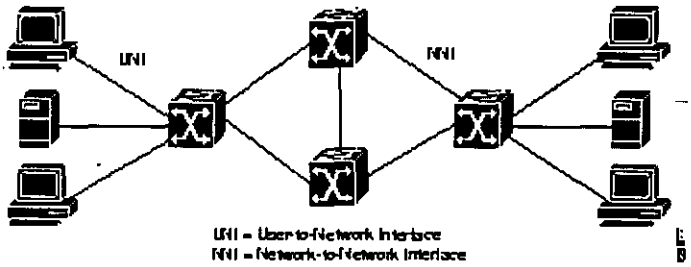
Funcionamiento de ATM

Dado que el propósito de este curso no es el aprender como funciona ATM a niveles muy específicos, se presentará únicamente una pequeña introducción de lo que es y en que nos puede beneficiar como diseñadores de redes que somos.

Estructura de una red ATM

Las redes ATM se basan en el concepto de que dos puntos finales se pueden comunicar entre sí mediante el uso de switches intermedios.

Figura 5-2 Componentes de una red ATM



Como se pude observar en la figura anterior, en ATM existen dos tipos de interfaces:

- UNI (User to Network Interface)
- NNI (Network to Network Interface)

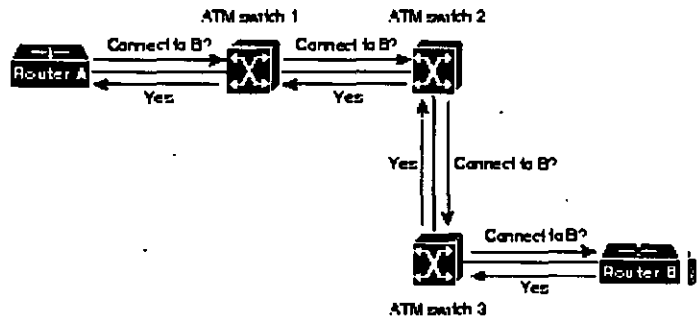
La conexión UNI se implementa entre el punto final (que puede ser un router, estación de trabajo, un servidor, etc.) y un switch ATM de una red pública o privada. NNI es usada para conectar entre sí. switches ATM. Tanto UNI como NNI pueden ser implementadas mediante diferentes tipos de conexiones físicas.

Además de UNI y NNI, el foro de ATM ha definido una serie de estándares para hacer una emulación de red local (LANE: LAN Emulation) y los protocolos del PNNI (Private Network to Network Interface). LANE es una tecnología que nos permite utilizar las redes locales con las que actualmente contamos (Ethernet, FDDI, Token Ring, etc.) he interactuar con los dispositivos conectados a las redes ATM. PNNI está basado en la versión 3.0 de UNI en cuanto a señalización y ruteo estático. El foro ATM está todavía trabajando en la siguiente fase que el ruteo dinámico. Muchas de las redes basadas en LANE con múltiples switches utilizan el protocolo PNNI.

Operación general de ATM

Dado que ATM es orientado a conexión, antes de transmitir datos los puntos finales de la red deben estar comunicados y sincronizados. Esta conexión está acompañada de un protocolo de señalización, tal y como se presenta en la siguiente figura.

Figura 5-3 Establecimiento de una conexión en una red ATM



Cuando el router A se quiere conectar con el router B, sucede lo siguiente.

1. El router A envía un paquete de señal de *request* al switch al cual está directamente conectado. Este request contiene la dirección ATM del router B así como cualquier tipo de parámetro de QoS (Quality of Service) requerido para la conexión.
2. El switch ATM 1 re-ensambla el paquete de señalización del router A y lo examina.
3. Si el switch ATM 1 tiene una entrada para el router B en su tabla de switcheo y puede brindar el QoS, establece una conexión virtual y reenvía el request hacia el siguiente switch (ATM switch 2) de la ruta.
4. Cada switch dentro de la ruta hacia router B re-ensambla y examina el paquete de señalización y lo reenvía al siguiente si puede soportar los parámetros del QoS. También cada switch establece la conexión virtual al mismo tiempo que reenvía el paquete de señalización hacia el siguiente. Si algún switch de la ruta no puede brindar los servicios del QoS, entonces dicho request es rechazado y un mensaje de "no aceptado" es enviado de regreso hacia el router A.
5. Cuando el paquete de señalización llega al router B, éste lo re-ensambla y lo evalúa. Si el router B puede soportar el request de QoS, lo responde con un mensaje de "aceptación". Al mismo tiempo que este paquete es propagado a través de los switches de la ruta, estos van estableciendo una conexión virtual.
6. El router A recibe el mensaje de "aceptación" del switch al cual está directamente conectado asi como el VPI (Virtual Path Identifier) y el VCI (Virtual Channel Identifier) que serán usados para transmitir las celdas hacia el router B.

Capas de ATM

Tal y como muchos otros protocolos, ATM está construido en base a varias capas que realizan ciertas acciones basadas en el modelo de referencia OSI. La función que desarrolla cada capa puede ser comparada con la definición del modelo OSI, de la siguiente manera:

Capa física:

Controla la transmisión y recepción de bits en el medio físico. También se encarga de hacer la reconstrucción de los frames que van a viajar por cada medio, dependiendo que de tipo de tecnología se esté manejando por cada interfaz particular (transformación de frames y celdas).

Capa de ATM:

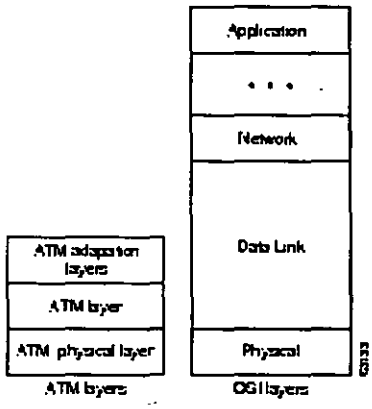
Establece las conexiones virtuales y pasa las celdas ATM a través de la red ATM, para realizarlo utiliza información contenida en las cabeceras de cada celda. Esta capa es responsable de realizar las cuatro funciones básicas siguientes.

- Multiplexaje/demultiplexaje de celdas de diferentes conexiones virtuales. Cada conexión se identifica de acuerdo a los valores de VCI y VPI.
- Traducción de los valores de VCI y VPI en los switches ATM.
- Extracción e inserción de las cabeceras antes de que la celda sea entregada o recibida desde o hacia una capa superior de adaptación.
- Implementación de un mecanismo de control de flujo a nivel de UNI.

Capa de Adaptación (AAL)

Esta capa traduce entre las grandes unidades de servicio de datos (SDUs Service Data Units) –por ejemplo: flujos de video y paquetes de datos- de las capas superiores y las celdas de ATM. Específicamente, AAL recibe paquetes de los protocolos superiores (por ejemplo: IP, AppleTalk, IPX) y los segmenta en celdas de 48 bytes que forman el *payload* de la celda ATM. Actualmente se han definido varias capas de adaptación.

Figura 5-5 Relación entre las capas de ATM y las del modelo OSI



Tipos de switches ATM

Aunque todos los switches ATM realizan el "acarreo" de celdas, entre ellos se pueden dar marcadas diferencias en los sentidos siguientes:

- Variedad de servicios e interfaces soportadas.
- Redundancia.
- Capacidad del interoperabilidad del software de ATM.
- Sofisticación de los mecanismos de administración.

Así como también existen routers que manejan diferentes funcionalidades y capacidades de procesamiento, los switches también los podemos encontrar de diferentes presentaciones y capacidades y por tanto los podemos clasificar de la siguiente manera:

Switches de Campus y para grupos de trabajo

Los switches para grupos de trabajo se caracterizan por tener puertos ethernet y un *uplink* de ATM que los conecta a la red ATM del campus.

Los switches de campus son normalmente utilizados en backbones de pequeña magnitud. Estos switches pueden incluso tener interfaces WAN que extiendan la red hacia las localidades remotas, y además añaden funcionalidades al backbone como las ELANs (Emulated LAN) que sirven para separar dominios de broadcast y así evitar las llamadas tormentas de broadcasts en el core de nuestra red.

Switches ATM de Corporativo

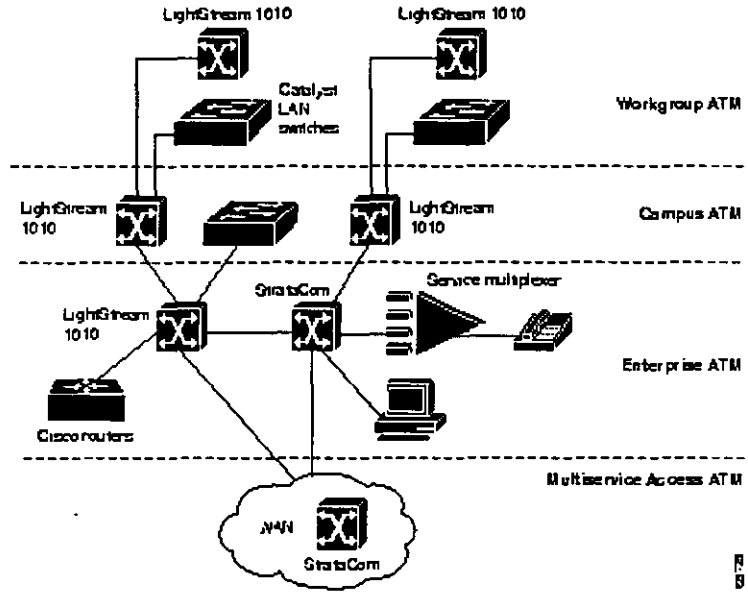
Estos switches son equipos multiservicio muy sofisticados que han sido diseñados para soportar el trafico de grandes backbones. Estos switches también son utilizados para interconectar switches de campus, pero también nos ofrecen la facilidad de integrar todos los servicios de nuestra red en nuestro backbone de ATM.

Switches de Multiservicio

Más allá de las redes privadas, los switches de multiservicio pueden ser utilizados para transportar grandes cantidades de información en las redes públicas. Estos tipos de switches están diseñados para ser empleados por los carriers, las grandes telefónicas y los ISPs que tarde o temprano ofrecerán servicios de valor agregado mediante el manejo del QoS de ATM a sus usuarios finales (que serán tanto grandes corporativos como medianas empresas).

En la siguiente figura se muestra el uso de estos diferentes tipos de switches en una red jerárquica. Los equipos mostrados son de la marca Cisco, pero la mayoría de las empresas que se dedican a producir este tipo de dispositivos, tienen sus modelos propios.

Figura 5-6 Disposición de los switches ATM en una internetwork



REFERENCIAS BIBLIOGRAFICAS

- Black, U. Data Networks: Concepts, theory and practice. Prentice Hall 1989.
- Comer, D.E. Internetworking with TCP/IP: Principles, protocols and architecture. Prentice Hall 1991.
- Meijer, A. Systems Network Architecture: A tutorial. John Willey & sons 1987
- Perlman, R. Interconections: Bridges and routers. Addison-Wesley 1992
- Schwarts, M. Telecomunications Networks: Protocols, modeling and analysis. Addison-Wesley 1987
- Spragins, J.D.Telecomunications protocols and design. Addion-Wesley 1991
- Stallings, W. Handbook of Computer-Communications Standards. Vols 1-3 Howard W. Sams Inc. 1990
- Sunshine, C.A. Computer Network Architectures and protocols Plenum Press 1989
- Spanier, S; Ford, M; Lew, K; Stevenson, K Internetworking Technologies Overview. New Riders 1997
- Halabi, B. Internet Routing Architectures. New Riders 1997

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

Palacio de Minería

Cursos Abiertos

DISEÑO DE REDES Y NUEVAS TECNOLOGIAS

PARTE II

CLAVE DEL CURSO CA144
19-23 OCTUBRE DE 1998

PROF. ING. FEDERICO VARGAS

DISEÑO DE REDES Y NUEVAS TECNOLOGIAS

INDICE

CAPÍTULO 3

MEDIOS DE TRANSMISIÓN

Se entiende por medio de transmisión a cualquier medio físico que pueda transportar información en forma de señales electromagnéticas. Los medios de transmisión permiten enviar la información de una estación de trabajo al servidor o a otra estación de trabajo y forman una parte esencial de una red local.

Para efectuar la transmisión de la información se utilizan lo que se denominan **TÉCNICAS DE TRANSMISIÓN.**

TÉCNICAS DE TRANSMISIÓN

Entre las más comunes están: banda base y banda ancha.

Banda base

Es el método más común dentro de las redes locales. Transmite las señales en forma digital sin emplear técnicas de modulación, en cada transmisión se utiliza todo el ancho de banda y, por tanto, sólo puede transmitir una señal simultáneamente.

Está especialmente indicada para cortas distancias, ya que en grandes distancias se producirían ruidos e interferencias (pueden utilizarse repetidores que vuelven a regenerar la señal).

Los medios de transmisión que se pueden utilizar son: el cable de par trenzado y el cable coaxial de banda base.

Banda ancha

Consiste en transmitir las señales en forma digital modulando la señal sobre ondas portadoras que pueden compartir el ancho de banda del medio de transmisión mediante multiplexación por división de frecuencia. Es decir, actúa como si en lugar de un único medio se estuvieran utilizando líneas distintas.

El ancho de banda depende de la velocidad de transmisión de los datos.

Este método hace imprescindible la utilización de un módem para poder modular y demodular la información.

La distancia máxima puede llegar hasta los 50 kms, permitiendo usar además los elementos de conexión de la red para transmitir otras señales distintas de las propias de la red como pueden ser señales de televisión o señales de voz.

Los medios de transmisión que se pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

TIPOS DE CABLES

En el siguiente esquema (aun con riesgo de realizar una excesiva simplificación) se muestran las características comparadas de los cuatro tipos de cables utilizados para transmisión de voz y datos:

	Par trenzado	Coaxial de banda base	Coaxial de banda ancha	Fibra óptica
Ancho de Banda	Baja	Moderada	Alta	Muy alta
Instalación	Sencilla	Fácil	Fácil	Difícil
Longitud	Baja	Moderada	Alta	Muy alta
Costo	Barato	Moderado	Caro	Muy caro
Fiabilidad de la transmisión	Baja	Alta	Alta	Muy alta
Interferencias	Alta	Moderada	Baja	Ninguna
Seguridad	Baja	Baja	Moderada	Alta
Topología	Bus Estrella Anillo	Bus – –	Bus estrella –	– estrella anillo

Cable de par trenzado

Es un cable formado por un par de hilos de cobre trenzados entre sí y recubierto de una vaina de plástico. El grosor de los hilos y el número de vueltas del trenzado pueden variar. Normalmente no tiene blindaje o es muy reducido.

Se usa normalmente para las instalaciones telefónicas y para la transmisión de señales digitales.

Puede ser apantallado (**STP**) con una impedancia de 120-150 ohmnios o sin apantallar (**UTP**) con una impedancia de 100 ohmnios.

Los conectores utilizados son los denominados **RJ45** y **RJ11**.

En función de sus características se clasifica en cinco categorías:

- **Categoría 1**: Es el cable telefónico tradicional de par trenzado sin apantallar. Se utiliza para transmitir voz pero no datos.

- **Categoría 2**: Es un cable de cuatro pares trenzados sin apantallar. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 4 **Mbps**.

- **Categoría 3**: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 10 **Mbps** (actualmente se puede utilizar en velocidades superiores) con longitudes de segmento inferiores a 100 metros y una máxima longitud de la red de 500 metros.

- **Categoría 4**: Es un cable de cuatro pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 16 **Mbps** (actualmente está en desuso).

- **Categoría 5**: Es un cable de cobre de dos pares trenzados. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 **Mbps** (actualmente, al reducirse su coste es el que está siendo más utilizado).

ANCHO DE BANDA

Se usa con técnicas de banda base y con un ancho de banda bajo.

INSTALACIÓN

Es muy sencillo de instalar y su uso está muy extendido.

LONGITUD

La distancia en la que se puede utilizar es baja y está limitada a un único edificio.

COSTO DE LA INSTALACIÓN

El costo de la instalación es muy bajo y depende del número de vueltas del trenzado, del grosor del hilo y del tipo de aislamiento.

FIABILIDAD

Es un cable muy fiable aunque de una gran vulnerabilidad debido a que se puede dañar si no se instala bien o se dobla demasiado.

INTERFERENCIAS

Es muy vulnerable a interferencias eléctricas, lo que produce altos índices de error en la transmisión de los datos. No se debe instalar cerca de dispositivos que produzcan fuertes campos electromagnéticos.

SEGURIDAD DE LA RED

Las señales emitidas pueden ser interceptadas fácilmente por estaciones ajenas a la red local.

TOPOLOGÍA

Es usado en topologías en forma de bus, estrella y anillo.

Cable coaxial de banda base

Es un cable formado por un hilo conductor central rodeado de un material aislante que, a su vez, está rodeado por una malla fina de hilos de cobre o aluminio o una malla fina cilíndrica. Todo el cable está rodeado por un aislamiento que le sirve de protección para reducir las emisiones eléctricas.

Se usa normalmente para las instalaciones telefónicas y para los sistemas de antenas colectivas de televisión.

Trasmite una sola señal a una velocidad de transmisión alta.

En función de sus características se clasifica en dos categorías:

- **Cable coaxial grueso (10BASE5).** Su impedancia es de 50 ohmnios y lleva un conector tipo "N". Alcanza una velocidad de transmisión de 10 **Mbps** y una longitud máxima de 500 metros de segmento de red.

- **Cable coaxial delgado (10BASE2).** Su impedancia es de 50 ohmnios y lleva un conector tipo "**BNC**". Alcanza una velocidad de transmisión de 10 **Mbps** y una longitud máxima de 200 metros de segmento de red.

ANCHO DE BANDA

Se usa con técnicas de banda base y con un ancho de banda bajo.

INSTALACIÓN

Es sencillo de instalar aunque más complicado que el cable de par trenzado, ya que se ha de introducir dentro de un portacables o bien empotrarlo en la pared.

LONGITUD

La distancia en la que se puede utilizar es moderada debido a que es muy sensible a los ruidos eléctricos.

COSTO DE LA INSTALACIÓN

El costo de la instalación es moderado aunque un poco más caro que el del cable de par trenzado.

FIABILIDAD

Es un cable fiable, fuerte y resistente, aunque se puede dañar si no se instala bien.

INTERFERENCIAS

Es vulnerable a interferencias eléctricas y muy sensible a los ruidos eléctricos, lo que produce índices de error en la transmisión de los datos. No se debe instalar cerca de dispositivos que produzcan fuertes campos electromagnéticos.

SEGURIDAD DE LA RED

Las señales emitidas pueden ser interceptadas por estaciones ajenas a la red local y, a su vez, emitir señales que pueden interferir en sistemas de televisión o de radio que se encuentren cerca de la red.

TOPOLOGÍA

Es usado principalmente en topologías en forma de bus.

Cable coaxial de banda ancha (10BROAD36)

Está construido de forma muy similar al coaxial de banda base aunque puede tener mayores diámetros y con diversos grosores de aislamiento.

Su impedancia es de 75 ohmnios. Alcanza una velocidad de transmisión de 10 **Mbps** y una longitud máxima de 1.800 metros de segmento de red.

Puede transportar miles de canales de datos a baja velocidad.

Debido a su limitación en la velocidad de transmisión, está siendo sustituido por cableados de par trenzado de la categoría 5 y cables de fibra óptica.

ANCHO DE BANDA

Se usa con técnicas de banda ancha y, si el sistema es de un solo cable, la señal se dividirá en dos frecuencias: la de transmisión y la de recepción.

INSTALACIÓN

Es sencillo de instalar aunque más complicado que el cable de par trenzado, ya que se ha de introducir dentro de un portacables o bien empotrarlo en la pared.

LONGITUD

La distancia en la que se puede utilizar es alta pudiendo llegar a varios kilómetros.

COSTO DE LA INSTALACIÓN

El costo de la instalación es caro debido al equipo que necesita para su utilización.

FIABILIDAD

Es un cable fiable, fuerte y resistente, aunque se puede dañar si no se instala bien.

INTERFERENCIAS

Capta únicamente interferencias electromagnéticas de baja frecuencia.

SEGURIDAD DE LA RED

Las señales emitidas pueden ser interceptadas por estaciones ajenas a la red local, pero no emite señales que puedan interferir en sistemas de televisión o de radio que se encuentren cerca de la red.

TOPOLOGÍA

Es usado en topologías en forma de bus y estrella.

Cable de fibra óptica

Está formado por un cable compuesto por fibras de vidrio. Cada filamento tiene un núcleo central de fibra de vidrio con un alto índice de refracción que está rodeado de una capa de material similar pero con un índice de refracción menor. De esa manera aísla las fibras y evita que se produzcan interferencias entre filamentos contiguos a la vez que protege al núcleo. Todo el conjunto está protegido por otras capas aislantes y absorbentes de luz.

Está formado por tres componentes:

- **Transmisor de energía óptica**. Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

- **Fibra óptica** Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

- **Detector de energía óptica**. Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal)

Puede alcanzar velocidades muy altas a grandes distancias sin necesidad de usar repetidores (el producto de la distancia en kilómetros por la velocidad en **Mbps** no puede ser superior a 30. Por ejemplo, puede alcanzar una velocidad de 50 **Mbps** en una distancia de 600 metros o una velocidad de 10 **Mbps** a 3.000 metros).

ANCHO DE BANDA

Se usa con técnicas de banda ancha y con un ancho de banda muy elevado.

INSTALACIÓN

Es difícil de instalar porque las conexiones han de ser muy precisas.

LONGITUD

La distancia en la que se puede utilizar es muy alta pudiendo llegar a varios kilómetros.

COSTO DE LA INSTALACIÓN

La instalación es muy cara debido al alto costo de la instalación y al equipo que necesita para su funcionamiento.

FIABILIDAD

Es un cable fiable, fuerte y muy resistente, con un período de vida largo aunque vulnerable a pérdidas de señal por presión excesiva o por dobleces en el cable.

INTERFERENCIAS

No capta ninguna interferencia electromagnética.

SEGURIDAD DE LA RED

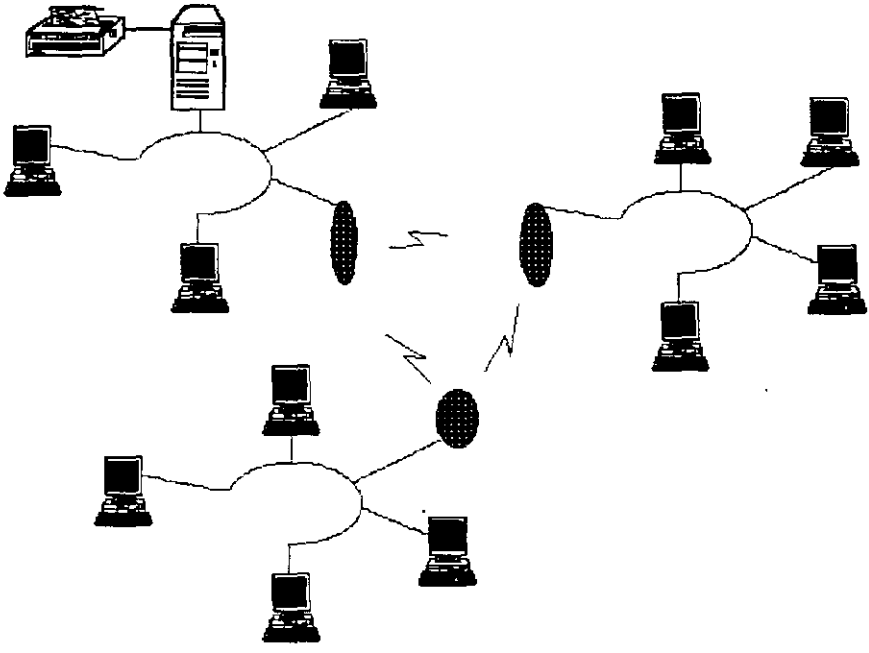
Las señales emitidas no pueden ser interceptadas por estaciones ajenas a la red local y no emite ninguna señal que pueda interferir en sistemas de televisión o de radio que se encuentren cerca de la red.

TOPOLOGÍA

Es usado en topologías en forma de estrella y de anillo.

Redes locales inalámbricas

Una red local se denomina inalámbrica cuando los medios de unión entre las estaciones no son cables.



Configuración en anillo compuesto

Las principales ventajas de este tipo de redes son:

- Permiten una amplia libertad de movimientos.
- Sencillez en la reubicación de las estaciones de trabajo evitando la necesidad de establecer un cableado.

- Rapidez en la instalación.

Los principales inconvenientes son:

- Dudas sobre si afecta a la salud de los usuarios.
- Faltan normas estándar.
- Poca compatibilidad con las redes fijas.
- Problemas con la obtención de licencias para aquellas que utilizan el espectro radioeléctrico.
- Su utilización está especialmente recomendada para la instalación de redes en aquellos lugares donde no pueda realizarse un cableado o en lugares con una movilidad de las estaciones de trabajo muy grande.

Actualmente existen cuatro técnicas para su utilización en redes inalámbricas que son: infrarrojos, radio en **UHF**, microondas y láser.

Infrarrojos

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta y que pueden ser interrumpidas por cuerpos opacos.

No se ven afectados por interferencias externas y pueden alcanzar hasta 200 metros entre el emisor y el receptor. No es necesaria la obtención de una licencia administrativa para su uso.

Existe una red basada en infrarrojos compatible con la red **TOKEN RING** de **IBM** denominada **InfraLAN** que tiene una velocidad de transmisión de 4 **Mbps**.

Radio UHF

Una red basada en equipos de radio en **UHF** necesita para su instalación la obtención de una licencia administrativa. No se ve interrumpida por cuerpos opacos gracias a su cualidad de difracción.

Hay dos tipos de redes que utilizan esta técnica:

- **PureLAN.** Es una red compatible con **Novell NetWare, LAN Manager, LAN Server** y **TCP/IP**. Tiene una velocidad de transmisión de 2 **Mbps** y una cobertura de 240 metros.

- **WaveLAN.** Es compatible con **Novell NetWare.** Tiene una velocidad de transmisión de 2 **Mbps** y una cobertura de 335 metros.

Microondas

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las super altas frecuencias, utilizándose para las redes inalámbricas la banda de los 18-19 **Ghz**.

Rialta de **Motorola** es una red de este tipo. Cuenta con una velocidad de transmisión de 10 **Mbps** y una cobertura de 500 metros.

Láser

Esta tecnología para redes inalámbricas, que está en fase de investigación, es útil actualmente para conexiones punto a punto con visibilidad directa, y se utiliza fundamentalmente para interconectar segmentos distantes de redes locales convencionales (**ETHERNET** y **TOKEN RING**), llegando a cubrir distancias de hasta 1000 metros.

CAPÍTULO 4

NORMAS ESTÁNDAR

Para poder establecer una comunicación entre ordenadores, lo mismo que para establecerla entre personas, es necesario contar con una serie de normas que regulen dicho proceso.

Esas normas las fija la sociedad en general (en el caso de las personas) o se hace a través de organismos internacionales de normalización (en el caso de las máquinas).

Se entiende por protocolo al conjunto de reglas que hacen posible el intercambio fiable de comunicación entre dos equipos informáticos.

NIVELES OSI

Al principio del desarrollo de la informática, cada fabricante establecía los procedimientos de comunicación entre sus ordenadores de forma independiente siendo muy difícil, por no decir imposible, la comunicación entre ordenadores de fabricantes distintos.

Poco a poco se fue haciendo necesario disponer de unas normas comunes que permitiesen la intercomunicación entre todos los ordenadores.

De todos los protocolos propuestos destaca el modelo **OSI (Open Systems Interconnection)**, cuya traducción al castellano es **Interconexión de Sistemas Abiertos**, que fue propuesto por la **Organización Internacional de Normalización (ISO)**.

ISO que es una organización no gubernamental fundada en 1947, tiene por misión la coordinación del desarrollo y aprobación de estándares a nivel internacional. Su ámbito de trabajo cubre todas las áreas, incluyendo las redes locales, a excepción de las áreas electrotécnicas que son coordinadas por **IEC (International Electrotechnical Commission)**.

Cada país únicamente puede estar representado en **ISO** por una organización (en el caso de España, está representada por **AENOR (Asociación Española de Normalización)** y en el caso de EE.UU, está representada por **ANSI (American National Standards Institute)**.

El modelo **OSI**, cuya actividad se empezó a desarrollar en 1977 y llegó a constituirse como estándar internacional en 1983, trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos.

Propone dividir en niveles todas las tareas que se llevan a cabo en una comunicación entre ordenadores. Todos los niveles estarían bien definidos y no interferirían con los demás. De ese modo, si fuera necesaria una corrección o modificación en un nivel no afectaría al resto.

En total se formarían siete niveles (los cuatro primeros tendrían funciones de comunicación y los tres restantes de proceso).

Cada uno de los siete niveles dispondría de los protocolos específicos para el control de dicho nivel.

NIVEL 1	FÍSICO
NIVEL 2	ENLACE DE DATOS
NIVEL 3	RED
NIVEL 4	TRANSPORTE
NIVEL 5	SESIÓN
NIVEL 6	PRESENTACIÓN
NIVEL 7	APLICACIÓN

Nivel físico

En este nivel se definen las características eléctricas y mecánicas de la red necesarios para establecer y mantener la conexión física (se incluyen las dimensiones físicas de los conectores, los cables y los tipos de señales que van a circular por ellos). Los sistemas de redes locales más habituales definidos en este nivel son: **Ethernet**, red en anillo con paso de testigo (**Token Ring**) e interfaz de datos distribuidos por fibra (**FDDI**, **Fiber Distributed Data Interface**).

Nivel de enlace de datos

Se encarga de establecer y mantener el flujo de datos que discurre entre los usuarios. Controla si se van a producir errores y los corrige (se incluye el formato de los bloques de datos, los códigos de dirección, el orden de los datos transmitidos, la detección y la recuperación de errores). Las normas **Ethernet** y **Token Ring** también están definidas en este nivel.

Nivel de red

Se encarga de decidir por dónde se han de transmitir los datos dentro de la red (se incluye la administración y gestión de los datos, la emisión de mensajes y la regulación del tráfico de la red). Entre los protocolos más utilizados definidos en este nivel se encuentran: **Protocolo Internet** (**IP, Internet Protocol**) y el **Intercambio de paquetes entre redes** (**IPX, Internetwork Packet Exchange**) de **Novell**.

Nivel de transporte

Asegura la transferencia de la información a pesar de los fallos que pudieran ocurrir en los niveles anteriores (se incluye la detección de bloqueos, caídas del sistema, asegurar la igualdad entre la velocidad de transmisión y la velocidad de recepción y la búsqueda de rutas alternativas). Entre los protocolos de este nivel más utilizados se encuentran el **Protocolo de Control de la Transmisión** (**TCP, Transmission Control Protocol**) de **Internet**, el **Intercambio Secuencial de paquetes** (**SPX, Sequenced Packet Exchange**) de **Novell** y **NetBIOS/NetBEUI** de **Microsoft**.

Nivel de sesión

Organiza las funciones que permiten que dos usuarios se comuniquen a través de la red (se incluyen las tareas de seguridad, las contraseñas de usuarios y la administración del sistema).

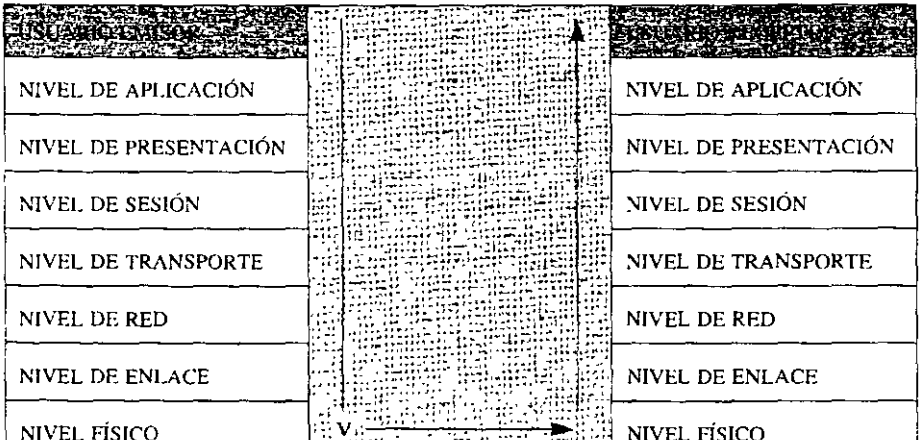
Nivel de presentación

Traduce la información del formato de la máquina a un formato entendible por los usuarios (se incluyen el control de las impresoras, la emulación de terminal y los sistemas de codificación).

Nivel de aplicación

Se encarga del intercambio de información entre los usuarios y el sistema operativo (se incluyen la transferencia de archivos y los programas de aplicación).

El proceso que se produce desde que un usuario envía un mensaje hasta que llega a su destino consiste en una bajada a través de todos los niveles (con sus correspondientes protocolos) desde el nivel séptimo hasta llegar al primero. Allí se encontrará en el canal de datos que le dirigirá al usuario destino y volverá a subir por todos los niveles hasta llegar al último de ellos.



CONTROL DE ERRORES

Debido a las interferencias, ruidos y distorsiones que aparecen en la línea, los datos al llegar a la estación destino pueden haber sufrido alguna modificación y no corresponder exactamente con los que fueron emitidos.

Para detectar estos errores se emplean diversas técnicas, que dependen del protocolo elegido.

Los métodos más utilizados para el control de los errores son:

- Método de paridad.
- Método de Redundancia Cíclica.

Método de paridad

Este método, también llamado geométrico, consiste en añadir un **bit** (**bit** de paridad) a cada uno de los caracteres enviados. Este **bit** debe tener el valor cero o uno y será tal que haga que el carácter, contando el **bit** de paridad, tenga un número par de **bits** con valor uno (en el caso de la paridad par) o que tenga un número impar de unos (en el caso de la paridad impar).

La estación destino cuenta el número de **bits** uno de cada carácter recibido y, si el valor calculado coincide con el correspondiente a la paridad utilizada, la transmisión ha sido correcta, pero si no ha sido así, solicita a la estación emisora que repita el envío.

Este **bit de paridad** (par o impar) que se añade al final de cada carácter, también recibe los nombres de **bit de paridad transversal**, **bit de paridad vertical** o **comprobación de redundancia vertical** (**VRC**).

He aquí un ejemplo de paridad par, donde se indican en negrita los **bits de paridad**:

11100010
00011101
11001001
01101100

Este método cuenta con el problema de que únicamente puede detectar el error si se ha modificado un solo **bit**. Pero si se modifica un número par de **bits**, no se detectará el error. Para evitar este problema, se puede incluir al final de cada paquete un **bit** de comprobación de error que hará que la suma de unos de cada columna de **bits** corresponda con la paridad par o impar que se está utilizando.

11100010
00011101
11001001
01101100
01011010

A este **bit** se le denomina **carácter de comprobación horizontal, suma de comprobación (checksum), paridad horizontal** o **comprobación de redundancia horizontal (LRC).**

Si se emplea la paridad vertical y la horizontal, se podrían llegar a detectar todos los errores de un **bit** que se produzcan.

Método de Redundancia Cíclica

Este método consiste en que la estación emisora agrega al final de cada bloque de datos una información calculada de acuerdo con una formula polinómica cuyas variables son los ceros y unos enviados en el bloque de datos (se divide el valor binario numérico total por un valor constante definido por el protocolo, se desecha el cociente y el resto es lo que se añade al final del bloque de datos).

La estación destino realiza el mismo cálculo. Si le produce el mismo resultado la transmisión es correcta, pero si no ha sido así, solicita a la estación emisora que repita el proceso.

Este método recibe el nombre de **Código de Redundancia Cíclica (CRC)** y a los valores añadidos al bloque de datos se le denomina **Carácter de Comprobación de Bloque (BCC)** o simplemente **Redundancia.**

La ventaja de este método estriba en que el número de **bits** que se añaden a cada bloque de datos es mucho menor al del método anterior.

Normalmente, la estación destino no corrige los bloques de datos erróneos sino que se limita a detectar la existencia del error, pidiéndole a la estación emisora que vuelva a emitir dicho bloque de datos.

Para la retransmisión del bloque de datos erróneo existen dos técnicas:

- Parada y espera.
- Envío continuo.

Parada y espera

Esta técnica consiste en que la estación emisora, después de enviar el bloque de datos, espera a recibir una contestación de confirmación o error del envío.

Si la transmisión es correcta, la estación receptora envía un mensaje de confirmación (**ACK**) y, si la transmisión es errónea, envía un mensaje de rechazo (**NAK**). AL recibir el mensaje de rechazo, la estación emisora procede a retransmitir el bloque de datos erróneo.

El inconveniente de esta técnica es el tiempo que pierde la estación emisora en esperar el mensaje de la estación receptora antes de proceder a un nuevo envío.

Envío continuo

Esta técnica consiste en que la estación emisora está enviando bloques de datos continuamente sin tener que permanecer a la espera de la confirmación de la estación receptora. Para poder realizarlo, identifica cada bloque de datos con una identificación numérica.

Cuando se produce un error, la estación receptora solicita el reenvío del bloque erróneo y se pueden producir dos modalidades:

- **Envío continuo no selectivo**. En este modo, la estación emisora vuelve a retransmitir todos los bloques enviados desde aquel en el que se produjo el error. Esto provoca el reenvío de bloques que se podían haber recibido correctamente.
- **Envío continuo selectivo**. En este modo, la estación emisora vuelve a retransmitir únicamente aquel bloque en el que se produjo el error.

RECUPERACIÓN ANTE FALLOS

En el caso de que se produjera un envío de un bloque de datos, la estación emisora estuviera esperando el mensaje de confirmación o error y la estación receptora se desconectara o se perdiera dicho mensaje, la estación emisora estaría esperando indefinidamente dicha contestación.

En ese caso, el protocolo debería proceder de la siguiente manera:

- Establecer un tiempo de espera de dicha contestación.
- Solicitar una nueva respuesta cuando haya finalizado dicho tiempo de espera.
- Limitar el número de intentos, después de los cuales el fallo se da por irrecuperable y finalizaría la transmisión de datos con dicha estación.

CAPÍTULO 6

PROTOCOLOS DE RED Y DE TRANSPORTE

Entre los protocolos de red y de transporte se encuentran: **IPX/SPX**, **NetBIOS/NetBEUI** y **AppleTalk**.

IPX/SPX

Los protocolos de comunicación y transporte **IPX/SPX** fueron desarrollados por **Novell** a principios de los años ochenta inspirándose en los protocolos del **Sistema de Red de Xerox (XNS)**.

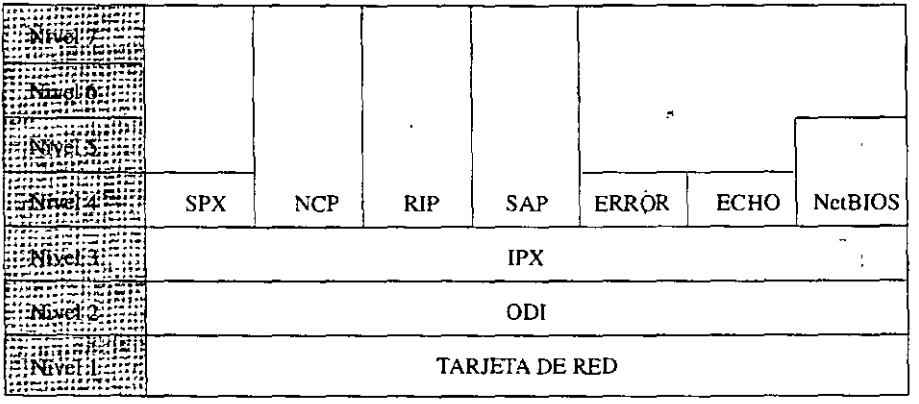
Sirven de interfaz entre el sistema operativo de red **NetWare** y las distintas arquitecturas de red (**Ethernet, Arcnet, Token Ring**).

Consiste en una variedad de protocolos iguales tales como:

- **IPX (Internetwork Packet Exchange)**.
- **SPX (Sequential Packet Exchange)**.
- **NCP (Network Core Protocol)**.
- **SAP (Service Advertising Protocol)**.
- **RIP (Router Information Protocol)**.

Novell ha implementado también un emulador **NetBIOS** para que las aplicaciones que utilicen **NetBIOS** puedan usar **IPX** como protocolo de red.

Además, se utilizan los protocolos **Echo** y **Error** para mantenimiento interno.



El nivel **ODI (Open Data-Link Interface)** de **Novell** proporciona una función parecida a la del nivel de enlace de datos de **OSI** (se verá en un capítulo posterior).

Ipx

El protocolo de red **IPX** es un protocolo que transmite los datos en **datagramas** (paquetes autocontenidos que viajan de forma independiente desde el origen al destino en modo sin conexión, pero no esperan una confirmación de la estación receptora indicando si ha recibido correctamente o no el bloque de datos).

De esa manera se mejora el rendimiento de la transmisión pero no pierde en fiabilidad por dos razones:

- Cada bloque de datos **IPX** contiene una suma de comprobación **CRC** que garantiza un 99% de precisión.

- En caso de no haber contestación en un intervalo determinado de tiempo, **IPX** reenvía el paquete de forma automática.

La estructura de un bloque de datos **IPX** es la siguiente:

Suma de comprobación	2 **Bytes**
Longitud	2 **bytes**
Control de transporte	1 **byte**
Tipo de paquete	1 **byte**
Red de destino	4 **bytes**
Nodo de destino	6 **bytes**
Conector de destino	2 **bytes**
Red de origen	4 **bytes**
Nodo de origen	6 **bytes**
Conector de origen	2 **bytes**
Datos	

Spx

El protocolo de transporte **SPX** es una extensión del protocolo de red **IPX** de nivel superior orientado a la conexión.

SPX utiliza **IPX** para enviar y recibir paquetes pero añade una interfaz para establecer una sesión entre la estación emisora y la receptora, de esa manera se obtiene una confirmación explícita de la recepción del paquete.

Además, proporciona un mecanismo de secuenciación de los paquetes. Como **IPX** envía los paquetes por el mejor camino disponible, es posible que éstos lleguen a la estación receptora en orden distinto al que fueron enviados, lo que provoca que lleguen fuera de secuencia. Así, **SPX** de la estación receptora puede organizar los paquetes en el orden adecuado o bien reclamar únicamente los paquetes perdidos.

Los paquetes **SPX** tienen la misma estructura que los **IPX**, pero añadiendo a la cabecera 12 **bytes** para el control de la conexión y el número de secuencia del paquete.

Ncp

El protocolo **NCP** es un conjunto propietario de mensajes bien definidos que controlan el funcionamiento del servidor y son la clave del acceso a los servicios de **NetWare**.

Define el procedimiento que sigue **NetWare** para aceptar y responder a las solicitudes de las estaciones. Existen protocolos de servicio **NCP** para cada servicio que una estación pueda solicitar a un servidor y sin los cuales no podría sacar ningún servicio del servidor.

Los **NCP** se pasan al servidor mediante paquetes **IPX** marcados de forma especial. No obstante, se pueden transmitir con cualquier otro protocolo de datagramas (como, por ejemplo, **UDP** de las redes basadas en **TCP/IP**).

Rip

El protocolo **RIP** es un protocolo de información de encaminamiento que incorpora **NetWare** y que se encarga de llevar los paquetes a su destino entre dos redes.

Cada servidor realiza un seguimiento de los otros servidores a intervalos regulares y conserva su posición y distancia en una tabla de información sobre encaminamiento.

Si un servidor detecta una inconsistencia en un encaminador existente, lo notifica a los demás para que actualicen sus tablas. Si un encaminador falla, los demás encaminadores lo descubren y buscan rutas alternativas que no tienen en cuenta al encaminador defectuoso.

El proceso de encaminamiento utiliza esa información para transmitir los paquetes por la ruta más corta hasta su destino final.

Sap

El protocolo de anuncio de servicios **SAP** es un mecanismo mediante el cual, **NetWare**, distribuye por toda la red información de los servicios disponibles.

Necesita un servidor que anuncie tres unidades de información a la red cada minuto: el nombre del servidor, el tipo de servidor y su dirección de red.

El resto de los servidores recogen la información y la guardan en su tabla correspondiente.

Cuando un servidor descubre que se está desactivando, se lo indica a **SAP** y éste lo transmite a los demás servidores que lo guardan en su tabla correspondiente.

Si un servidor deja de transmitir sin previo aviso, **SAP** supone que no está disponible y lo transmite a toda la red para que actualicen su tabla todos los servidores.

NETBIOS/NETBEUI

Cuando se empezaron a desarrollar las redes locales, **IBM** introdujo el protocolo **NetBIOS (Network Basic Input/Output System)**, debido a la falta de normas estándar para los niveles superiores.

IBM lo utiliza para proporcionar servicios de sesión entre **LAN Requester** y **LAN Server.**

NetBIOS mantiene la sesión enviando periódicamente un bloque de datos al nodo remoto para informarle de que se encuentra disponible y de que puede recibir datos, por lo que utiliza ciclos de memoria de manera continua aunque la aplicación del usuario no realice peticiones

Novell hizo una implementación de **NetBIOS** para **IPX** de forma análoga a **SPX**. Pero no genera bloques compatibles con el **NetBIOS** de **IBM**, por lo que no puede comunicarse con otra que utilice el entorno **IBM**.

El protocolo **NetBEUI (NetBios Extended User Interface)**. Es la extensión para **NetBIOS** utilizada por **LAN Manager, Microsoft Windows para Trabajo en Grupo** y **Microsoft Windows NT** que corresponde a los niveles de red y transporte.

APPLETALK

AppleTalk es un protocolo propietario que se utiliza para conectar ordenadores **Macintosh** de **Apple** en redes locales.

<table>
<tr><td>Nivel 7</td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">AFP</td><td rowspan="2">PRINT SERVICES</td></tr>
<tr><td>Nivel 6</td></tr>
<tr><td>Nivel 5</td><td>ADSP</td><td>ZIP</td><td>ASP</td><td>PAP</td></tr>
<tr><td>Nivel 4</td><td>RTMP</td><td>AEP</td><td colspan="2"></td><td>ATP</td><td>NBP</td></tr>
<tr><td>Nivel 3</td><td colspan="6">DDP</td></tr>
<tr><td>Nivel 2</td><td colspan="6" rowspan="2">LAP/AARP/TLAP/ELAP
TOKENTALK/ETHERTALK/LOCALTALK</td></tr>
<tr><td>Nivel 1</td></tr>
</table>

AppleTalk admite las tecnologías **Ethernet** y **Token Ring**, además de la propietaria **LocalTalk** que es un sistema de cableado con topología de bus, propio de **Apple**, fácilmente configurable que permite conectar estaciones de trabajo y otros dispositivos a un entorno de red (**EtherTalk** es la versión que proporciona acceso a **Ethernet** y **TokenTalk** es la que lo hace con **Token Ring**).

LAP (Link Access Protocol) es el protocolo de acceso de enlace que proporciona los servicios básicos de transmisión de paquetes entre nodos de la red (la identificación de los nodos se realiza de forma dinámica con 8 **bits**).

AARP (AppleTalk Address Resolution Protocol) es el protocolo que realiza la traducción de la identificación de los nodos de **AppleTalk** a los de una red **Ethernet** o **Token Ring** (la identificación se realiza con 48 **bits**).

TLAP (TokenTalk Link Access Protocol) es el protocolo que utiliza para tener acceso a la red **Token Ring**.

ELAP (EtherTalk Link Access Protocol) es el protocolo que utiliza para tener acceso a la red **Ethernet**.

DDP (Datagram Delivery Protocol) es el protocolo de entrega de datagramas con un tamaño máximo de paquete de 586 **bytes** (en la cabecera del paquete se incluye la información de dirección de destino y comprobación de errores).

AEP (AppleTalk Echo Protocol) es un protocolo que determina si un nodo de destino va a estar disponible para la comunicación. También se utiliza para determinar el tiempo que emplea un paquete en alcanzar un nodo de la red.

NBP (Name Binding Protocol) es el protocolo que traduce la dirección numérica de **Internet** de un nodo en una dirección con nombre.

ATP (AppleTalk Transaction Protocol) maneja las solicitudes, respuestas y liberaciones de transacciones para garantizar la entrega de los paquetes.

RTMP (Routing Table Maintenance Protocol) mantiene la tabla de encaminamiento con las direcciones y se comunica con otros encaminadores para determinar el estado de la red.

ASP (AppleTalk Session Protocol) es un cliente de **ATP** que se encarga de iniciar y terminar las sesiones entre dos nodos.

ZIP (Zone Information Protocol) es el encargado de mantener el mapa de red en lo referente al encaminamiento y control.

ADSP (AppleTalk Data Stream Protocol) gestiona la transmisión de datos entre dos ordenadores. Permite que ambos transmitan a la vez (transmisión **dúplex**).

PAP (Printer Access Protocol) mantiene la comunicación entre una estación de trabajo y una impresora.

AFP (AppleTalk Filing Protocol) proporciona acceso a los archivos remotos en servidores de la red.

CAPÍTULO 8

TIPOS DE REDES LOCALES

Hay muchos tipos distintos de redes locales, e incluso se pueden realizar múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de transmisión e incluso los protocolos utilizados. Estos factores van a determinar la **arquitectura de la red local**.

Sin embargo, de todas las posibles soluciones hay tres que ya están establecidas y que, al mismo tiempo, cuentan con una gran difusión dentro del mundo de las redes locales:

- Ethernet.
- Token Ring.
- Arcnet.

ETHERNET

Esta red fue desarrollada por **Xerox Corporation** para enlazar un grupo de microordenadores que estaban distribuidos por los laboratorios de investigación de **Palo Alto** en California para poder intercambiar programas y datos, así como compartir los periféricos.

En un principio se creó para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cable.

Si se utiliza cable coaxial grueso, se pueden tener hasta cuatro tramos de cable (unidos con repetidores) y los ordenadores se conectan al cable por medio de transceptores (la distancia máxima entre el ordenador y el transceptor ha de ser de 15 metros). Se pueden conectar ordenadores en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

Si se utiliza cable coaxial fino, no es necesario utilizar transceptores, pudiéndose conectar el cable al ordenador por medio de una conexión **BNC** en forma de **T**. El número máximo de tramos es de cinco y la longitud máxima de cada tramo es, aproximadamente, de un tercio de la longitud máxima conseguida con el cable coaxial grueso (550 metros). Así mismo, el número máximo de estaciones es de 30 por cada uno de los tres tramos en los que se pueden conectar ordenadores.

Los datos se transmiten a una velocidad de 10 **Mbps** a una distancia máxima de dos kilómetros.

Utiliza una topología en bus con protocolo de contienda **CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones)**. Como se vio anteriormente, cualquier estación puede intentar transmitir en cualquier momento pero, como todas utilizan un canal único, sólo una estación puede transmitir datos simultáneamente.

El tamaño del bloque de datos puede oscilar desde 72 hasta 1526 **bytes** (con un tamaño normal de 256 **bytes**).

Todas las estaciones tienen asignada una dirección de 48 **bytes** que permite que, cuando se cambia de lugar una estación, no haya posibilidad de conflictos y, por tanto, se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

TOKEN RING

Esta arquitectura de red fue creada por **IBM** en octubre de 1985 aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 **Kbps** para un máximo de 64 ordenadores y una red de banda ancha a 2 **Mbps** para un máximo de 72 ordenadores.

Emplea una topología de anillo con protocolo de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica.

Los datos se transmiten a una velocidad de 4 **Mbps** por segundo, pudiéndose conectar hasta un máximo de 8 ordenadores y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (**MAU**) si se utiliza con cable coaxial (si se utiliza con fibra óptica puede llegar hasta una velocidad de 16 **Mbps**).

No obstante, como se pueden conectar hasta 12 unidades de acceso multiestación (**MAU**), el número de ordenadores conectados y la distancia máxima pueden aumentar considerablemente.

ARCNET

Este tipo de arquitectura comenzó siendo un sistema de proceso distribuido de **Datapoint**, aunque fue potenciado en el mundo de los microordenadores por **Standard Microsystems**.

Es una red en banda base que utiliza una topología mixta estrella/bus con protocolo de paso de testigo.

Transmite a una velocidad de 2,5 **Mbps** y todos los ordenadores han de estar conectados a un concentrador (**HUB** activo). La distancia máxima entre el ordenador y el **HUB** activo no puede sobrepasar los 660 metros.

A cada **HUB** activo se le pueden conectar **HUB** pasivos (a cada **HUB** pasivo únicamente se le pueden conectar tres ordenadores con una distancia máxima entre el **HUB** pasivo y cada ordenador de 17 metros).

No obstante, se puede conectar más de un **HUB** activo (con una separación entre ellos de 660 metros), por lo que el número máximo de estaciones puede llegar a ser de 255.

ESTUDIO COMPARATIVO ENTRE LAS TRES ARQUITECTURAS

Se ha pretendido realizar un estudio comparativo, únicamente a efectos orientativos, entre los tres tipos de arquitecturas descritos anteriormente, suponiendo que las tres se instalan con cable coaxial.

En cada una de las filas de la tabla se ha hecho una valoración del 1 al 3 en función de las posibilidades de cada una de ellas, obteniéndose los siguientes resultados:

	ETHERNET	TOKEN RING	ARCNET
COSTE	1	3	2
VELOCIDAD	1	2	3
INSTALACIÓN	1	3	2
DISTANCIA	3	1	2
Nº ESTACIONES	1	3	2

Haciendo constar que el 1 corresponde a la máxima valoración y el 3 a la menor.

ıcterísticas	Ethernet Valor	Valores IEEE 802.3 10Base5	10Base2	10BaseT	10BaseFL	100BaseT
ı de datos ıps)	10	10	10	10	10	100
odo de ılización	Banda base	Banda base	Banda base	Banda base	Banda base	Banda base
ho amo de nento (m)	500	500	185	100	2,000	100
lios	50-ohm coaxial	50-ohm coaxial	50-ohm coaxial	Cable de par trenzado sin blindaje	Fibra óptica	Cable de par trenzado sin blindaje
ología	Bus	Bus	Bus	Estrella	Punto a punto	Bus

Tabla 7–1
Tabla comparativa de las diferentes especificaciones de la capa física del IEEE 802.3

CAPÍTULO 7

Tecnologías Ethernet

ANTECEDENTES

El término *Ethernet* se refiere a la familia de implementaciones de LAN que incluyen tres categorías principales:

- Ethernet e IEEE 802.3 — Son las especificaciones LAN que operan a 10 Mbps a través de cable coaxial.
- Ethernet a 100 Mbps — Es una sola especificación LAN, también conocida como Fast Ethernet, que opera a 100 Mbps a través de cable de par trenzado.
- Ethernet a 1000 Mbps — Es una sola especificación LAN, también conocida como Gigabit Ethernet, que opera a 1000 Mbps (1 Gbps) a través de cables de fibra óptica y de par trenzado.

Este capítulo analiza conceptos avanzados de cada una de las variantes tecnológicas.

La red Ethernet ha prevalecido como una tecnología de transmisión fundamental, gracias a su tremenda flexibilidad y a que es relativamente fácil de comprender e implementar. Aunque se han propuesto otras tecnologías como sus posibles reemplazos, los administradores de red prefieren la red Ethernet y sus tecnologías

derivadas como soluciones eficaces para un amplio rango de requerimientos de implementación en campus. Para resolver las limitaciones de Ethernet, los innovadores de redes (y las organizaciones encargadas de generar estándares), han creado, de manera continua, redes Ethernet de mayor cobertura. La crítica debiera dejar de pensar en Ethernet como una tecnología no escalable, puesto que el esquema de transmisión sobre el que se basa sigue siendo una de las formas principales de transporte de datos en aplicaciones modernas en campus. Este capítulo describe las diferentes tecnologías de Ethernet que se han desarrollado hasta nuestros días.

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 tráfico esporádico y ocasionalmente alto, y la especificación IEEE 802.3 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 10Base5. 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.

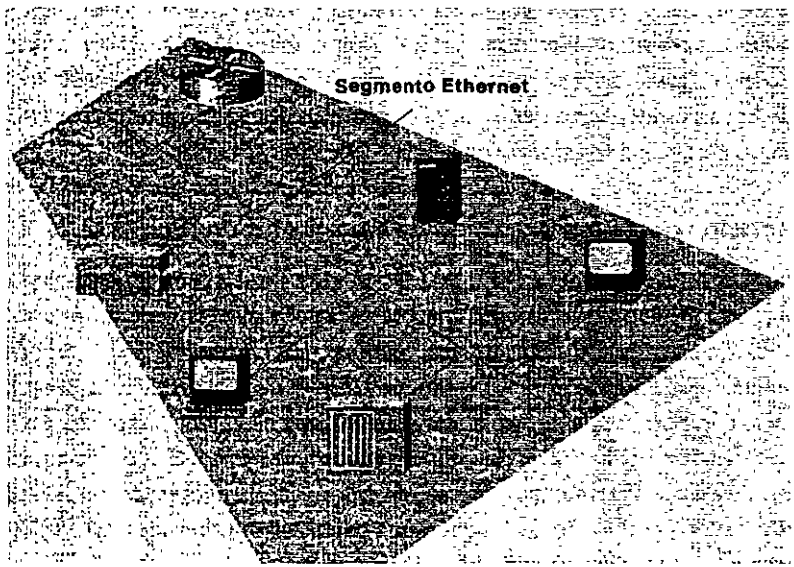


Figura 7–1
Una red Ethernet corre CSMA/CD a través de un cable coaxial.

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.

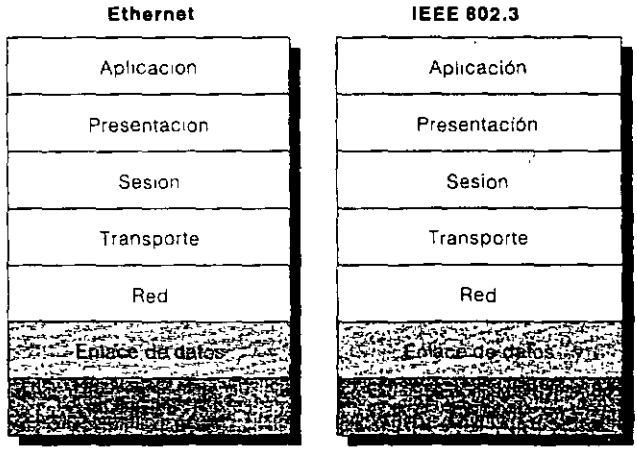


Figura 7-2 *Modelo de referencia OSI de Ethernet y del IEEE 802.3*

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.

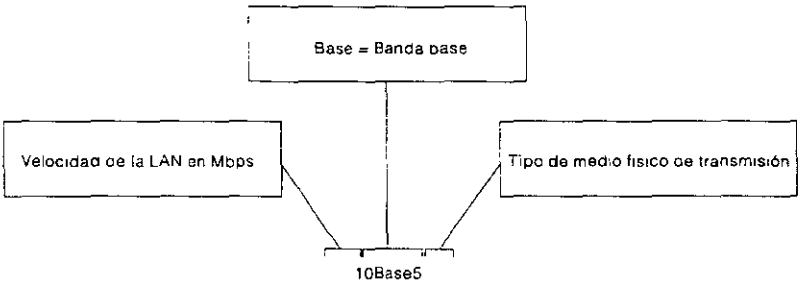


Figura 7–3
Los componentes del IEEE 802.3 se nombran de acuerdo con sus convenciones.

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.

	Ethernet	Valores IEEE 802.3				
Características	**Valor**	**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
Tabla comparativa de las diferentes especificaciones de la capa física del IEEE 802.3

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.

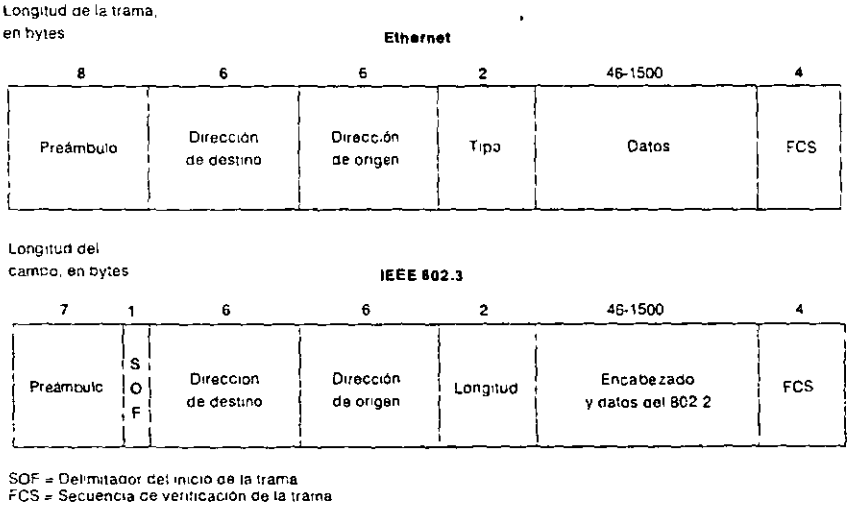


Figura 7–4 *Hay varios campos en las tramas de las especificaciones Ethernet e IEEE 802.3.*

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 informa 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 siguen 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 al menos 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 debe 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 emisor 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 banda 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 granjas 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: 100BaseT y 100VG-AnyLAN, respectivamente.

100BaseT es la especificación del IEEE para la implementación de Ethernet a 100 Mbps con UTP (Cableado de Par Trenzado Sin Blindaje) 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 Grupo 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 100BaseT

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 10 Mbps, 100 Mbps o ambas. La figura 7-5 muestra cómo la subcapa MAC 802.3 y las capas superiores operan con 100BaseT, sin necesidad de modificación alguna.

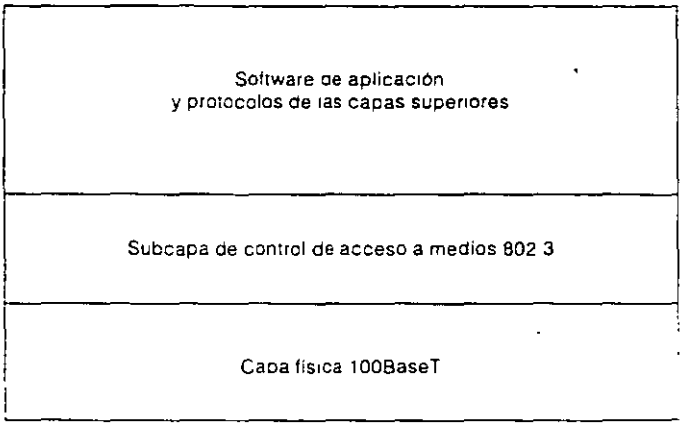


Figura 7–5
Los protocolos de las capas superiores y MAC 802.3 operan en 100BaseT.

Señalización 100BaseT

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.

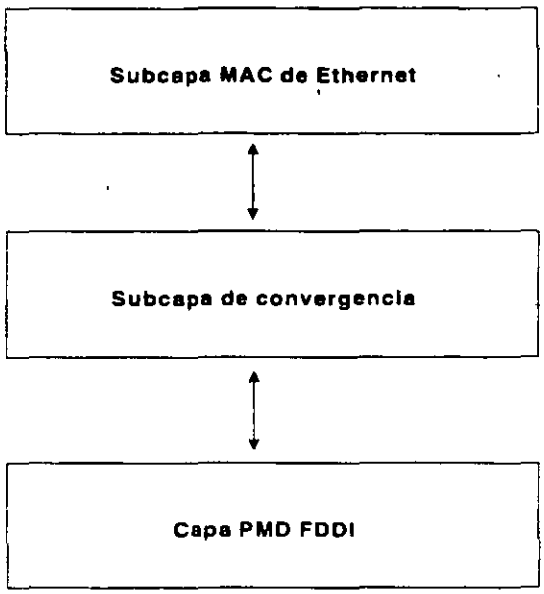


Figura 7–6
La subcapa de convergencia 100BaseX se pone en interfase con los dos esquemas de señalización.

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 100BaseT

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:
  - 100BaseTX
  - 100BaseFX
  - 100BaseT4

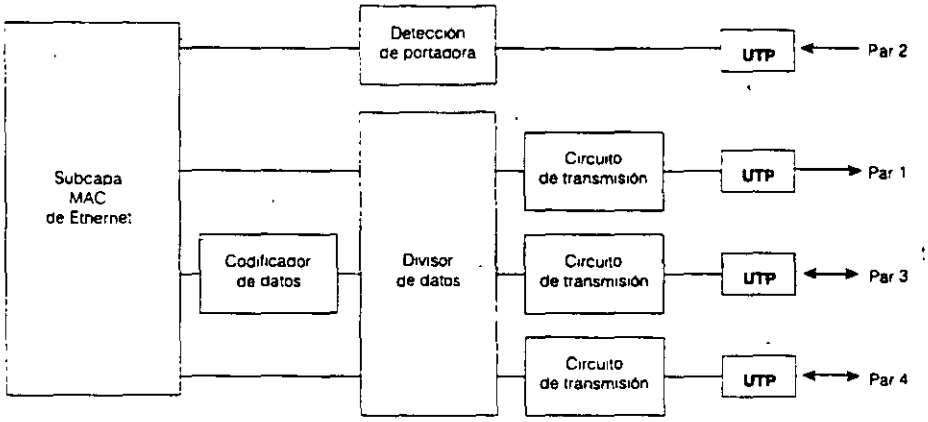


Figura 7–7
La señalización 4T+ requiere cuatro pares de UTP.

- *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 Ethernet 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.

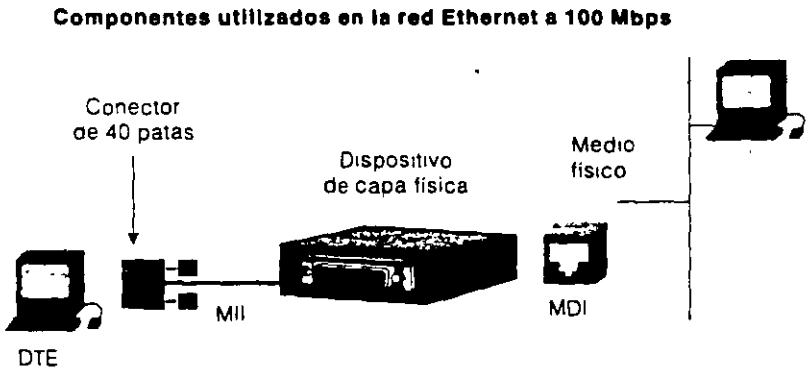


Figura 7–8
100BaseT requiere varios componentes de hardware.

Operación 100BaseT

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 10BaseT 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 10 veces 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 100BaseT

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 100BaseT

Las redes 100BaseT 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 100BaseT

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.

100BaseTX

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
En la capa física hay tres tipos de medios de transmisión para 100BaseT.

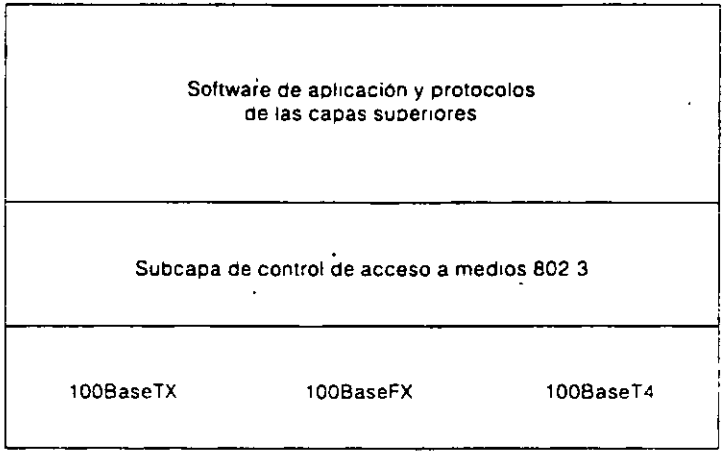


Tabla 7–2
Características de los tipos de medios de transmisión en 100BaseT

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

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.

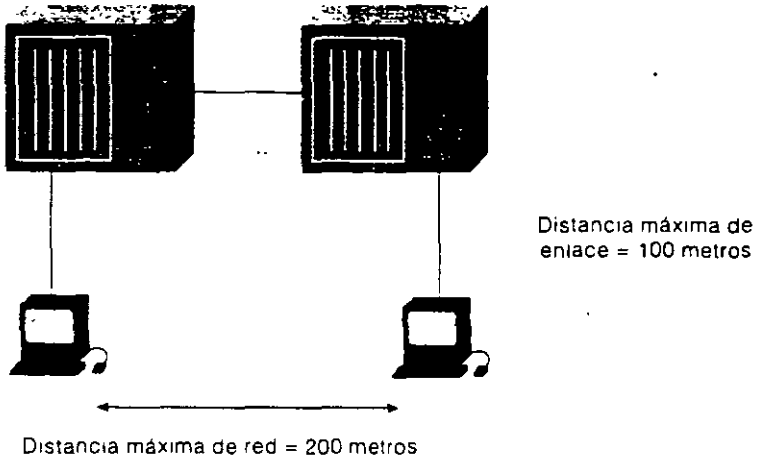


Figura 7–10
La red 100BaseTX está limitada a una distancia de enlace de 100 metros.

100BaseFX

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.

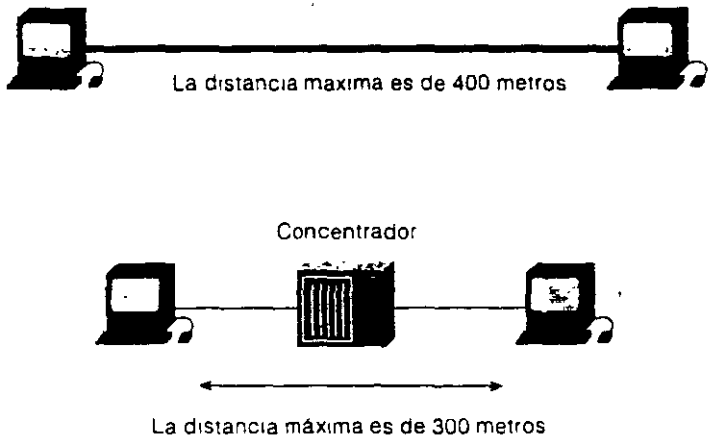


Figura 7-11
El límite entre DTE y DTE en 100BaseFX es de 400 metros.

100BaseT4

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.

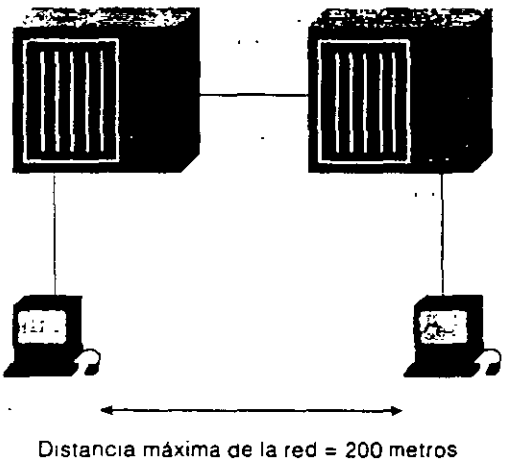


Figura 7–12
La tecnología 100BaseT4 soporta una distancia máxima de enlace de 100 metros.

100VG-AnyLAN

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

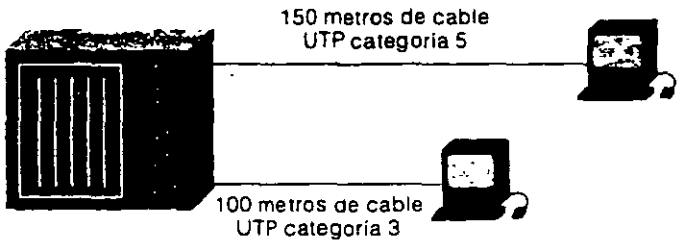


Figura 7–13
Las limitaciones en cuanto a la longitud del enlace en 100VG-AnyLAN difieren de las de los enlaces que utilizan UTP categorías 3 y 5.

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 (UTP categoría 5). La figura 7-14 muestra la configuración de concentradores en 100VG-AnyLAN.

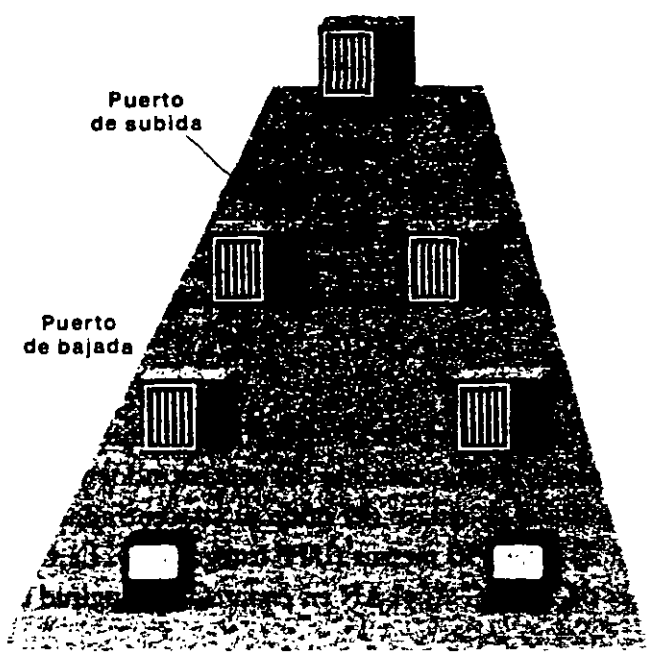


Figura 7–14
Los concentradores 100VG-AnyLAN están dispuestos jerárquicamente.

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.

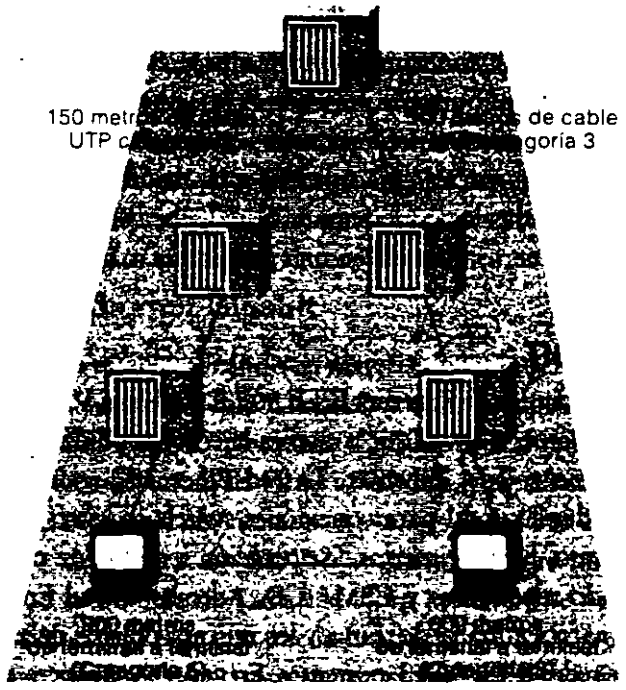


Figura 7–15
Las limitaciones de longitud de extremo a extremo difieren en las implementaciones 100VG-AnyLAN.

Operación de 100VG-AnyLAN

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/CD, 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 confirmar cada solicitud que se le presente. A las solicitudes de alta prioridad, como las aplicaciones de videoconferencia, que son sensibles al tiempo, se les da 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 dúplex total para conexiones switch a switch y switch a estación terminal. Asimismo, permite modos de operación semidúplex para conexiones compartidas utilizando repetidores y CSMA/CD. Además, la red Ethernet Gigabit utiliza el mismo formato y tamaño de trama y los mismos objetos de administración 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 Blindaje) 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, mismas que están dirigidas por el grupo de trabajo IEEE 802.3, y también contribuye 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 sigan este estándar utilizarán el formato de trama del IEEE 802.3/Ethernet, así como el método CSMA/CD 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/Fast 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 utilizarán componentes ópticos de Canal de Fibra a 780 nm (pequeña longitud de onda) de alta velocidad para efectuar la señalización a través de la 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 sea posible ofrecer una velocidad total de transmisión de datos 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 silicio y el procesamiento 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.

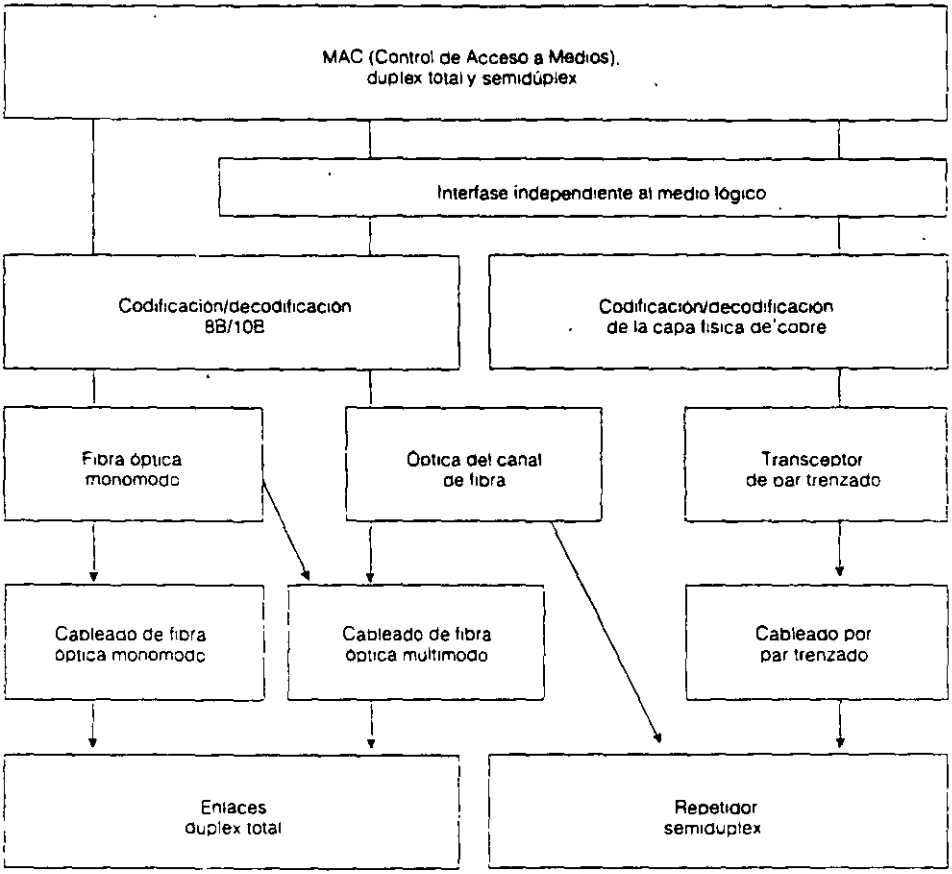


Figura 7–16 *Elementos funcionales de la red Ethernet Gigabit.*

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 ello 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 conectaran 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 12

COMUNICACIÓN CON EL EXTERIOR

Cuando se está trabajando en una red local, puede ser necesaria determinada información que procede del exterior de la red.

Estos datos pueden proceder de otro ordenador, de otra red o de un **mainframe**/miniordenador y, por tanto, antes de proceder a establecer conexión con ellos, se han de resolver los problemas que existen en las comunicaciones (direccionamiento, control de errores, método de transmisión, formato, etc).

Dentro de los equipos necesarios para realizar la transmisión de datos con el exterior de la red, se encuentran:

- Un repetidor, si se necesita regenerar la señal entre dos segmentos de red que se interconectan.
- Un módem, si se va a acceder a un microordenador independiente o a otro sistema que está lejos y no se accede a él de forma periódica.
- Un puente (**bridge**) para conectar dos redes.
- Un encaminador (**router**) que dirige el paquete de datos determinando la ruta hacia su destino.
- Una pasarela (**gateway**) para e .blecer un enlace con un miniordenador o con un **mainframe**.

Todos ellos han de estar situados en un servidor de archivos o, si la red tiene una gran demanda de comunicación con el exterior, en un servidor de comunicaciones para que puedan ser utilizados por todas las estaciones de la red local.

REPETIDOR

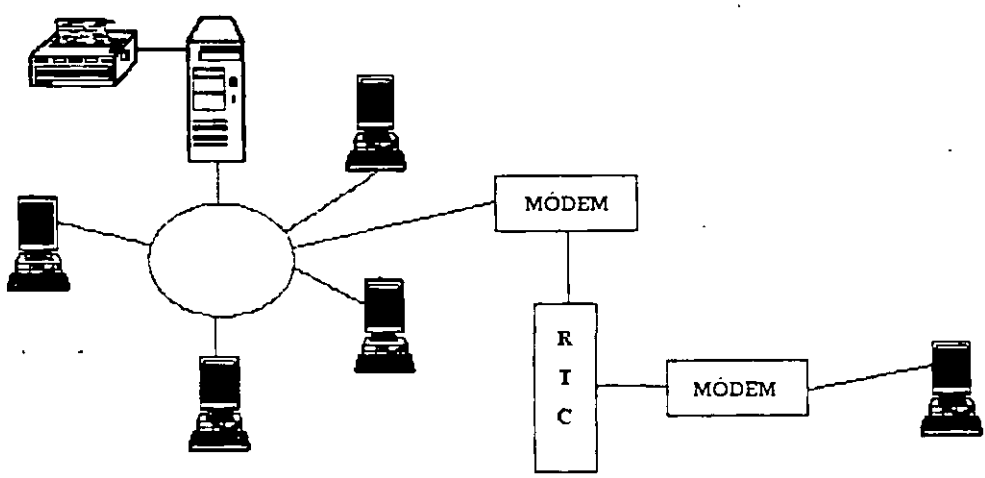
Un repetidor es un dispositivo encargado de regenerar la señal entre los dos segmentos de una red homogénea que se interconectan ampliando su cobertura. Operan en el nivel físico del modelo de referencia **OSI**.

Su forma de actuar es la siguiente: recogen la señal que circula por la red y la reenvían por la misma red o por otra distinta sin efectuar ningún tipo de interpretación de dicha señal.

Son capaces de conectar diferentes medios físicos de transmisión. Sin embargo, no suelen utilizarse para conectar redes de banda base con redes de banda ancha, ya que los métodos de decodificación de la información son muy diferentes.

MÓDEM

La función básica que desarrolla un módem es aceptar datos de un ordenador y convertir las señales digitales en señales analógicas para que se transmitan a través de la línea telefónica.



Representación esquemática de una estación unida a la red con un módem a través de la red telefónica conmutada (RTC)

Cuando los datos llegan al punto de destino, el módem receptor realiza la función inversa, es decir, vuelve a transformar las señales analógicas en señales digitales para que el ordenador las pueda entender.

Es importante destacar que es importante para la velocidad del proceso que el módem cuente con una velocidad alta, ya que cuanto mayor sea la velocidad menor será el tiempo que invierte en el proceso (como ejemplo, un módem a 2.400 **bps** tarda en transmitir los datos una duración 8 veces menor que uno de 300 **bps**).

De todas formas, si se transmite por la red telefónica conmutada (**RTC**), la velocidad máxima que se puede conseguir actualmente es de, aproximadamente, 9.600 **bps** sin técnicas de compresión y un bit detrás de otro (con técnicas avanzadas de compresión pueden sobrepasarse los 115.000 bps); por tanto, si se desean conseguir velocidades mayores es necesario disponer de líneas dedicadas.

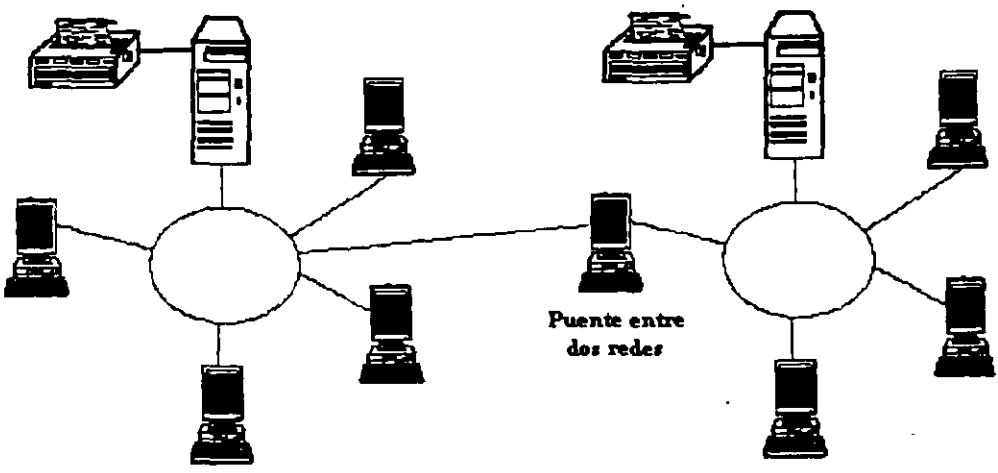
Entre sus características más importantes está la de poseer listín telefónico donde almacena los números de teléfono que puede marcarlos automáticamente en el momento o bien en una fecha y hora programada. En el caso de estar la línea ocupada, vuelven a intentar la llamada al cabo de un tiempo preestablecido.

También cuentan con respuesta automática a una llamada y la posibilidad de que se devuelva la llamada una vez comprobado que el emisor está autorizado para solicitarlo.

Su mayor utilidad para la expansión de una red es para el acceso remoto de una estación de trabajo móvil.

PUENTE (BRIDGE)

Cuando dos redes locales necesitan comunicarse entre sí, necesitan contar con un puente en cada una de ellas para poder conectarse.



Representación esquemática de dos redes unidas por un puente

Ambas redes han de usar el mismo protocolo de comunicaciones.

A diferencia de un repetidor, un puente actúa sobre los paquetes de datos o tramas que se transfieren en los niveles de enlace de datos, particularmente sobre el nivel de Control de Acceso al Medio (**MAC**).

Sus funciones básicas son las de autoaprendizaje, filtrado y reenvío. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no está incluida en su tabla de destinos, examina los campos de dirección del paquete (filtrado) y las dirige a la dirección que ha localizado (reenvío). A continuación, la añade a su tabla de destinos (autoaprendizaje).

La utilización de puentes para unir redes es una idea mejor que la configuración de una red grande que englobe a las dos. La razón está en que las redes van perdiendo rendimiento al aumentar el tráfico y se va perdiendo tiempo de respuesta, de este modo, al estar dividida la red se reduce el tráfico y el tiempo de respuesta.

Otra razón es el límite de expansión de la red grande. Todas las redes cuentan con un número máximo de estaciones que pueden soportar, si se desea sobrepasar ese número la única alternativa pasa por crear otra red conectada por un puente.

ENCAMINADOR (ROUTER)

Un encaminador no sólo incorpora la función de filtrado característica de los puentes sino que, además, determina la ruta hacia su destino. Se utiliza tanto en redes de área local como en redes de área extensa.

Los encaminadores se diferencian de los puentes en dos aspectos:

- Actúa sobre los paquetes transferidos entre los niveles de red de las estaciones, a diferencia de los puentes que lo hacen sobre el nivel de enlace de datos.

- Ambos equipos son, teóricamente, transparentes a las estaciones finales que comunican, sin embargo, normalmente las estaciones tienen definido el encaminador al que deben dirigirse.

Se basan en la utilización de un esquema de direccionamiento jerárquico (tablas de rutas) que distinguen entre la dirección del dispositivo dentro de la red y la dirección de la red. Para ello, incorporan protocolos de nivel de red.

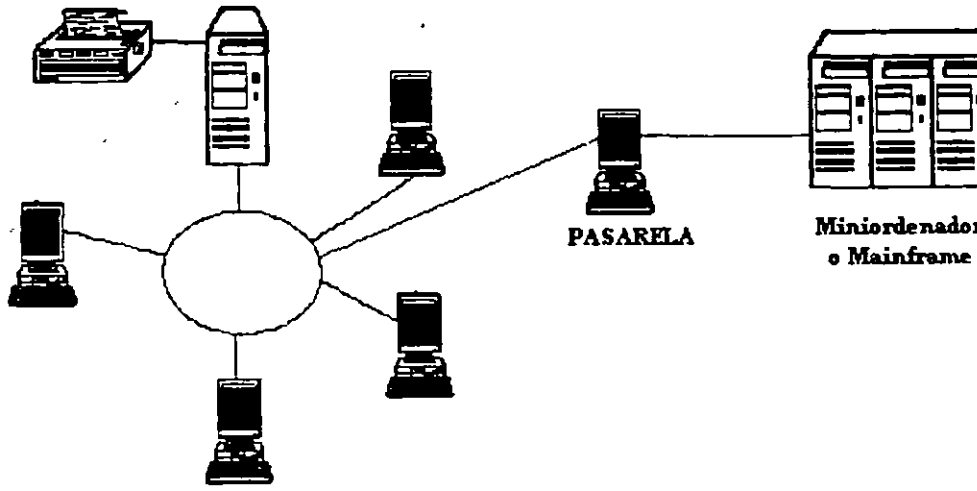
Para realizar su función, incorporan algún tipo de algoritmo, siendo uno de los más básicos el **Protocolo de Información de Encaminamiento (RIP)** que calcula la distancia entre el encaminador y la estación receptora de un paquete como el número de saltos requeridos, ignorando otros tipos de atributos como el tiempo de transferencia entre dos saltos, etc.

Los protocolos de encaminamiento varían en función de las diferentes arquitecturas de comunicaciones de red existentes, por lo que se diseñan para una arquitectura específica.

Existen algunos dispositivos que poseen características tanto de los puentes (transparencia a los protocolos con aprendizaje) como de los encaminadores (selección del camino óptimo) y que se denominan **brouters** (es la unión de **bridges** y **routers**). Este dispositivo funciona normalmente como un encaminador siempre que los protocolos de nivel superior permitan el encaminamiento. En caso contrario funcionan como puentes.

PASARELA (GATEWAY)

Cuando tenga que comunicar una red local y un gran ordenador (**mainframe**) o un miniordenador (porque utilizan protocolos de nivel de transporte, sesión, presentación y aplicación distintos), necesitará una pasarela.



Representación esquemática de una red unida a un miniordenador o a un mainframe

De este modo podrá obtener datos del mini o del **mainframe** o enviarles datos para su almacenamiento.

La pasarela realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.

El enlace entre ambos protocolos necesitará algún tipo de emulación que haga que la estación de trabajo imite el funcionamiento de un terminal y ceda el control al mini o al **mainframe**. Esta emulación se puede conseguir por medio de **software** (con un programa), de **hardware** (con una tarjeta) o de ambos.

Al igual que los encaminadores, están definidos para un determinado escenario de comunicaciones.

Pero a cambio de sus ventajas, el retardo de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en los otros dispositivos.

Los repetidores, concentradores y extendedores de las LANs se estudian brevemente en esta sección. La función y operación de puentes, switches y ruteadores se analizan de manera general en el capítulo 4 "Fundamentos del puenteo y la conmutación" y en el capítulo 5 "Fundamentos del ruteo".

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.

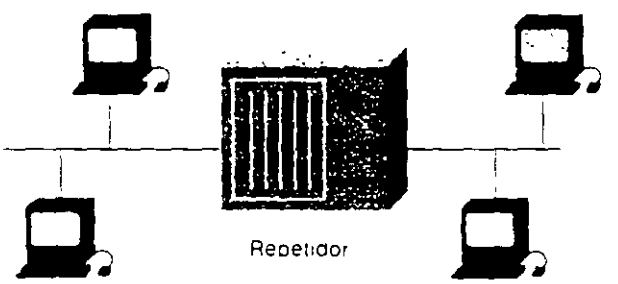


Figura 2–6
Un repetidor conecta dos segmentos de red.

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.

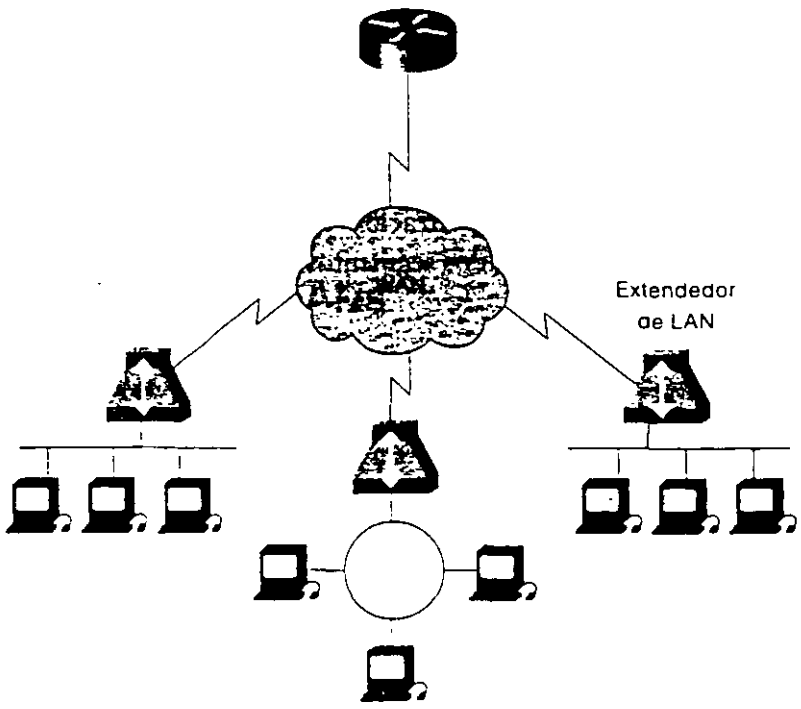


Figura 2–7
Varios extendedores de LAN se pueden conectar al ruteador host por medio de una WAN.

FUNDAMENTOS DE MULTIPLEXAJE

El multiplexaje es un proceso en el que varios canales de datos se combinan en un solo canal físico de datos en el origen. El multiplexaje se puede implementar en cualquiera de las capas de OSI. Por el contrario, el demultiplexaje es el proceso de separar en el destino los canales de datos multiplexados. Un ejemplo de multiplexaje es cuando los datos de varias aplicaciones se multiplexan en un solo paquete de datos de las capas inferiores.

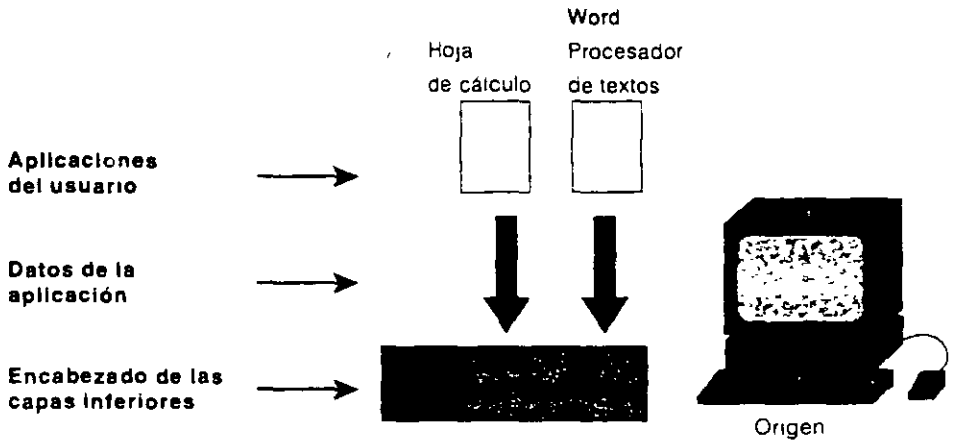


Figura 1–18
En un solo paquete de datos de las capas inferiores se pueden multiplexar varias aplicaciones

Otro ejemplo de multiplexaje es cuando se combinan los datos de varios dispositivos en un solo canal físico (por medio de un dispositivo llamado multiplexor). La figura 1-19 muestra dicho ejemplo.

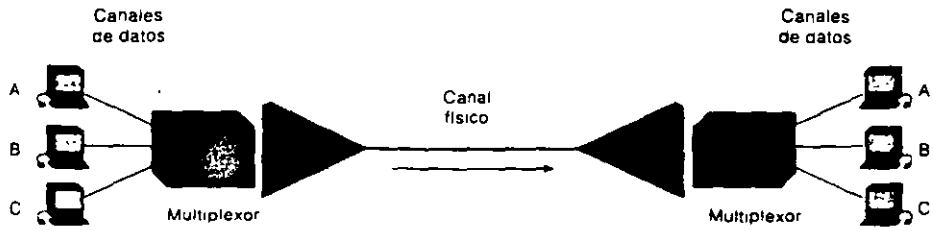


Figura 1-19
En un solo canal físico se pueden multiplexar varios dispositivos.

Un multiplexor es un dispositivo de la capa física que combina múltiples ráfagas de datos en uno o más canales de salida en el origen. Los multiplexores, demultiplexan los canales en varias ráfagas de datos en el extremo remoto y, por lo tanto, maximizan el uso del ancho de banda del medio físico y permiten que éste sea compartido por varias fuentes de tráfico.

Algunos métodos que se utilizan para multiplexar datos son TDM (Multiplexaje por División de Tiempo), ATDM (Multiplexaje Asíncrono por División de Tiempo), FDM (Multiplexaje por División de Frecuencia) y el multiplexaje estadístico.

En TDM, se asigna ancho de banda a la información de cada canal de datos con base en ranuras de tiempo preasignadas, sin tomar en cuenta si hay datos para enviar o no. En ATDM, se asigna ancho de banda a la información de los canales de datos, a medida que éstos la necesiten, a través de ranuras de tiempo asignadas de manera dinámica. En FDM, se asigna ancho de banda a la información de cada canal de datos con base en la frecuencia de la señal del tráfico. En el multiplexaje estadístico, se asigna ancho de banda de manera dinámica a cualquier canal de datos que tenga información para transmitir.

CAPÍTULO 4

Fundamentos del puenteo y la conmutación

Este capítulo presenta las tecnologías que se utilizan en los dispositivos conocidos como *puentes* y *switches*. Entre los temas propuestos se estudian las operaciones generales a nivel capa de enlace de datos de los dispositivos, el puenteo local y remoto, la conmutación de ATM y la conmutación LAN. Más adelante, en los capítulos de la parte 4, "Puenteo y conmutación" se estudian en más detalle las tecnologías específicas.

¿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 combinados 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 capas 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 AppleTalk, DECnet, TCP/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 una 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 de 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 Mbps pueden conectarse por medio de un switch. Asimismo, los switches pueden soportar una densidad mayor de puertos que los puentes. Algunos 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.

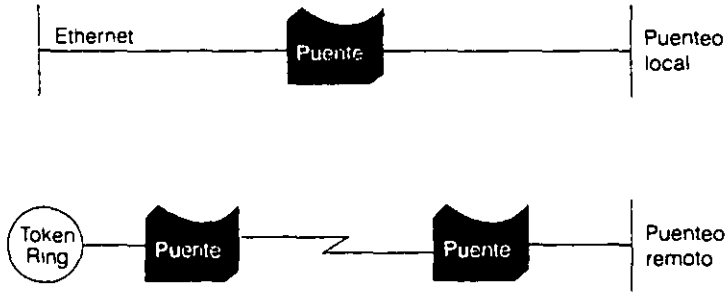


Figura 4–1
Los puentes locales y remotos conectan segmentos de LAN en áreas específicas.

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 las WAN. Las diferencias significativas en cuanto a velocidad de las 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 almacenán-

dose 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 presenten 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 de 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 802.3), en tanto que otros pueden traducir entre los diferentes protocolos de la capa de enlace de datos (por ejemplo, IEEE 802.3 e IEEE 802.5). 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 802.5 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.

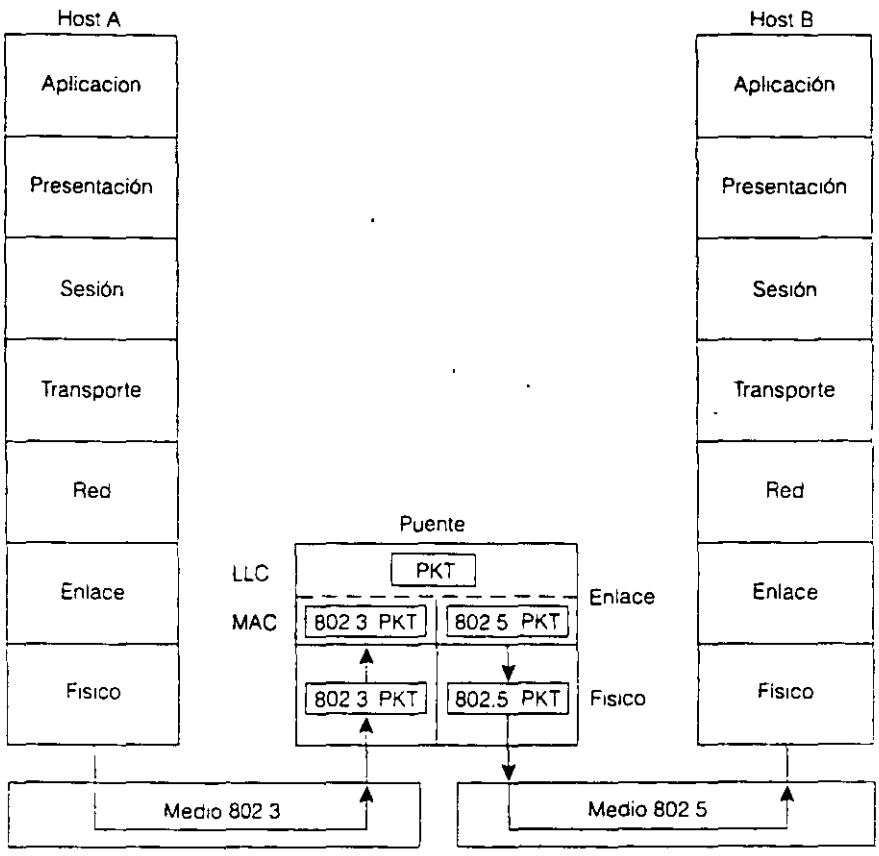


Figura 4–2
Un puente de la capa MAC conecta las redes IEEE 802.3 e IEEE 802.5.

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.

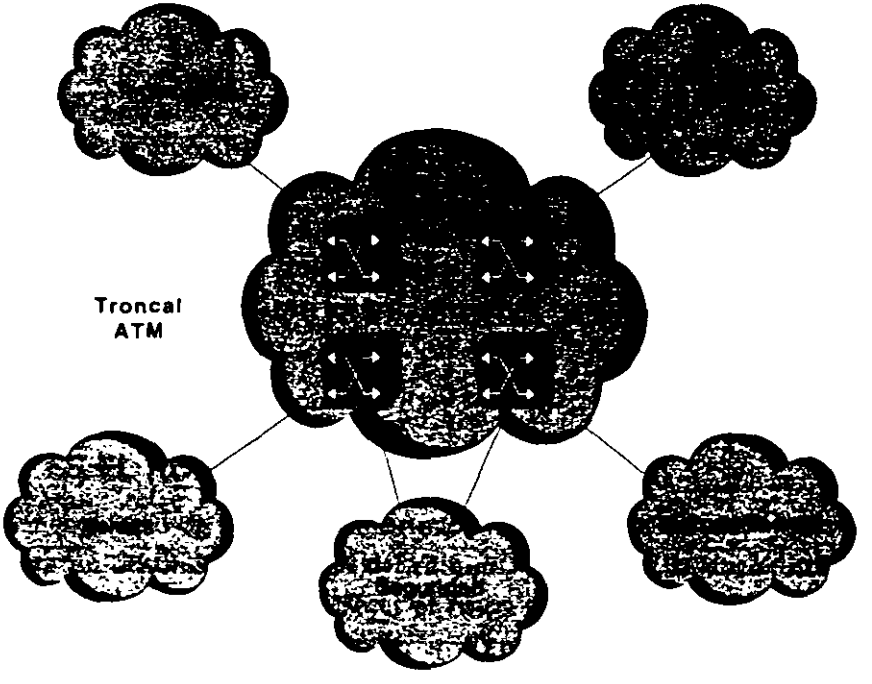


Figura 4–3
Las redes múltiples LAN pueden utilizar una troncal basada en ATM para la conmutación de celdas.

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

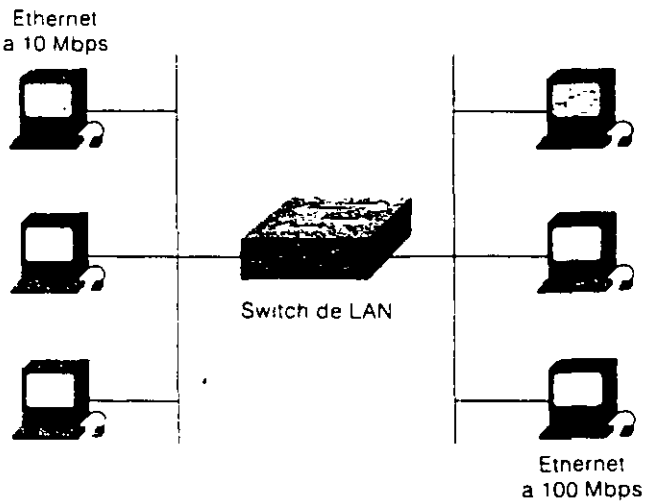


Figura 4–4
Un switch LAN puede enlazar segmentos de redes Ethernet a 10 Mbps y a 100 Mbps.

CAPÍTULO 5

Fundamentos del ruteo

Este capítulo presenta los conceptos básicos que se utilizan ampliamente en los protocolos de ruteo. Entre los temas que se presentan a continuación están los componentes y algoritmos de los protocolos de ruteo. Además, el papel de los protocolos de ruteo se compara brevemente con los protocolos ruteados o de red. Los capítulos de la parte 6 "Protocolos de ruteo" de este libro, se ocupan con mayor detalle de los protocolos de ruteo específico, en tanto que los protocolos de red que utilizan los protocolos de ruteo se analizan en la parte 5, "Protocolos de red".

¿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; ambas 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 ruteo 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 ruteo 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 asociaciones de salto destino/próximo determinan la trayectoria óptima de los datos.

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. En este capítulo se presentarán y describirán muchos parámetros diferentes de uso común en el ruteo.

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 la 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 el 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.

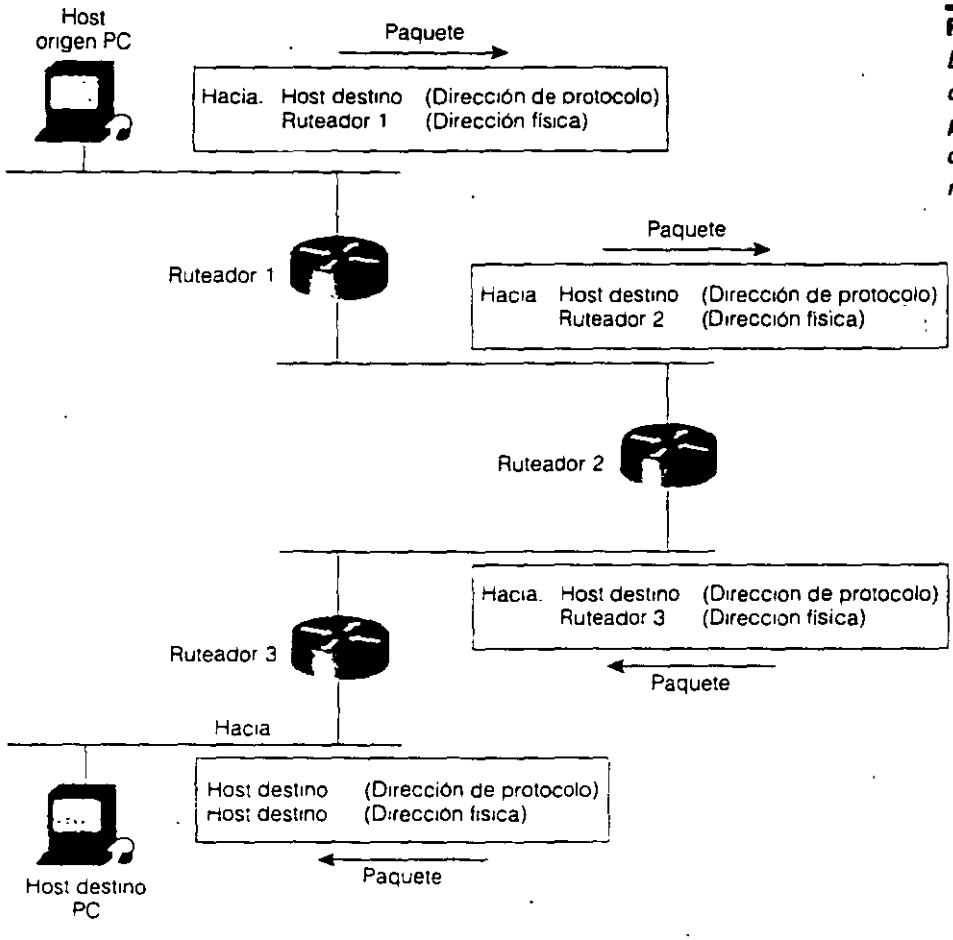


Figura 5–2
En el proceso de conmutación puede participar una gran cantidad de ruteadores.

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 las secciones siguientes se estudian estos atributos de los algoritmos de ruteo.

9

Modelo de interacción cliente-servidor

9.1 Introducción

n los primeros capítulos presentamos los detalles de la tecnología TCP/IP, incluyendo los proto-los que proporcionan los servicios básicos y la arquitectura de ruteo que provee la información cesaria de ruteo. Ahora que comprendemos la tecnología básica, podemos examinar los progra-as de aplicación que se aprovechan del uso cooperativo de una red de redes de TCP. Las aplica-ones de ejemplo son prácticas e interesantes pero no hacen el énfasis principal. De hecho, el foque descansa sobre los patrones de interacción de los programas de aplicación de comunica-ón. El patrón de interacción primario que se da entre las aplicaciones de cooperación se conoce mo paradigma *cliente-servidor*. La interacción cliente-servidor forma la base de la mayor parte la comunicación por redes y es fundamental ya que nos ayuda a comprender las bases sobre las e están construidos los algoritmos distribuidos. En este capítulo, se considera la relación entre ente y servidor; en capítulos posteriores se ilustra el patrón cliente-servidor con más ejemplos.

9.2 Modelo cliente servidor

término *servidor* se aplica a cualquier programa que ofrece un servicio que se puede obtener en a red. Un servidor acepta la petición desde la red, realiza el servicio y devuelve el resultado al icitante. En el caso de los servicios más sencillos, cada petición llega en un solo datagrama IP y servidor devuelve una respuesta en otro datagrama.

Un programa ejecutable se convierte en un *cliente* cuando manda una petición a un servi y espera una respuesta. Debido a que el modelo cliente-servidor es de extensión conveniente y tural en la comunicación de interproceso en una sola máquina, es fácil construir programas que licen el modelo para interactuar.

Los servidores pueden ejecutar tareas simples o complejas. Por ejemplo, un *servidor hora día* simplemente devuelve la hora actual cuando un cliente manda un paquete al servidor. Un *ser dor de archivo* recibe las peticiones para realizar las operaciones de almacenaje o recuperacion datos de un archivo; el servidor realiza la operación y devuelve el resultado.

Los servidores se suelen implantar como aplicaciones de programas.[1] La ventaja de impl tar los servidores como programas de aplicación es que pueden ejecutarse en cualquier sist computacional que soporte la comunicación TCP/IP. De este modo, el servidor de un servicio particular puede ejecutarse en un sistema de tiempo compartido junto con otros programas o en computadora personal. Los servidores múltiples pueden ofrecer el mismo servicio y ejecutarse la misma máquina o en múltiples máquinas. De hecho, los administradores comúnmente duplic copias de un servidor dado en máquinas físicamente independientes para incrementar la disponib lidad o mejorar la ejecución. Si el propósito principal de una computadora es apoyar un progra servidor en particular, el término "servidor" se puede aplicar tanto a la computadora como al pr grama servidor. De este modo, podemos escuchar frases como "la máquina A es nuestro servi de archivos".

19.3 Un ejemplo simple: servidor de eco UDP

La manera más simple de interacción cliente-servidor se vale de un datagrama de entrega no co fiable para transportar los mensajes de un cliente a un servidor y de regreso. Consideremos, p ejemplo un *servidor de eco UDP*. Como se muestra en la figura 19.1, el aspecto mecánico es dire to En el lugar del servidor comienza un *proceso de servidor de eco* UDP mediante la negociació con su sistema operativo, de la obtención del permiso para utilizar la ID de puerto UDP reserv para el servicio de *eco*, el *puerto de eco* UDP. Una vez que se ha obtenido el permiso, el proce de servidor de eco entra en un ciclo interminable que incluye tres pasos: (a) espera a que el da grama llegue al puerto de eco, (b) se invierten las direcciones de fuente y destino[2] (incluyendo t to las direcciones de IP de fuente y destino como las identificaciones de UDP), y (c) se devuelve datagrama al emisor original En algún otro lugar, un programa se convierte en un UDP *eco-clie* cuando ubica un puerto de protocolo UDP no utilizado, manda un mensaje UDP al UDP eco-serv dor y espera la respuesta. El cliente espera recibir exactamente los mismos datos que mandó

En el servicio de eco de UDP se ilustran dos puntos importantes acerca de la interacci cliente-servidor que por lo general son ciertos El primero se refiere a la diferencia entre el tiem de vida de los servidores y los clientes

> *Un servidor comienza la ejecución antes de que empiece la interacción y (usualmente) continúa aceptando las peticiones y mandando las respuestas sin termi-*

---

[1] Muchos de los sistemas operativos se refieren a programas de aplicacion que estan corriendo como a un *proces* a un *proceso de usuario*

[2] En uno de los ejercicios sugeridos se considera este paso con mayor detalle

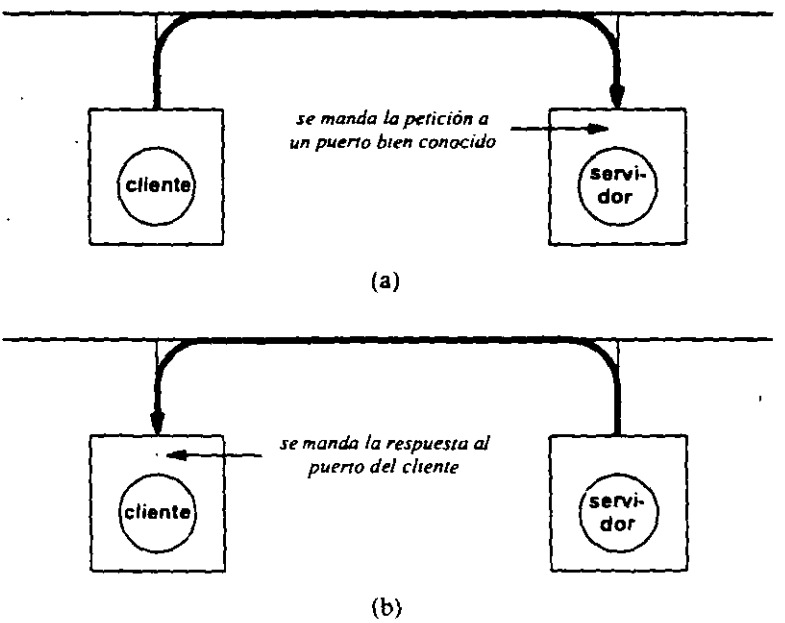


Figura 19.1 Eco UDP como ejemplo del modelo cliente-servidor. En el inciso (a) el cliente manda una petición al servidor a una dirección IP conocida y al puerto bien conocido UDP, y en el inciso (b) el servidor devuelve una respuesta. Los clientes utilizan cualquier puerto UDP que esté disponible.

nar nunca. Un cliente es cualquier programa que hace una petición, por lo general espera una respuesta y termina después de que ha utilizado un servidor un número finito de veces.

El segundo punto, mucho mas técnico, se ocupa del uso de los identificadores de puerto reservados y no reservados.

Un servidor espera las peticiones en un puerto bien conocido que ha sido reservado para el servicio que ofrece. Un cliente ubica un puerto arbitrario no utilizado y no reservado para su comunicación.

En una interacción cliente-servidor se necesita reservar sólo uno de los dos puertos. Asignando un identificador único de puerto para cada servicio, se facilita la construcción de clientes y servidores.

¿Quién podrá utilizar un servicio eco? No todos los clientes promedio están interesados en el servicio. Sin embargo, los programadores que diseñan, implantan, miden o modifican el software de protocolo de la red o los gerentes de red que prueban las rutas y depuran los problemas de comunicación, a menudo, utilizan los servicios de eco en sus pruebas. Por ejemplo, un servicio de eco puede también emplearse para determinar si es posible conectarse con una máquina remota.

19.4 Servicio de fecha y hora

El servidor eco es muy sencillo y se requiere muy poca codificación para implantar ya sea el lado del servidor o el del cliente (siempre que el sistema operativo ofrezca una manera razonable de acceder a los protocolos UDP/IP implícitos). Nuestro segundo ejemplo, que es un servidor de hora, muestra que aun una sencilla interacción cliente-servidor puede proporcionar servicios útiles. El problema que un servidor de hora resuelve es el de definir el reloj de hora del día de una computadora. El reloj de hora del día es un dispositivo de hardware que mantiene la fecha y hora actuales, poniéndolos a disposición de los programas. Una vez que se ha definido, el reloj mantiene dicha hora del día tan precisa como un reloj de pulso.

Muchos sistemas resuelven el problema pidiéndole al programador que introduzca la hora y la fecha cuando se inicia el sistema. El sistema incrementa el reloj de manera periódica (es decir, cada segundo). Cuando un programa de aplicación pregunta por la fecha o la hora, el sistema consulta su reloj interno y da un formato a la hora del día en forma legible para cualquier persona. Podemos utilizar una interacción cliente-servidor para definir el sistema de reloj automáticamente cuando se inicia la máquina. Para hacerlo, el administrador configura una máquina que suele ser la máquina con el reloj de mayor exactitud, a fin de correr un servidor de hora del día. Cuando otras máquinas arrancan, se ponen en contacto con el servidor para obtener la hora actual.

19.4.1 Representación de la fecha y la hora

¿Cómo se supone que deberá mantener un sistema operativo la fecha y la hora del día? Una representación útil almacena la hora y la fecha como un conteo de segundos a partir de una fecha de época. Por ejemplo, el sistema operativo de UNIX utiliza el segundo cero del primero de enero de 1970 como su fecha de época. Los protocolos del TCP/IP también definen un fecha de época y reportan las horas conforme los segundos pasan la época. Para el TCP/IP, la época se define como el segundo cero del primero de enero de 1900 y la hora se mantiene en un entero de 32 bits, representación que se adaptará a todas las fechas de un futuro cercano.

Se mantiene a la fecha como a la hora en segundos pues la época hace que la representación se comparta y permite que se compare fácilmente. Enlaza a la fecha con la hora del día y hace posible que se mida el tiempo incrementando un simple entero binario

19.4.2 Hora local y universal

Ya que se ha dado una fecha de época y una representación para la hora, ¿a la hora de qué zona se refiere el conteo? Cuando dos sistemas se comunican a través de grandes distancias geográficas, utilizar la zona de la hora local para una u otra se vuelve difícil; deben acordar una zona de hora estándar para mantener los valores de fecha y hora comparables. De este modo, además de definir una representación para la fecha y elegir una época, el servidor de tiempo TCP/IP estándar especifica que todos los valores se dan con respecto a una sola zona de tiempo. Originalmente se le llamaba tiempo medio de Greenwich, la zona de tiempo ahora se conoce como *tiempo coordinado universal* o *tiempo universal*

La interacción entre un cliente y un servidor que ofrece servicio de tiempo funciona de manera muy parecida a un servidor eco. Del lado del servidor, la aplicación obtiene permiso para utilizar el puerto reservado asignado a los servidores de tiempo, espera el mensaje UDP dirigido a ese puerto y responde con un mensaje UDP que contiene la hora actual en un entero de 32 bits. Podemos resumir que:

El envío de un datagrama a un servidor de tiempo es equivalente a pedir la hora actual; el servidor responde con un mensaje UDP que contiene la hora actual.

19.5 La complejidad de los servidores

En nuestros ejemplos, los servidores son bastante sencillos debido a que son secuenciales. Esto quiere decir que el servidor procesa una petición a la vez. Después de aceptar una petición, el servidor forma una respuesta y la manda antes de volver a ver si ha llegado otra petición. Implícitamente asumimos que el sistema operativo hará una cola de peticiones que lleguen para un servidor mientras esté ocupado, y que dicha cola no será demasiado larga porque el servidor tiene sólo una pequeña cantidad de trabajo que realizar.

En la práctica, los servidores suelen ser mucho más difíciles de construir que los clientes, ya que necesitan acomodar varias peticiones concurrentes, aun cuando una sola petición se lleve una cantidad de tiempo considerable para ser procesada. Por ejemplo, consideremos que un servidor de transferencia de archivos es el responsable de copiar un archivo a otra máquina bajo pedido. En general, los servidores tiene dos partes. Un programa maestro sencillo, responsable de aceptar nuevas peticiones, y un conjunto de esclavos, los responsables de manejar las peticiones individuales. El servidor maestro ejecuta los cinco pasos siguientes:

Abrir puerto
: El servidor maestro abre el puerto bien conocido al que se puede accesar.

En espera del cliente
: El maestro espera a que un nuevo cliente mande una petición.

Elección de puerto
: Si es necesario, el maestro ubica un nuevo puerto de protocolo local para esta petición e informa al cliente (veremos más adelante que este paso es innecesario con el TCP/IP).

Se inicia el esclavo
: El maestro inicia un esclavo independiente y concurrente para que maneje esta petición (por ejemplo, en UNIX, se realiza una copia del proceso del servidor) Nótese que el esclavo maneja una petición y después termina, el esclavo no espera a que lleguen peticiones de otros clientes.

Continua
: El maestro regresa al paso de *espera* y continúa aceptando nuevas peticiones mientras el esclavo recientemente creado maneja de manera concurrente las peticiones previas

Como el maestro inicia un esclavo para cada nueva petición el procesamiento procede de manera concurrente. De este modo, las peticiones que requieren de poco tiempo para completarse pueden terminar antes que las peticiones que se llevan más tiempo, independientemente del orden en que se hayan comenzado. Por ejemplo, supongamos que el primer cliente que contacta a un servidor de archivos pide la transferencia de un archivo grande que se llevará varios minutos. Si un segundo cliente se pone en contacto con el servidor para pedir una transferencia que se lleva solamente unos segundos, la segunda transferencia puede iniciarse y completarse mientras que la primera transferencia aún continúa.

Además de la complejidad que resulta de que los servidores manejen peticiones concurrentes, la complejidad también surge porque los servidores deben reforzar las reglas de autorización y protección. Los programas servidor suelen requerir una ejecución de alta prioridad pues tienen que leer archivos del sistema, mantenerse en línea y tener acceso a datos protegidos. El sistema operativo no restringirá un programa servidor si intenta tener acceso a los archivos del usuario. De este modo, los servidores no pueden cumplir a ciegas las peticiones de otras localidades. Por el contrario, cada servidor toma la responsabilidad para reforzar el acceso al sistema y las políticas de protección.

Por último, los servidores deben protegerse a sí mismos contra las peticiones formadas equivocadamente o contra las peticiones que causarán que el mismo programa servidor se aborte. A menudo, es difícil prever los problemas potenciales. Por ejemplo, en un proyecto, en la Universidad de Purdue, se diseñó un servidor de archivos que permitió que los sistemas operativos de los estudiantes accesaran archivos en un sistema UNIX de tiempo compartido. Los estudiantes descubrieron que la petición al servidor de que abriera un archivo llamado */dev/tty* ocasionaba que el servidor abortara el proceso pues UNIX asocia ese nombre con la terminal de control a la que está unida un programa. El servidor que fue creado por una iniciación de sistema no tenía dicha terminal. Una vez que se abortaba el proceso, ningún cliente podía accesar archivos hasta que un programador de sistemas reiniciaba el servidor.

Hubo casos más serios de la vulnerabilidad del servidor en el verano de 1988, cuando un estudiante de la Universidad Cornell diseñó un programa *gusano* que atacó a las computadoras en toda la red Internet. Una vez que el gusano comenzó a correr en una máquina, buscó el acceso a Internet para llegar a computadoras con servidores que sabía cómo explotar y usó a los servidores para crear más copias de sí mismo. En uno de los ataques, el gusano aprovechó un bug[3] en el servidor *fingerd* de UNIX. Debido a que el servidor no revisó las peticiones que entraban, el gusano fue capaz de mandar una cadena de entrada ilegal que causó que el servidor sobrescribiera partes de sus áreas internas de datos. El servidor, que se ejecutaba con el privilegio más alto, no se comportó debidamente y permitió que el gusano creara copias de sí mismo.

Podemos resumir nuestro análisis sobre servidores de la siguiente forma:

> *Los servidores suelen ser más difíciles de construir que los clientes porque, aun cuando pueden implantarse con programas de aplicación, los servidores deben reforzar todos los procedimientos de acceso y protección del sistema computacional en el que corren, además tienen que protegerse contra todos los errores posibles*

---

[3] N. del T. textualmente: bicho o piojo. Se refiere a un desperfecto en el programa.

19.6 Servidor RARP

Hasta ahora, todos nuestros ejemplos de interacción cliente-servidor requieren que el cliente sepa la dirección completa del servidor. El protocolo RARP, del capítulo 6, proporciona un ejemplo de interacción cliente-servidor con un cambio levemente diferente. Recordemos que cuando una máquina sin disco se reinicia, utiliza RARP para encontrar su dirección IP. En lugar de tener al cliente comunicado directamente con el servidor, los clientes de RARP difunden sus peticiones. Una o más máquinas ejecutan los procesos de respuesta del servidor RARP y cada una de ellas devuelve un paquete que responde a la búsqueda.

Hay dos diferencias significativas entre el servidor RARP y un eco UDP o servidor de tiempo. En primer lugar, los paquetes RARP viajan a través de una red física directamente en las estructuras del hardware y no en los datagramas del IP. De este modo, a diferencia del servidor UDP de eco que permite al cliente ponerse en contacto con un servidor en cualquier lugar de la red de redes, el servidor RARP requiere que el cliente esté en la misma red física. En segundo lugar, RARP no puede implantarse mediante un programa de aplicación. Los servidores de eco y tiempo se pueden construir como programas de aplicación porque utilizan el UDP. En contraste, un servidor RARP necesita tener acceso a los paquetes de hardware primarios.

19.7 Alternativas al modelo cliente-servidor

¿Cuáles son las alternativas para la interacción cliente-servidor y cuándo podrían éstas ser atractivas? En esta sección se ofrece al menos una respuesta a estas preguntas.

En el modelo cliente servidor, los programas suelen actuar como clientes cuando necesitan información, pero algunas veces es importante minimizar dichas interacciones. El protocolo ARP del capítulo 5 nos brinda un ejemplo. Utiliza una forma modificada de la interacción cliente-servidor para obtener transformaciones de las direcciones físicas. Las máquinas que se valen de ARP mantienen una memoria intermedia (caché) de respuestas para mejorar la eficiencia de las búsquedas que surjan después. El proceso de memoria intermedia (caching) mejora el desempeño de la interacción cliente-servidor en casos en los que la historia reciente de búsquedas ha sido un buen indicador de lo que será su uso futuro.

Aunque el proceso de memoria intermedia mejora el desempeño, no cambia la esencia de la interacción cliente-servidor. La esencia descansa en que suponemos que el procesamiento debe estar dirigido por la demanda. Todos hemos asumido que un programa se ejecuta hasta que se necesita información y, entonces, actúa como un cliente para obtener la información que necesita. Adoptar una opinión del mundo enfocada a la demanda es natural y surge de la experiencia. El proceso de memoria intermedia ayuda a aliviar el costo de la obtención de información, bajando los costos de recuperación para todo a excepción del primer proceso en el que se hace una petición.

¿Cómo podemos disminuir el costo de recuperación de información en la primera petición? En un sistema distribuido, es posible tener actividades de respaldo concurrentes que recolecten y difundan la información *antes* de que algún programa en particular la requiera, logrando que los costos de recuperación sean aún más bajos para la petición inicial. Lo más importante es que la recolección de información permite que un sistema dado continúe ejecutándose aun cuando algunas máquinas o redes conectadas a ella hayan fallado.

La prerrecolección es la base para el comando *ruptime* de UNIX 4BSD. Cuando se inv *ruptime*, éste reporta la carga de CPU e indica desde hace cuánto tiempo se inició el sistema cada máquina en la red local. Un programa de respaldo que corre en cada máquina emplea el UD para difundir la información acerca de la máquina de manera periódica. El mismo programa tam bién recolecta la información de entrada y la coloca en un archivo. Debido a que las máquinas difunden información continuamente, cada máquina tiene una copia de la última información a mano: el cliente que busque información, nunca necesitará acceder a la red. De hecho, puede le la información de un almacén secundario e imprimirla para su lectura.

La ventaja principal de tener la información reunida localmente, antes de que el cliente la ne cesite, es la velocidad. El comando *ruptime* responde de manera inmediata cuando se invoca sin es perar los mensajes que atraviesan la red. El segundo beneficio ocurre cuando el cliente puede en contrar algo acerca de las máquinas que ya no están operando. En particular, si una máquina dej de radiotransmitir información, el cliente puede reportar el tiempo que ha transcurrido desde la ú tima radiotransmisión (es decir, puede reportar cuánto tiempo ha estado la máquina fuera de línea)

La prerrecolección tiene una gran desventaja: utiliza tiempo del procesador y ancho de ban da de la red, aun cuando a nadie le importen los datos que se estan recolectando. Por ejemplo, l difusión de ruptime y la recolección continúan corriendo durante toda la noche, aunque nadie es presente para leer la información. Si sólo algunas máquinas están conectadas a una red dada, costo de prerrecolección es insignificante. Se puede pensar como una actividad de respaldo inocu Sin embargo, para las redes con muchos anfitriones, el gran volumen de tráfico de difusión gener do por la prerrecolección, se hace muy caro. En particular, el costo de leer y procesar los mensaj de radiodifusión se vuelve alto. De este modo, la prerrecolección no está entre las alternativas m populares para cliente-servidor

CAPÍTULO 44

Administración de red de IBM

ANTECEDENTES

La administración de red de IBM se refiere a cualquier arquitectura utilizada para administrar redes con SNA (Arquitectura de Sistemas de Red de IBM) o APPN (Conectividad Avanzada de Redes entre Equivalentes). La administración de red de IBM es parte de ONA (Arquitectura de Redes Abiertas) y se realiza de manera central a través de plataformas de administración como NetView y otras. Se divide en cinco funciones que son similares a las funciones de administración de red especificadas en el modelo OSI (Interconexión de Sistemas Abiertos). Este capítulo describe las áreas funcionales de la administración de red de IBM, la arquitectura de administración de red de ONA y las plataformas de administración. La figura 44-1 muestra una red básica IBM administrada.

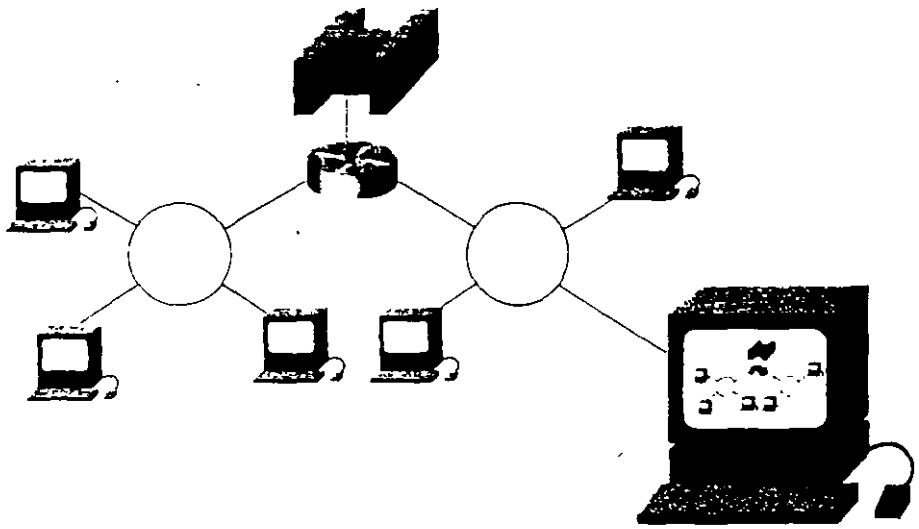


Figura 44–1
La administración de red de IBM maneja las redes SNA o APPN.

ÁREAS FUNCIONALES DE LA ADMINISTRACIÓN DE REDES IBM

IBM divide la administración de red en las cinco siguientes funciones basadas en el usuario: *administración de la configuración, administración del desempeño y la contabilidad, administración de problemas administración de operaciones y administración de cambios.*

Administración de la configuración de IBM

La primera de las cinco funciones controla la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recursos. Un sistema de administración central almacena los datos en las bases de datos de la administración de la configuración e incluye información como los números de versión del software del sistema o microcódigo; números de serie del hardware y software; ubicación física de los dispositivos de red; nombres, direcciones y números telefónicos de contactos. Como se puede esperar, la administración de la configuración en IBM corresponde de manera muy cercana a la administración de la configuración de OSI.

Los elementos de la administración de la configuración ayudan a llevar un inventario de los recursos de la red y asegurar que los cambios en la configuración de la red se reflejen en la base de datos de la administración de la configuración. La administración de la configuración también proporciona información que se utiliza en los sistemas de administración de problemas y en la administración de cambios. Los sistemas de administración de problemas utilizan esta información para comparar las diferencias en versión y para ubicar, identificar y verificar las características de los recursos de la red. Los sistemas de administración de cambios utilizan la información para analizar el efecto de los cambios y para programar los cambios en momentos de impacto mínimo de la red.

Administración del desempeño y la contabilidad en IBM

La segunda función proporciona información respecto al funcionamiento de los recursos de red. Las funciones de los equipos de administración de desempeño y contabilidad incluyen el monitoreo de los tiempos de respuesta de los sistemas; la medición de los recursos disponibles; la sintonía, rastreo y control del desempeño de la red. La información recabada por las funciones de administración de la contabilidad y el desempeño es útil para determinar si se están alcanzando los objetivos de desempeño de la red o si, con base en el desempeño se deben iniciar procedimientos de determinación de problemas. La administración de la contabilidad y el desempeño de IBM realiza funciones similares a las que cumple la administración del desempeño y la contabilidad en OSI.

Administración de problemas en IBM

Esta función es semejante a la administración de fallas en OSI, en que maneja las condiciones de error que hacen que los usuarios pierdan toda la funcionalidad de un recurso de la red. La administración de problemas se lleva a cabo en cinco pasos: determinación del problema, diagnóstico del problema, recuperación y desvío del problema, resolución del problema y rastreo y control del problema. La determinación del problema consiste en detectar un problema y dar todos los pasos necesarios para comenzar el diagnóstico del problema, como confinar el problema a un subsistema en particular. El diagnóstico del problema consiste en determinar la causa precisa del mismo y la medida que es necesario tomar para resolverlo. El des-

vío y recuperación del problema son intentos para desviar el problema, parcial o totalmente. Sólo da una solución temporal y depende del módulo de resolución de problemas para resolverlo permanentemente. La resolución del problema es la suma de los esfuerzos para eliminarlo. En general comienza una vez terminado el diagnóstico del problema y suele implicar acciones correctivas, como el reemplazo de hardware o software en estado de falla. El rastreo y control de problemas consiste en el rastreo de cada uno de ellos hasta llegar a su solución final. La información vital que describe el problema se almacena en una base de datos de problemas.

Administración de operaciones de IBM

La cuarta función consiste en la administración distribuida de los recursos de la red desde un punto central por medio de dos conjuntos de funciones: servicios de administración de operaciones y servicios de operaciones comunes. Los servicios de administración de operaciones permiten controlar los recursos remotos centralmente por medio de las funciones siguientes: activación y desactivación de recursos, cancelación de comandos y configuración del reloj. Los servicios de administración de operaciones se pueden iniciar automáticamente en respuesta a ciertas notificaciones de problemas en el sistema.

Los servicios de operaciones comunes permiten la administración de recursos que no son manejados explícitamente por otras área de administración, por medio de una comunicación especializada a través de aplicaciones nuevas y más capaces. Los servicios de operaciones comunes proporcionan dos servicios importantes, el comando ejecutar y la administración de recursos. El comando ejecutar representa una forma estándar para ejecutar comandos remotos. El servicio de administración de recursos proporciona una forma de transportar información en una manera independiente del contexto.

Administración de cambios en IBM

Esta última función rastrea los cambios en la red y mantiene archivos de modificaciones en los nodos remotos. Los cambios en la red ocurren principalmente por dos razones: cambios en los requerimientos del usuario y evitar problemas. Los cambios en los requerimientos del usuario incluyen las actualizaciones en hardware y software, nuevas aplicaciones y servicios, y otros fac-

res que modifican constantemente las necesidades de los usuarios de la red. itar problemas es necesario para enfrentar cambios inesperados producidos mo resultado de la falla de hardware, software u otros componentes de la d. La administración de cambios tiene como objetivo minimizar los proble- s promoviendo de manera ordenada los cambios de la red y administrando s archivos de cambios, los cuales guardan una bitácora de las modificaciones alizadas en la red. La administración de cambios en IBM es semejante en lgunos aspectos a la administración de contabilidad de OSI.

ARQUITECTURAS DE LA ADMINISTRACIÓN DE RED EN IBM

os de las arquitecturas de administración de red IBM más conocidas son *ONA* y *System View*.

rquitectura ONA

NA (*Arquitectura de Redes Abiertas*) es una arquitectura generalizada de dministración de red que define cuatro entidades de administración clave: el nto focal, el punto de colección, el punto de parámetro y el punto de servicio.

l punto focal es una entidad de administración que proporciona el soporte para s operaciones de administración de red centralizada. Responde a las alertas de la ación terminal, conserva las bases de datos de administración y representa una terfase de usuario para el operador de la administración de red. Existen tres pos de puntos focales: principal, secundario y anidado. Los puntos focales princi- les llevan a cabo todas las funciones focales. El punto focal secundario actúa mo respaldo de los puntos focales principales y se utiliza en el caso de una falla el punto focal principal. El punto focal anidado proporciona el soporte de la dministración distribuida en redes grandes. Los puntos focales anidados son sponsables del reenvío de información crítica a los puntos focales globales.

os puntos de reunión transfieren información desde las subredes SNA auto- ntenidas hasta los puntos focales y se suelen utilizar para reenviar datos sde redes entre equivalentes de IBM hasta una jerarquía ONA.

n punto de parámetro es un dispositivo SNA que puede implementar un NA en sí mismo y otros dispositivos. La mayor parte de los dispositivos SNA ándar tienen la capacidad de ser puntos de parámetros.

Un punto de servicio es un sistema que ofrece acceso a ONA para dispositivos no SNA y es, en esencia, una puerta de enlace hacia ONA. Los puntos de servicio tienen la capacidad de enviar información de administración sobre sistemas no SNA hacia los puntos focales, recibir comandos de los puntos focales, traducir comandos en un formato aceptable hacia dispositivos no SNA y reenviar comandos a dispositivos no SNA para su ejecución.

La figura 44-2 muestra la relación entre las diferentes entidades de administración de ONA.

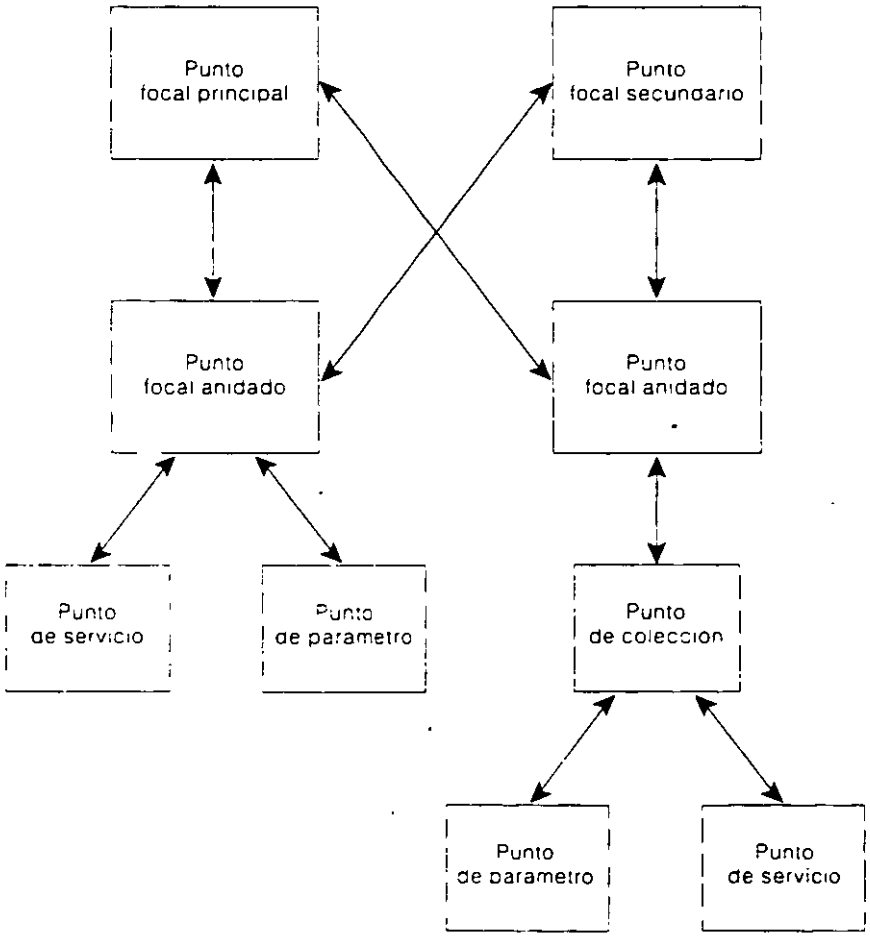


Figura 44-2
Los cuatro tipos de puntos focales se enlazan entre sí en un entorno ONA.

SystemView

SystemView es un plano de prueba que sirve para crear aplicaciones de administración capaces de manejar sistemas de información de diferentes proveedores. El SystemView describe cómo las administraciones que manejan las redes heterogéneas operan con otros sistemas de administración. Es la estrategia oficial de administración de sistemas de la arquitectura de sistemas de aplicación de IBM.

PLATAFORMAS DE ADMINISTRACIÓN DE LA RED IBM

La administración de red de IBM está implementada en diferentes plataformas, entre las que se incluyen *NetView, LNM* y *SNMP.*

NetView

NetView es una plataforma de administración de red corporativa de IBM de gran alcance, que ofrece servicios de administración de red SNA centralizados. Se utiliza en mainframes IBM y es parte del ONA. NetView consta de *equipo de control de comandos, monitor de hardware, monitor de sesión, función de ayuda, monitor de status, monitor de desempeño* y *monitor de distribución.* El equipo de control de comandos proporciona el control de la red mediante la generación de comandos básicos de operación y de acceso a archivos a las aplicaciones VTAM (Método de Acceso de Telecomunicaciones Virtuales), controladores, sistemas operativos y NetView/PC (una interfase entre NetView y los dispositivos no SNA). La función de monitor de hardware monitorea la red y automáticamente pone en alerta al operador de la red cuando se presentan errores en hardware. El monitor de sesión actúa como un monitor del desempeño de VTAM y permite determinar problemas de software y administrar la configuración. La función de ayuda proporciona ayuda a los usuarios de NetView e incluye un equipo de navegación, un equipo de escritorio de ayuda y una biblioteca de las situaciones de operación de red que se presentan más comúnmente. El monitor de status describe y presenta información sobre el status de la red. La función del monitor del desempeño vigila el desempeño de los FEPs (procesadores de sistema frontal), el NCP (Programa de Control de Red) y otros

recursos conectados. El administrador de distribución planea, programa y rastrea la distribución de datos, software y microcódigo en entornos SNA.

Administrador de LAN

LNM (Administrador de la Red LAN) es una aplicación de administración de red de IBM que controla las LANs Token Ring desde una ubicación de soporte central. LNM es un producto basado en la Edición Extendida del OS/2 que interopera con NetView de IBM (que está al tanto de actividades LNM como las alarmas) y otro software de administración de IBM.

Protocolo SNMP

La administración de la red de IBM se puede implementar mediante SNMP (*Protocolo Simple de Administración de Red*). Refiérase al capítulo 46, "El Protocolo SNMP" para conocer los detalles de la implementación de SNMP.

SEGURIDAD DE LOS DATOS.

Es importante que los datos que están ubicados en el servidor de la red se encuentren bien protegidos.

Para que los datos se encuentren perfectamente protegidos, hay que considerar dos apartados:

- Seguridad del almacenamiento en el disco duro.
- Copias de seguridad de los datos.

Seguridad del almacenamiento en el disco duro

Actualmente, la unidad básica de almacenamiento de la información es el disco duro. Su capacidad está en constante incremento (en la actualidad oscila entre 1.2 **GB** y 10 **GB**).

La forma más común de organizar el almacenamiento de la información es a través de un único disco duro (cuenta con la ventaja de la simplicidad de su configuración); aunque, dependiendo del tamaño de la empresa, se puede considerar la posibilidad de trabajar con dos o más discos duros asociados.

Cada disco duro del sistema tiene asignado un número (comenzando en el cero) y se asignan de forma diferente en función del tipo de disco:

- **SCSI**. En una controladora primaria de este tipo, los números van del cero al seis (aunque posee otra dirección que suele estar reservada para el adaptador del bus). Cuando esta controladora se completa puede recurrirse a una controladora secundaria y así sucesivamente hasta un total de cuatro (lo que permitiría disponer de hasta un total de 28 unidades).

- **IDE** y **ESDI**. En una controladora primaria de estos dos tipos, los números van del cero al uno. Cuando esta controladora se completa se puede recurrir a una segunda controladora (lo que permitiría disponer hasta un total de cuatro discos).

Todos los discos duros deben estar formateados a bajo nivel para poder utilizarse.

Particiones

La partición hace que un disco duro, o una parte de él, pueda ser utilizada como medio de almacenamiento.

Por medio de las particiones, el disco duro se puede dividir en unidades lógicas de las que cada una dará acceso a una parte del disco duro.

Las particiones pueden ser de dos tipos:

- **Particiones primarias** que son reconocidas por la **BIOS** del ordenador como capaces de iniciar el sistema operativo desde ella. Para ello, disponen de un sector de arranque (**BOOT SECTOR**).

  Pueden existir hasta un máximo de cuatro particiones primarias de las cuales solamente una puede estar activa en cada momento.

  Con un programa de inicialización adecuado se podría seleccionar entre los diferentes sistema operativos para su arranque (cada uno deberá estar en su propia partición primaria).

- **Particiones secundarias** que se forman en las áreas del disco duro que no tienen particiones primarias y que están contiguas.

  Puede haber, como mucho, una partición secundaria (en este caso, el disco duro no podría tener más de tres particiones primarias).

Unidades lógicas

Las particiones deben estar formateadas para establecer letras de unidades que van de la **C:** en adelante (con la excepción de la unidad **CD-ROM** que se reserva la letra **D:**).

La partición primaria corresponde a la unidad **C:**.

Las particiones secundarias se pueden dividir en una o varias unidades lógicas.

Espacio libre de almacenamiento

Con este término se designa el espacio del disco duro que no pertenece a ninguna partición y que puede utilizarse para crear otra partición.

Conjunto de volúmenes

Un conjunto de volúmenes es la unión de una o más áreas de espacio disponibles (que pueden estar en uno o varios discos duros) que, a su vez, puede dividirse en particiones y unidades lógicas (no es reconocido por **MS-DOS**). Habrá una letra de unidad que representará al conjunto de volúmenes.

Cuando se guardan datos en un conjunto, primero se ocupa el espacio libre del primer segmento, cuando éste se ha llenado se pasa al segundo y así sucesivamente.

El usar un conjunto de volúmenes tiene la ventaja de poder utilizar pequeñas partes de espacio libre para formar un volumen con mayores dimensiones, pero cuenta con el inconveniente de que si se estropea cualquier parte de un disco, toda la información del volumen se perderá.

Conjunto de bandas

Se entiende por conjunto de bandas a la unión de dos o más áreas de espacio disponibles (que pueden estar en dos o más discos duros) que, a su vez, se dividirán en bandas. En cada disco duro se creará una partición y todas ellas tendrán aproximadamente el mismo tamaño (no es reconocido por **MS-DOS**). Habrá una letra de unidad que representará al conjunto de bandas.

Los conjuntos de bandas pueden ser **Con paridad** o **Sin paridad**.

- Un conjunto de bandas sin paridad dividirá cada uno de los discos duros en partes pequeñas llamadas bandas (así, si tiene cuatro discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cuatro bandas cada una).

  Al guardar un archivo no lo hará como se describió en el conjunto de volúmenes, sino que lo distribuirá en las bandas (**RAID 0**) de todos los discos duros (ocupando la primera fila de bandas disponible de cada disco duro antes de pasar a la segunda).

  De esa manera, el acceso será más rápido, ya que se elimina parte del tiempo que tarda el cabezal en buscar los sectores y las pistas donde se encuentra el archivo, pero tiene el inconveniente de que si se estropea un disco duro se pierde toda la información del conjunto de bandas.

- Un conjunto de bandas con paridad utilizará una banda de cada fila del disco duro para guardar información de paridad de todas las bandas de esa fila (así, si tiene cinco discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cinco bandas cada una y en cada fila hay una banda denominada de paridad).

  La información se guarda igual que en el conjunto de bandas sin paridad, pero guardando, en la banda de paridad de cada fila, información que permitirá recuperar los datos de cualquier banda de dicha fila si dejara de funcionar.

  Este método ofrece el mayor nivel de seguridad de los datos (**RAID 5**), ya que cuando falla una banda se pueden recuperar los datos defectuosos que contenía, aunque pierde velocidad de almacenamiento.

  Un inconveniente que tiene es la disminución del espacio libre para guardar información en un porcentaje igual al número de discos duros que forman parte del conjunto de bandas con paridad (así, si hay cinco discos duros se perderá un 20% y si hay cuatro discos duros se perderá un 25%) y, también, que necesita mayor cantidad de memoria **RAM** para no ver disminuir el rendimiento del equipo (aproximadamente, un 25% más de memoria).

Conjunto de espejos

Se entiende por conjunto de espejos a dos particiones de dos discos duros distintos que se configuran para que una sea idéntica a la otra.

Este método hace que el nivel de seguridad sea alto (**RAID 1**), aunque no se evitan los virus, ya que estarían grabados en ambas particiones.

Se pueden dar dos configuraciones:

- Los dos discos duros están conectados al mismo controlador (en este caso, si falla el controlador dejará de funcionar el conjunto de espejos). A este método también se le llama **duplicación**.

- Los dos discos duros están conectados a controladores distintos (en este caso, si falla un controlador el conjunto de espejos seguirá funcionando con el otro controlador). Éste es el nivel más alto de seguridad. A este método también se le llama **duplexación**.

La partición espejo sólo sirve para reflejar los datos de la otra partición (que entrará en funcionamiento cuando falle la primera partición).

Este método hace que el nivel de seguridad sea alto (aunque no se evitan los virus, ya que estarían grabados en ambas particiones).

Copias de seguridad de los datos

Pero qué ocurre si por error, distracción, etc, se produce una perdida de datos importante. Pues no pasaría nada si se cuenta con un buen sistema de copias de seguridad de dichos datos que van a permitir restaurar la información prácticamente al mismo nivel que se encontraba antes de su pérdida.

Antes de empezar con las copias de seguridad, es necesario determinar quién va a ser el responsable o los responsables de su realización.

Algunos administradores de red dejan los procesos de copias de seguridad a usuarios individuales, lo que significa que cada uno de ellos se responsabiliza únicamente de guardar sus propios archivos.

Esta forma de actuar no es buena, ya que los usuarios no dedican el tiempo ni la periodicidad necesaria para hacer una copia de seguridad adecuada de sus archivos.

Por tanto, es mucho más positivo que sea un administrador de la red, como responsable de mantener el funcionamiento y mantenimiento del sistema, el que se

encargue de las copias de seguridad o delegue en otros usuarios que pertenezcan a un grupo de **Operadores de copia**.

Elegir entre copias de seguridad o copiado de archivos

Las redes requieren dos tipos diferentes de protección:

- Las copias de seguridad.
- El copiado de archivos.

La diferencia básica entre ambos sistemas está en el motivo de su realización.

Normalmente se hace una copia de seguridad del sistema para proteger la red de los errores mecánicos y humanos. Las copias de seguridad protegen a la red de los problemas de **hardware** como, por ejemplo, fallos en algún disco duro del servidor.

También son útiles cuando los usuarios borran, sin darse cuenta, sus archivos o los programas.

El copiado de los archivos se realiza, sin embargo, para guardar ciertos archivos a lo largo del tiempo. Los usuarios desean guardar copias de sus archivos de la misma forma que guardan copias de sus documentos en papel.

Un buen procedimiento de copiado es una gran ayuda para gestionar el espacio en el disco duro, ya que hay archivos que no se necesitan de forma continuada y, sin embargo, están ocupando espacio en el disco.

Hay algunas normas que es aconsejable seguir:

- Respalde diariamente los archivos modificados.
- Respalde semanalmente el sistema entero.
- Copie mensualmente los archivos.
- Realice el proceso de copia cuando los usuarios no estén conectados a la red.
- Asigne a alguien para los procesos de respaldo y archivado que pertenezca a un grupo de **Operadores de copia**.

El respaldo diario de los archivos

El proceso de respaldo de los archivos casi siempre necesita bastante tiempo para su realización. Por tanto, es conveniente que sólo realice el respaldo diario de los archivos que hayan sido modificados.

Primero, deberá determinar cuáles son los archivos de la red que deben respaldarse. Por lo general, los programas de aplicaciones y del sistema operativo no suelen sufrir variaciones y, por tanto, no necesitan respaldarse diariamente.

En cambio, los archivos con datos de los usuarios y de configuración de los programas o del sistema operativo son los que sufren variaciones, por tanto deberá respaldarlos diariamente.

Para ello, podrá realizar dos métodos de respaldo:

- **Respaldo diferencial**. Se realiza con los archivos cuyo **bit de archivación** se puso a uno en el último respaldo completo pero no se restaura a cero (dicho **bit de archivación**) para que los archivos vuelvan a respaldarse al día siguiente.

- **Respaldo incremental**. Se realiza con los archivos cuyo **bit de archivación** se puso a uno en el último respaldo completo pero se restaura a cero (dicho **bit de archivación**) para que los archivos no se vuelvan a respaldar al día siguiente (a no ser que se hayan vuelto a modificar).

Para poder localizar fácilmente el respaldo realizado en último lugar, es muy recomendable poner en cada uno la fecha y la hora en que se hizo.

El respaldo semanal del sistema completo

Este método consiste en realizar un respaldo completo de todo el contenido del servidor y, al igual que el método diario, es recomendable que se realice en unidades de cinta.

De este modo, en caso de tener que restaurar el contenido del servidor se realizará de forma fácil y rápida.

Es el método más adecuado, porque permite tener pocas copias y, de esa forma, poder encontrar fácilmente la adecuada.

El copiado mensual de los archivos

Por lo general, el copiado de los archivos es suficiente con que se realice una vez al mes. Asegúrese de que tiene copiados los archivos en un medio o soporte diferente

(cinta, disco, disquete) que las copias de seguridad, para que en caso de perdida o deterioro de la cinta pueda recuperar la información.

El objetivo del copiado es distinto al del respaldo de los archivos, por lo que tendrá que seguir diferentes procedimientos. Entre los cuales están:

- Determine qué directorios y archivos son los que van a copiarse.
- Determine si los archivos van a ser borrados después de ser copiados.
- Es recomendable que comprima los archivos antes de copiarlos, ya que reducirá el espacio de almacenamiento y el tiempo que tardará en realizarse el proceso.
- Indique quién va a realizar el procedimiento de copiado y borrado de los archivos que no desea guardar en el servidor.
- Pida que saquen un listado de los archivos que se han copiado.
- Guarde en lugar seguro las copias de los archivos.

lección del hardware de la copia de seguridad

En redes con discos duros de gran capacidad, el mejor dispositivo para el spaldo del sistema es una unidad de cinta.

Las unidades de cinta son más rápidas y producen mejores resultados que otros étodos, ya que no requieren discos duros ni disquetes.

Existen actualmente cuatro formatos de cinta que se pueden usar para hacer spaldos de una red:

formato DC-6000

Este formato es el más antiguo de ellos (fue creado por **3M** en 1971) y el de ayor tamaño.

Su capacidad se ha ido incrementando en función de tres valores: la longitud de a cinta (puede llegar hasta un máximo de 600 pies), la densidad (**bits** por pulgada) de a cinta y el número de pistas.

Con los últimos avances tecnológicos puede llegar hasta 2 **GB** (usando 30 pistas con una densidad de 68 **kilobits** por pulgada).

Es fiable el resultado del respaldo pero lento (aproximadamente 5 **MB** por minuto). Así mismo, la búsqueda de un fichero en la cinta es secuencial por lo que habrá que buscar en la cinta entera para conseguir encontrarlo.

El nombre de las cintas indica su capacidad. Por ejemplo, la cinta **DC-6525**, indica que tiene una capacidad de 525 **MB**.

El formato DC-2000

Este formato, de tamaño algo más pequeño que el anterior, también fue diseñado por **3M**.

Se usa principalmente para hacer respaldos de discos duros de pequeño tamaño (como los de las estaciones de trabajo).

Su capacidad ha ido en aumento y actualmente puede llegar a guardar 420 **MB** de datos sin comprimir (850 **MB** si están comprimidos).

El cartucho 8 mm

Este formato fue desarrollado por **Exabyte** y está basado en la tecnología desarrollada por **Sony** para sus cámaras de vídeo.

Usa el mismo cartucho que el de las cámaras de vídeo de 8 mm, aunque su medio magnético es de mejor calidad.

Su capacidad ha ido en aumento pudiendo llegar a guardar 5 **GB** de datos sin comprimir (10 **GB** si están comprimidos).

El cartucho 4 mm

Este formato deriva del formato **DAT** desarrollado por **Sony**.

La densidad de la cinta es muy alta y su velocidad de transferencia de datos puede llegar hasta 30 **MB** por segundo.

Su capacidad de datos puede llegar a ser de 2 **GB** sin comprimir para una cinta de 90 metros (4 **GB** si están comprimidos).

La búsqueda de datos es muy rápida y el coste del **hardware** es relativamente bajo.

Por todo ello, este formato es, actualmente, el más usado para realizar respaldos en redes.

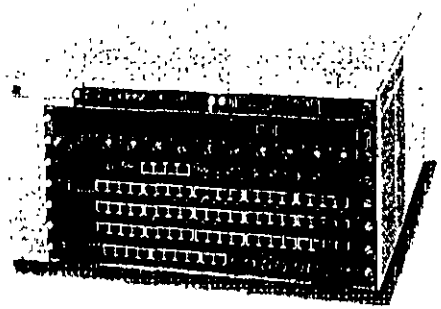
Pasos a seguir en las copias de seguridad	Frecuencia	Archivos a copiar	Lugar de almacenamiento
1.° sistema	Diario	Archivos modificados	Cinta
2.° sistema	Semanal	Sistema completo	Cinta
3.° sistema	Mensual	Archivos no modificados en el último mes	Disco o disquetes

3Com ofrece más que ninguna otra compañía de redes, soluciones de switcheo para un mayor número de ambientes LAN.

Nuestros Boundary Switches proveen un aumento del rendimiento en la periferia de las grandes redes o en oficinas locales en donde la simplicidad y facilidad de uso son consideraciones de importancia. Nuestros High-Function Switches ofrecen un ancho de banda agregado y un control del núcleo de la red sin igual. Y nuestros switches Token Ring incrementan el rendimiento en las redes LAN Token Ring en donde las aplicaciones cliente/servidor y otras aplicaciones que demandan gran ancho de banda exceden la capacidad actual.

Los switches 3Com emplean chips ASICs para alcanzar niveles de rendimiento, confiabilidad y valor sin precedentes.

Boundary Switches

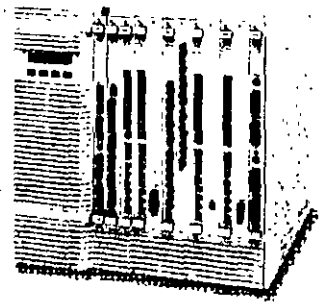


Los Boundary Switches de 3Com, que incluyen los switches apilables SuperStack II, los switches OfficeConnect™ y los FastModules para la plataforma CoreBuilder™ 5000, hacen que la eliminación de la congestión de tráfico en los ambientes Ethernet, Fast Ethernet, FDDI y ATM sea fácil y económica. La tecnología de switcheo de 3Com basada en ASIC y líder en la industria, ofrece un rendimiento más alto al dedicar un ancho de banda LAN completo a cada cliente y servidor de la red LAN.

Productos y Soluciones...

- Los switches SuperStack II ofrecen las mejores tecnologías de switcheo basadas en ASIC y una selección de conexiones a backbones de alta velocidad (Fast Ethernet, FDDI y ATM), además de características modernas tales como Monitoreo Remoto (RMON) estándar, redes LAN virtuales (VLAN) y soporte de multimedia PACE™ de 3Com. Los sistemas opcionales de fuentes de poder, redundantes e ininterrumpibles, sirven para asegurar una operación continua.
- El switcheo Ethernet y Fast Ethernet garantiza una transmisión rápida de archivos grandes y un acceso rápido a datos basados en un servidor para que se tenga una mayor productividad a bajo costo. 3Com ofrece también un switcheo ATM de alta velocidad y económico para grupos de trabajo que tienen 10 Mbps dedicados para los usuarios que emplean el sistema constantemente.
- Con los FastModules Ethernet y Fast Ethernet, la plataforma CoreBuilder 5000 de 3Com ofrece soluciones de switcheo altamente escalables para configuraciones de red a nivel frontera. Los módulos se comunican unos con otros a través del backplane FastChannel del sistema y se conectan a un backbone a través de enlaces ATM o Fast Ethernet.

High-Function Switches



La familia de CoreBuilder High Function Switches de 3Com ofrece megas de ancho de banda poderosas junto con una variedad de características modernas para el núcleo de la red. Estos switches están diseñados para funcionar como puntos para arreglar recursos de la red, puntos de control y administración del ancho de banda y puntos de concentración para la conectividad, resiliencia y migración del rendimiento.

Productos y Soluciones...

- Los switches CoreBuilder 2500 y 6000 de 3Com, construidos en una arquitectura hardware líder en la industria, ofrecen características superiores que comprenden el Elastic Packet Buffering, routing integrado, redes VLAN, soporte multiprotocolo/variedad de medios, tolerancia a fallas/seguridad y administración. Soportan Ethernet, Fast Ethernet, Token Ring, FDDI y switcheo ATM, transparent bridging Ethernet a FDDI y concentración FDDI.
- Equipados con unidades de switcheo poderosas y diseñados para contar con una óptima tolerancia a las fallas, los switches de alta calidad de la familia CoreBuilder 7000 de 3Com proveen switcheo de alta velocidad para redes con backbones ATM. los modulos de switcheo Ethernet/ATM y Fast Ethernet integran redes LAN tradicionales con redes ATM utilizando clientes de LAN emulation y configuraciones VLAN por puerto.
- La plataforma CoreBuilder 5000 de 3Com con su arquitectura tolerante a fallas que es líder en la industria, ofrece switcheo Ethernet, Fast Ethernet y FDDI de alto rendimiento, y provee un espectro completo de caracteristicas modernas que comprende switches virtuales y soporte RMON completo. Una opción ATM provee un camino de migracion hacia futuras redes de muy alto ancho de banda.

Token Ring Switches

Los switches Token Ring de 3Com optimizan el rendimiento de las redes Token Ring en donde el crecimiento y las configuraciones de ancho de banda estén retrasando el tráfico de datos, en el Centro de Datos y en la periferia de la red. Las soluciones de switcheo de 3Com ofrecen un complemento integral de características dedicadas al escalamiento del ancho de banda, la garantía de confiabilidad y la integración de switcheo sin dificultades en las redes LAN Token Ring existentes.

Productos y Soluciones...

- 3Com ofrece dos productos de switcheo Token Ring flexibles para las redes cliente-servidor en crecimiento. Ambos productos soportan el source route bridging, transparent bridging y SRT.
- Los switches Token Ring de 3Com proveen un método efectivo con una buena relacion costo-beneficio para segmentar el ancho de banda. Además, ofrecen una solución inicial para la expansión fácil de las infraestructuras de red existentes basadas en IBM. El 802.1d y el Spanning Tree basado en IBM facilitan aun más la integración de switcheo y garantizan la integridad de la red.
- El SuperStack II Switch 2000 TR utiliza la innovadora tecnología de ASIC Token Ring Switching Engine (TRSE) para entregar un switcheo Token Ring a velocidad máxima para el Centro de Datos o el grupo de trabajo. Las caracteristicas de Control de Flujo y Control de Prioridad aumentan la confiabilidad a la voz que el soporte VLAN y RMON simplifica la administracion, y la fuente de poder opcional asegura el tiempo de operacion activa. Los modos de switcheo por puerto que pueden seleccionarse aumentan la flexibilidad y mejoran la eficiencia.
- El switch CoreBuilder 6000 con un Modulo de Switcheo Token Ring provee alta velocidad, switcheo de alta densidad de hasta 88 Token Rings, así como un anillo de backbone FDDI.

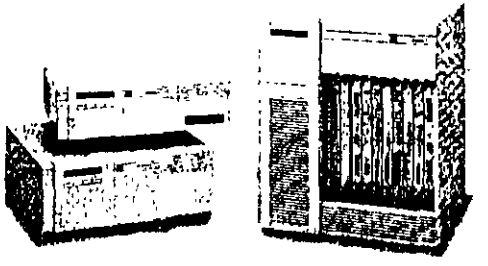
Routers y Conectividad SNA

Los routers de 3Com y los dispositivos de conversión SNA permiten a las redes de área local comunicarse sin dificultades entre ellas y con redes de hosts basadas en la System Network Architecture (SNA).

Al operar en redes de área amplia (WAN), los routers 3Com de backbone y de la oficina remota cumplen con la alta demanda de ancho de banda, administran un amplio espectro de protocolos de comunicación, simplifican la interconectividad de sucursales y de oficina remota y además, ahorran en costos administrativos.

En ambientes combinados de cliente/servidor y sistema central IBM, los convertidores SNA a LAN de 3Com extienden la conectividad que hay a través de la empresa y protegen la inversión en equipos SNA tradicional.

Routers



El NETBuilder II® router de 3Com, con su arquitectura de multiprocesador flexible, diseño modular y con los últimos adelantos técnicos, es la mejor elección para integrar múltiples conexiones LAN y WAN en el backbone de una empresa. El procesamiento RISC, los chips ASIC personalizados y un backplane de 800 Mbps proporcionan enlaces de alta velocidad para las redes de área amplia y Ethernet, Fast Ethernet, Token Ring y FDDI. Además, los routers NETBuilder II permiten la migración fácil hacia ATM y opciones multiprotocolo IBM SNA. Una variedad de chasis y módulos compatibles, más la habilidad de agregar potencia de procesamiento, aseguran la escalabilidad.

Productos y Soluciones...

- Los modelos NETBuilder II WAN Extender integran los servicios Integrated Services Digital Network (ISDN), Switched 56 y los T1 o E1
- Los servicios WAN que ahorran costos incluyen la compresión de datos estándar de la industria, una amplia gama de funciones dis cadas y la innovadora arquitectura de sistemas Boundary Routing® de 3Com para centralizar la complejidad del routing remoto en un lugar central
- La Flash memory opcional ofrece una iniciación confiable y permite la fácil actualización remota de software en la red
- La opción EZBuilt System incluye todos los elementos básicos de un sistema NETBuilder II para ahorrar costos, tiempo de instalación y esfuerzos de soporte

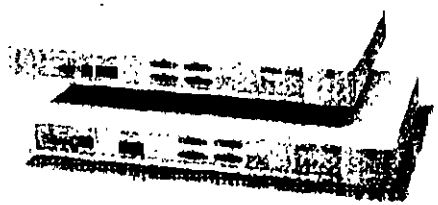
Routers de Oficina Remota

3Com ofrece una línea completa de routers para expandir las conexiones de lugares remotos fácilmente y con una buena relación costo beneficio. La familia SuperStack II NETBuilder® soporta redes LAN Ethernet y Token Ring, líneas análogas e ISDN y aplicaciones SNA que usan la arquitectura Boundary Routing de 3Com. Elija entre dispositivos que ofrecen un soporte de protocolo completo, enlaces sólo IP conexiones X.25 para redes LAN IP y Open System Interconnection (OSI), Ethernet Boundary Routing o funcionalidad solamente de bridge. Para los negocios pequeños, 3Com ofrece también bridge/routers OfficeConnect Remote.

Productos y Soluciones...

- La arquitectura Boundary Routing de 3Com reduce dramaticamente el costo de la administración del bridge/router Ethernet y Token Ring y le permite enlazar de cinco a 10 veces más lugares remotos sin tener que agregar complejidad administrativa.
- Las características de reducción de costos de WAN incluyen soporte para la compresion de datos estándar de la industria, ancho de banda de demanda, filtro inteligente y conexiones de demanda.
- El soporte IBM incluye el Boundary Routing optimizado para SNA, y Data Link Switching (DLSw) para dirigir el trafico SNA y NetBIOS por las redes IP.
- Los routers SuperStack II NETBuilder soportan una gama de protocolos WAN, ademas de conexiones de discado. La SuperStack II NETBuilder Remote Office ISDN cuenta con adaptadores de terminal integrados ISDN. Se dispone también de fuentes de poder de respaldo.
- El bridge/router OfficeConnect Remote ofrece ISDN y enlaces de línea dedicada a lugares centrales, además de conexiones análo

Conectividad SNA



El SuperStack II LinkConverter™ II es un convertidor SNA a LAN que le permite integrar un gran número de dispositivos SNA tradicionales con las redes Token Ring y Ethernet de hoy. Utilizando una conversión confiable, con una buena relación costo beneficio, de redes tradicionales a LCC2, el LinkConverter II proporciona compatibilidad completa con los dispositivos SNA basados en el mainframe (IBM y sistemas principales compatibles con IBM, procesadores front-end, controladores y terminales), junto con conexiones directas o de router a minicomputadoras IBM AS/400®. Los sistemas opcionales de fuentes de poder SuperStack II, redundantes e ininterrumpibles, sirven para asegurar una operación continua.

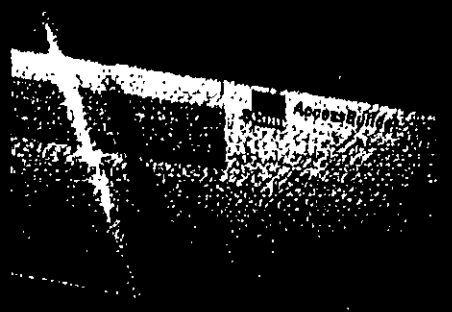
Productos y Soluciones...

- Las opciones del software ofrecen conversión LAN para Synchronous Data Link Control (SDLC), Binary Synchronous Communication (BSC), Async Alarms o Qualified Logical Link Control (QLLC) para las comunicaciones de alto rendimiento entre los sistemas IBM, dispositivos SNA tradicionales y usuarios Token Ring o Ethernet.
- Las licencias de software opcionales permiten el uso de software que traduce datos BSC para soportar cajeros automáticos o para soportar controladores de dispositivos 3270, alarmas de seguridad asincronas o conversión QLLC del lado del terminal.
- El convertidor soporta las plataformas de servicios financieros IBM (3600, 4700) terminales del punto de venta y los controladores de grupo de red IBM. Tambien proporciona soporte para la administración NetView® de IBM.

El acceso a los recursos corporativos y de la Internet en cualquier momento y en cualquier lugar se han vuelto cruciales para las empresas, los negocios pequeños y las personas, a nivel mundial.

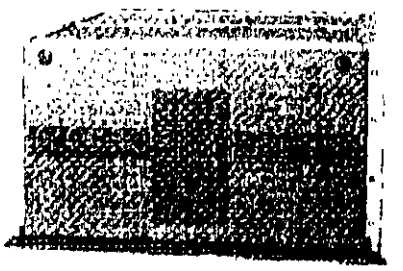
3Com ofrece una selección completa de soluciones de extremo a extremo para cumplir con las diversas necesidades de acceso remoto de hoy, que varían de un concentrador de acceso de alto rendimiento diseñado especialmente para los puntos de presencia del proveedor de la red hasta los routers y módems digitales optimizados para grupos de trabajo pequeños y estaciones de trabajo individuales.

Las soluciones de 3Com ofrecen conexiones rápidas, flexibles y sólidas que simplifican la complejidad del acceso de red remoto para los usuarios finales.



Acceso Remoto

Concentradores de Acceso

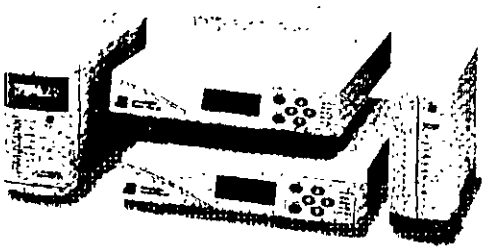


Los concentradores de acceso 3Com ofrecen soluciones completas de conectividad basadas en software para redes empresariales y proveedores de servicios de red. El concentrador AccessBuilder® 7000, optimizado para oficinas corporativas centralizadas que necesitan enlaces de gran ancho de banda, intensivo para redes LAN Ethernet, se ha creado alrededor de una arquitectura sólida y tolerante a las fallas que usa una interfaz de línea flexible para tecnologías clave de carriers WAN. El concentrador AccessBuilder 8000 es un sistema de acceso digital de alto rendimiento que provee soluciones de acceso remoto, confiables y escalables, para los proveedores de servicio y las empresas.

Productos y Soluciones...

- El concentrador AccessBuilder 7000 ofrece routing de llamadas altamente inteligente entre bridges, routers, adaptadores de terminal y otras tarjetas de interfaz de red instaladas en un chasis de alta densidad y manejo centralizado. Provee interfaz de línea flexible para líneas dedicadas, dial up análogo e ISDN Primary Rate Interface (PRI) y Basic Rate Interface (BRI), que soporta hasta 112 conexiones de datos de 64 Kbps simultáneas.
- Dependiendo de los módulos que se utilicen, un sistema AccessBuilder 8000 puede escalar de 24 a 388 puertos, y proporcionar el potencial de crecimiento óptimo para los proveedores de servicio y las empresas. El sistema integra enlaces telefónicos análogos T1/E1 e ISDN PRI, V120, adaptadores de terminal, comunicaciones celulares V.34 y transacciones de conexiones de módem. Las interfaces LAN y WAN incluyen el soporte TCP/IP y X.25.

Conectividad para Oficinas Pequeñas y Remotas

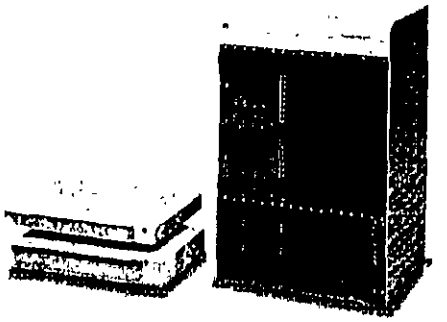


La familia del bridge/router AccessBuilder Remote Office de 3Com, los routers de acceso OfficeConnect Remote, dispositivos gateway OfficeConnect y los dispositivos client-side ofrecen conectividad remota que es más accesible y fácil de usar. Estos productos están diseñados para dar a las oficinas sucursales, los negocios pequeños y a los usuarios individuales que usan frecuentemente el sistema, el mismo acceso a los recursos de la red y las herramientas para mejorar la productividad de que disfrutan los usuarios empresariales, sin tener que contar con un alto nivel de conocimientos especializados sobre la red en el lugar donde se requiere.

Productos y Soluciones...

- Los bridges/routers AccessBuilder Remote Office ISDN utilizan enlaces ISDN BRI (64 Kbps) y ISDN PRI (128 Kbps) junto con líneas dedicadas digitales para proporcionar conexiones rápidas y confiables entre las redes LAN Ethernet que implementan los protocolos de red TCP/IP y Novell IPX®
- Los routers OfficeConnect Remote, de rápida instalación y fácil configuración, proporcionan conexiones de ISDN de línea dedicada a otras redes, la Internet y servicios comerciales
- Los dispositivos gateway 3Com OfficeConnect ofrecen a las oficinas pequeñas que tienen redes LAN Novell NetWare® conexiones Internet simples, accesibles y seguras por medio de ISDN o WAN/líneas dedicadas que utilizan sólo una dirección IP para hasta 50 computadoras personales
- El router de acceso AccessBuilder Remote User 400 proporciona interfaces ISDN y LAN Ethernet para usuarios individuales o hasta para cuatro usuarios de oficina remota
- 3ComImpact™ IQ es el módem ISDN externo de mejor rendimiento y más fácil de usar en el mercado.

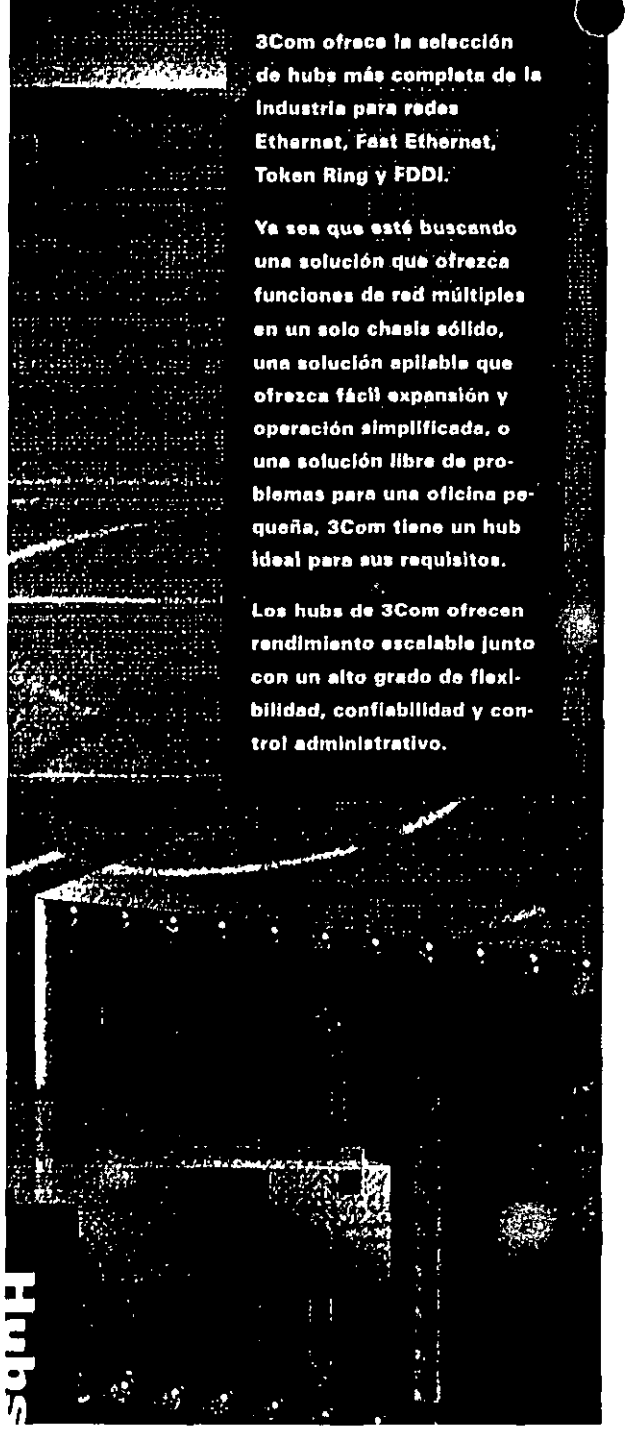
Acceso Remoto Empresarial



Los switches y servidores de acceso remoto AccessBuilder Enterprise ofrecen a los usuarios remotos un acceso de dial-up completo a grupos de trabajo y oficinas remotas y recursos de LAN Ethernet o Token Ring empresariales. Los modelos de esta familia comparten una funcionalidad común y ofrecen características para optimizar la conectividad en varios ambientes de red. El software de administración grafica SNMP Transcend AccessBuilder Manager de 3Com se incluye con cada sistema para tener una configuración rápida y fácil en las redes LAN TCP/IP y Novell IPX. Un software de seguridad opcional soporta una variedad de sistemas de seguridad externos.

Productos y Soluciones...

- El AccessBuilder 5000 Remote Access LAN/WAN switch es una solución de acceso Ethernet o Token Ring de alto rendimiento para oficinas corporativas centralizadas que ofrece una densidad de puerto que es líder en la industria (16 a 256 puertos de usuarios) utilizando una combinación de conexiones de módem análogas, T1, ISDN y digitales
- Los servidores AccessBuilder 4000 Remote Access están diseñados con base en una arquitectura RISC de alto rendimiento para conexiones rápidas de dial up ISDN BRI y análogas (8 a 16 puertos) a la red LAN Ethernet o Token Ring, además de bridging y routing multiprotocolo concurrente
- Los servidores de SuperStack II AccessBuilder 2000 fáciles de configurar, ofrecen un acceso a módem análogo listo para conectar y usar a redes LAN Ethernet de grupos de trabajo y oficinas remotas

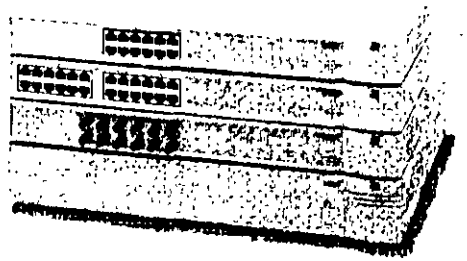


3Com ofrece la selección de hubs más completa de la industria para redes Ethernet, Fast Ethernet, Token Ring y FDDI.

Ya sea que esté buscando una solución que ofrezca funciones de red múltiples en un solo chasis sólido, una solución apilable que ofrezca fácil expansión y operación simplificada, o una solución libre de problemas para una oficina pequeña, 3Com tiene un hub ideal para sus requisitos.

Los hubs de 3Com ofrecen rendimiento escalable junto con un alto grado de flexibilidad, confiabilidad y control administrativo.

Hubs Apilables

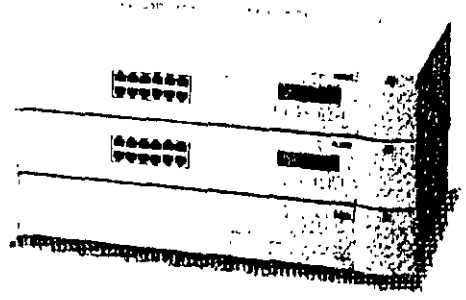


Los hubs SuperStack II ofrecen el ahorro y la facilidad de instalación que usted espera de los hubs apilables, además de una variedad de agregados modulares que mejoran la flexibilidad, calidad de manejo y rendimiento de las conexiones. Estos sólidos hubs, diseñados para grupos de trabajo en crecimiento, se integran fácilmente a otras unidades de sistemas SuperStack II para proporcionar switcheo, conectividad remota y sistema de fuente de poder redundante e ininterrumpible. Además, el software y hardware de administración Transcend ofrecen un control global y ayuda en la resolución de problemas

Productos y Soluciones...

- La tecnología SuperStack II PS Hub 40 con Power Grouping™ utiliza la segmentación para administrar el tamaño de los grupos de trabajo y equilibrar las cargas de tráfico entre los segmentos Ethernet. Los puertos pueden ser asignados individualmente por medio de software, lo que le da a usted la oportunidad de variar el número de usuarios por segmento y configurar la red lógicamente.
- Los hubs SuperStack II Hub 10 Ethernet y los SuperStack II Hub 100 Fast Ethernet soportan conexiones de medios individuales o combinados en pilas de hasta ocho unidades (208 puertos). Los módulos de backbone/downlink que pueden ser instalados por el usuario y los módulos de administración le permiten agregar mayor conectividad y funcionalidad si lo necesita
- La familia SuperStack II Hub TR se ha optimizado para servir ambientes Token Ring dinámicos y de misión crítica con soporte hasta para 260 usuarios, capacidades amplias de administración y un amplio espectro de características tolerantes a fallas para garantizar el tiempo de actividad

Hubs Multifunciones

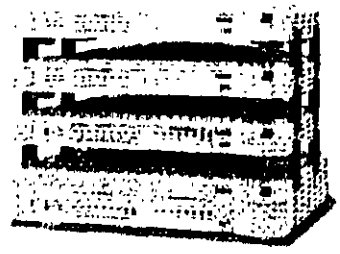


Los hubs multifunciones de 3Com reúnen una multitud de características y funciones en un solo chasis. La poderosa plataforma CoreBuilder 5000 combina la conectividad Ethernet, Token Ring, FDDI y ATM, incluyendo grupos de trabajo y switcheo de backbone, en un paquete administrable, confiable y seguro. Los chasis hubs de multifunción ONline® System Concentrator y LinkBuilder® MSH™ proporcionan conectividad Ethernet, Token Ring y FDDI. Los hubs multifunciones de 3Com satisfacen las necesidades de diversos ambientes empresariales, desde Centros de Datos de alta densidad hasta closets de cableado departamentales.

Productos y Soluciones...

- Las arquitecturas flexibles y escalables administran una amplia gama de ambientes y tecnologías LAN en una plataforma sólida, preservando la inversión existente y soportando actualizaciones a medida que la red se expande.
- Se dispone de switcheo de alto rendimiento (consulte la sección Switches de este folleto)
- Las características de tolerancia a fallas, como fuente de poder redundante y soporte de enlace resiliente, aseguran el tiempo de actividad para las aplicaciones de misión crítica
- Una selección de tamaños de chasis le permite adaptar una variedad de ambientes de red de manera eficaz en función de los costos

Hubs y Repetidores para Negocios Pequeños

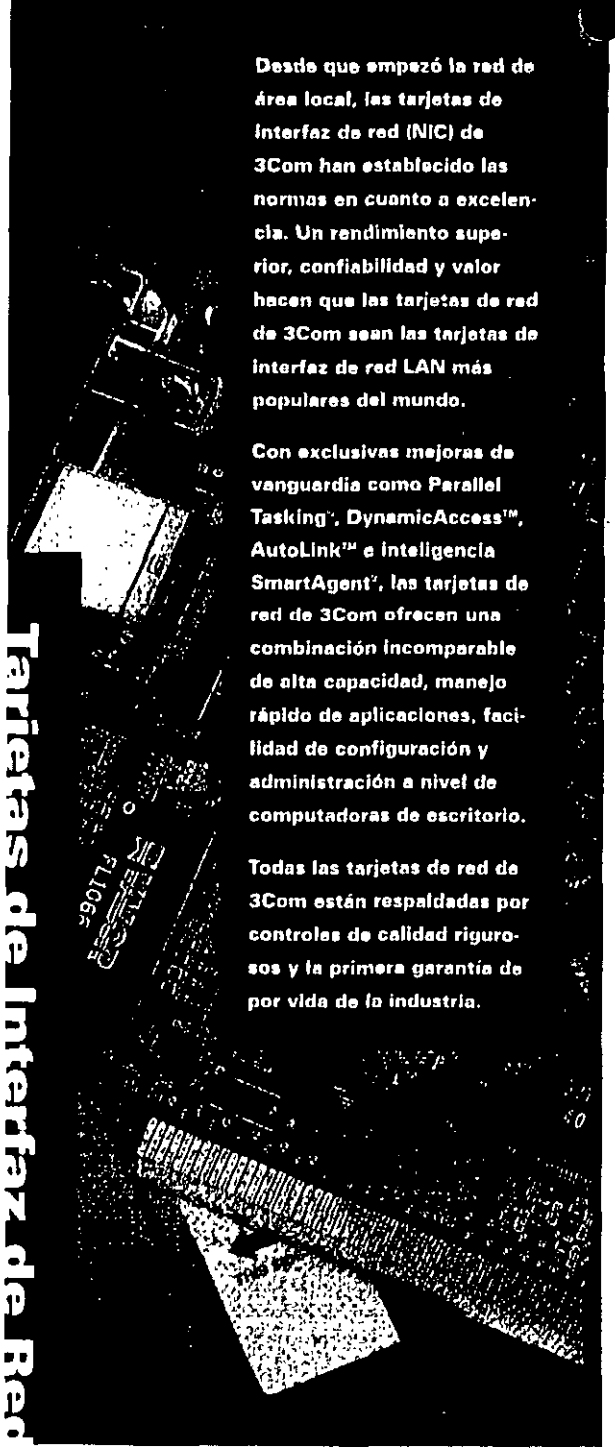


Los hubs para oficinas pequeñas Ethernet y Fast Ethernet de 3Com, que pueden instalarse en sólo minutos y requieren poco mantenimiento cuando están en operación, hacen que el compartir recursos sea fácil y eficaz. Los hubs OfficeConnect de 3Com se ofrecen en una variedad de características y precios, desde un modelo básico económico hasta una unidad expandible y totalmente administrable con un puerto backbone. Todos los productos OfficeConnect que se han unido se diseñaron para trabajar juntos, con un mínimo de configuración.

Productos y Soluciones...

- La operación silenciosa y el agradable diseño estético y compacto hacen que los hubs OfficeConnect sean ideales para oficinas pequeñas
- Una variedad de hubs Ethernet y Fast Ethernet no administrables y un hub Ethernet completamente administrable aseguran la flexibilidad
- Un indicador Alerta LED (diodo emisor de luz) único y otros indicadores LED permiten que el personal no técnico de la oficina pueda detectar los problemas.
- El hub Fast Ethernet ofrece diez veces más de ancho de banda de 10 Mbps Ethernet para acomodar a los usuarios que emplean el sistema constantemente
- Transcend Quick Configuration Manager (incluido con el modelo OfficeConnect 8/TPMI) proporciona administración local por medio de una interfaz Windows® fácil de usar y se integra perfectamente con la administración corporativa Protocolo Simple de Administración de red (SNMP)
- La línea OfficeConnect incluye también servidores, diseñados por Castelle® líder del mercado, que proporcionan capacidades de red de impresión, fax y CD ROM

Tarjetas de Interfaz de Red

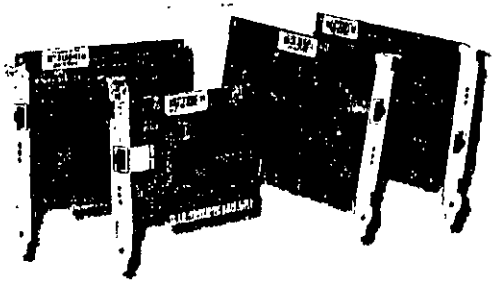


Desde que empezó la red de área local, las tarjetas de interfaz de red (NIC) de 3Com han establecido las normas en cuanto a excelencia. Un rendimiento superior, confiabilidad y valor hacen que las tarjetas de red de 3Com sean las tarjetas de interfaz de red LAN más populares del mundo.

Con exclusivas mejoras de vanguardia como Parallel Tasking®, DynamicAccess™, AutoLink™ e inteligencia SmartAgent®, las tarjetas de red de 3Com ofrecen una combinación incomparable de alta capacidad, manejo rápido de aplicaciones, facilidad de configuración y administración a nivel de computadoras de escritorio.

Todas las tarjetas de red de 3Com están respaldadas por controles de calidad rigurosos y la primera garantía de por vida de la industria.

Tarjetas de Red Ethernet y Fast Ethernet para Computadoras de Escritorio y Portátiles

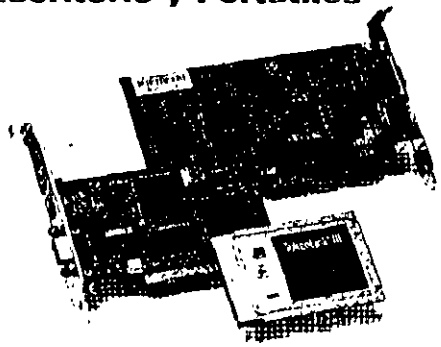


EtherLink® es el nombre principal en las tarjetas de interfaz de red Ethernet a nivel mundial. La familia EtherLink de 3Com supera a las tarjetas de red de la competencia en las redes LAN Ethernet de 10 Mbps hasta en un 133 por ciento. Las tarjetas Fast Ethernet de doble velocidad se adaptan automáticamente a las redes LAN Ethernet o Fast Ethernet, permitiendo que haya una migración fácil de una operación de 10 Mbps a 100 Mbps. Para las computadoras portátiles, la familia EtherLink III de tarjetas de red PC Card (PCMCIA) ofrece la mayoría de los beneficios de las tarjetas de tamaño completo de 3Com en un paquete del tamaño de una tarjeta de crédito. También se dispone de una combinación EtherLink III LAN + 33.6 Modem PC Card.

Productos y Soluciones...

- Las tarjetas de vanguardia EtherLink XL PCI y Fast EtherLink XL PCI de 3Com combinan el control de bus de 32 bit, la arquitectura patentada Parallel Tasking de 3Com y las características de DynamicAccess para optimizar la capacidad y la utilización del procesador y tener un mayor rendimiento
- El software AutoLink le permite configurar una tarjeta de red e instalar archivos Novell NetWare en clientes DOS/Windows en sólo minutos. Windows 95 Plug and Play está soportado en modelos de bus PCI
- DynamicAccess con la tecnología PACE en las tarjetas de red EtherLink XL PCI y Fast EtherLink XL PCI adapta fácilmente las aplicaciones con ancho de banda, incluyendo multimedia, en redes LAN Ethernet y Fast Ethernet compartidas o switchoadas
- Las tarjetas de red EtherLink ofrecen numerosas opciones de bus PC y conectividad de cableado, y el software Ethernet de soporte más completo de la industria

Tarjetas NIC Token Ring para Computadoras de Escritorio y Portátiles

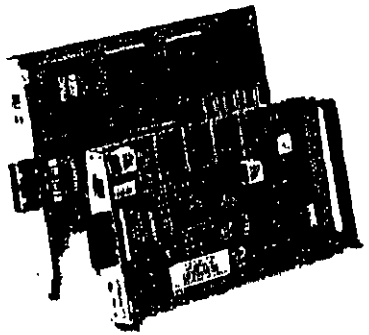


La familia de tarjetas de red Token Ring, TokenLink® Velocity™ de 3Com, es ideal para las aplicaciones intensivas en ancho de banda y los ambientes Token Ring switcheados, lo que proporciona rendimiento y tiempos de respuesta de red no superados. La instalación es más rápida que la de las tarjetas de la competencia gracias al software AutoLink y el soporte de Windows 95 PCI Plug and Play. En las computadoras portátiles, la TokenLink III PC Card resulta fácil de instalar y de usar y es compatible con cualquier laptop IBM o compatible con IBM que cuente con ranuras para PC Card Type II o Type III está garantizada.

Productos y Soluciones...

- La interfaz de control de bus de 32 bits de la tarjeta TokenLink Velocity PCI y la arquitectura Parallel Tasking de la tarjeta TokenLink Velocity ISA producen una capacidad sin igual
- La utilización excepcionalmente baja de la CPU de la tarjeta TokenLink Velocity PCI ofrece un rendimiento máximo para los servidores y los clientes de alta calidad
- Las tarjetas TokenLink Velocity ISA y TokenLink III PC Card son completamente compatibles con los controladores IBM, las aplicaciones y los sistemas operativos existentes, lo que asegura que haya una integración transparente con las redes LAN Token Ring de 4 Mbps y 16 Mbps
- Las tarjetas NIC TokenLink Velocity ISA proporcionan una operación full duplex para velocidad de transferencia alta cuando se utilizan con los switches Token Ring

Tarjetas de Red FDDI y ATM para Computadoras de Escritorio y Servidores



La familia FDDILink™, la familia ATMLink™ y las tarjetas de red ATM PC y de estaciones de trabajo proporcionan conexiones rápidas y confiables para computadoras de escritorio y servidores de las redes Fiber Distributed Data Interface (FDDI) y Asynchronous Transfer Mode (ATM).

Productos y Soluciones...

- Las tarjetas de red FDDILink de 3Com conectan a los servidores y a los clientes de equipo de alto desempeño equipados con buses PCI y EISA con redes FDDI. Estas tarjetas económicas y de alto rendimiento ofrecen la más baja utilización de la CPU que hay en la industria, entregando la velocidad de transferencia de datos óptima en una variedad de tipos de cableado.
- Las tarjetas de red ATMLink para computadoras con bus PCI y estaciones de trabajo Sbus de Sun Microsystems brindan un rendimiento ATM ultrarrápido de 155 Mbps a la computadora de escritorio. Se ciñen a las normas del Foro ATM y permiten una migración sin dificultades, de las redes LAN tradicionales a ATM, con soporte del cliente para LAN Emulation. Las tarjetas de red ATMLink también están optimizadas para aplicaciones con uso intenso del ancho de banda con soporte para conexiones virtuales, segmentación y reensamblaje basados en hardware, y AAL5
- 3Com ofrece una variedad de tarjetas de red ATM para PCs y estaciones de trabajo para redes con la plataforma CoreBuilder 5000 y las redes CELLplex® 4000 Switch; estas tarjetas soportan velocidades de datos de 25 Mbps y 100 Mbps en diferentes tipos de bus de cliente

CAPÍTULO 20

Conmutación LAN

ANTECEDENTES

Un switch LAN es un dispositivo que presenta una densidad de puertos mucho mayor, a un costo más bajo que los puentes tradicionales. Por esta razón, los switches LAN pueden dar cabida a diseños de red que tengan un menor número de usuarios por segmento, incrementando así el ancho de banda promedio disponible por usuario. En este capítulo se presenta un resumen de la operación general del switch LAN y se mapea la conmutación LAN con el modelo de referencia OSI.

A la tendencia hacia un menor número de usuarios por segmento se le conoce como *microsegmentación*. Ésta permite la creación de segmentos privados o dedicados, esto es, un usuario por segmento. Cada usuario recibe acceso instantáneo a todo el ancho de banda y no tiene que luchar con otros usuarios por el uso del ancho de banda disponible. Como resultado, no se presentan colisiones (un fenómeno normal en las redes de medio compartido que emplean concentradores). Un switch LAN envía las tramas con base en la dirección de la Capa 2 de la trama (switch LAN de la Capa 2) o, en algunos casos, la dirección de la Capa 3 de la trama (switch LAN multicapa). A un switch LAN también se le llama switch de tramas ya que envía tramas de la Capa 2, en tanto que un switch ATM envía celdas. Aunque los switches LAN Ethernet son los más comunes, los switches Token Ring y FDDI LAN son cada vez más importantes a medida que aumenta el uso de la red.

La figura 20-1 muestra un switch LAN que ofrece un ancho de banda dedicado a los dispositivos y muestra la relación de la conmutación LAN de la Capa 2 con la capa de enlace de datos de la OSI:

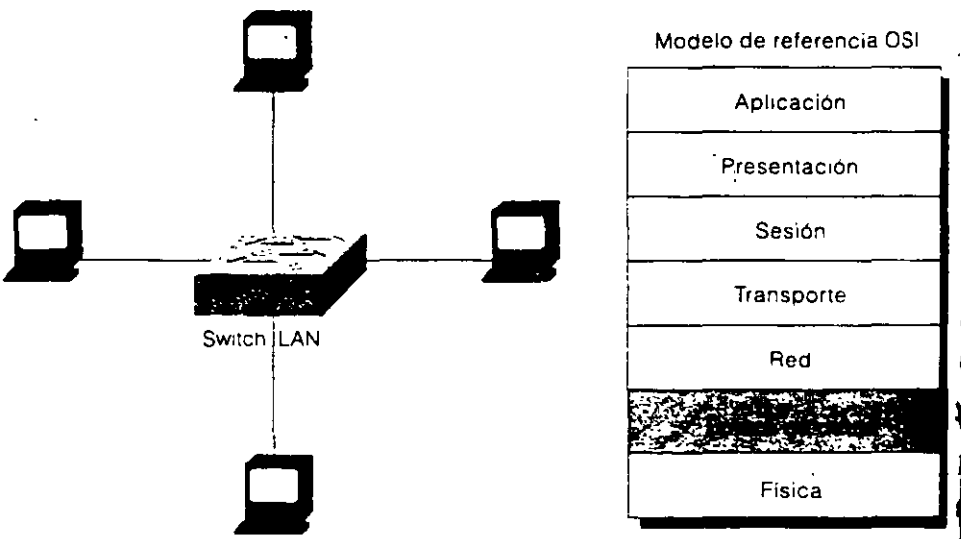


Figura 20–1
Un switch LAN es un dispositivo de la capa de enlace de datos.

Historia

Los primeros switches LAN fueron desarrollados en 1990. Eran dispositivos de la Capa 2 dedicados a resolver problemas de ancho de banda. Los más recientes están evolucionando hacia dispositivos multicapa capaces de manejar los problemas de protocolo asociados a las aplicaciones de gran ancho de banda que, históricamente, han sido resueltos por los ruteadores. En la actualidad, los switches LAN se están utilizando para reemplazar a los concentradores en el gabinete de cableado, ya que las aplicaciones de usuario están demandando un mayor ancho de banda.

Operación del switch LAN

Los switches LAN son similares a los puentes transparentes en cuanto a funciones como el aprendizaje de topología, el envío y el filtrado. Estos switches

También soportan algunas características únicas y novedosas, como la comunicación dedicada entre dispositivos, la comunicación simultánea múltiple, la comunicación dúplex total y la adaptación a la tasa del medio de transmisión.

Con la comunicación dedicada libre de colisiones entre los dispositivos de red, aumenta el rendimiento efectivo total de la transferencia de archivos. Por medio del envío o conmutación de varios paquetes al mismo tiempo, pueden ocurrir múltiples conversaciones simultáneas, lo que incrementa la capacidad de conversaciones soportadas en la red. Con la comunicación dúplex total se duplica efectivamente el rendimiento total, en tanto que con la adaptación a la tasa del medio de transmisión, el switch LAN puede traducir entre 10 y 100 Mbps, lo que permite que el ancho de banda se ofrezca conforme se vaya necesitando.

Para que los switches LAN se puedan usar no es necesario hacer cambios en los concentradores existentes, ni en las NICs (Tarjetas de Interfase de Red) ni en el cableado.

Reenvío en la conmutación LAN

Los switches LAN se pueden caracterizar por el método de reenvío que soportan. En el método de conmutación almacenar y enviar se verifican los errores y se eliminan las tramas erróneas. En el método de conmutación rápida de paquetes, la latencia se reduce eliminando la verificación de errores.

Con el método de conmutación almacenar y enviar, el switch LAN copia toda la trama en sus memorias de almacenamiento que están sobre la propia tarjeta y calcula la CRC (Verificación de la Redundancia Cíclica). La trama se elimina si contiene un error en la CRC o si es un *enano* (menos de 64 bytes incluyendo la CRC) o un *gigante* (más de 1518 bytes incluyendo la CRC). Si la trama no contiene ningún error, el switch LAN mira la dirección destino en su tabla de conmutación o de envío y determina la interfase de salida. Después, envía la trama hacia su destino.

Con el método de conmutación rápida de paquetes, el switch LAN copia solamente la dirección destino (los primeros 6 bytes que siguen al preámbulo) en las memorias de almacenamiento sobre la misma tarjeta. Posteriormente, mira

la dirección destino en su tabla de conmutación, determina la interfase de salida y envía la trama hacia su destino. Un switch que utiliza la conmutación rápida presenta una latencia muy pequeña ya que empieza a enviar la trama tan pronto como lee la dirección destino y determina la interfase de salida.

Algunos switches se pueden configurar para que desempeñen la conmutación rápida puerto por puerto hasta alcanzar un umbral de error definido por el usuario; en ese momento, los switches cambiarán automáticamente al modo almacenar y enviar. Cuando la tasa de errores queda por debajo del umbral, el puerto cambia automáticamente de nuevo al modo almacenar y enviar.

Ancho de banda de la conmutación LAN

Los switches LAN también pueden ser caracterizados de acuerdo con la proporción de ancho de banda que se asigne a cada puerto. La conmutación simétrica ofrece una distribución equitativa del ancho de banda a cada puerto, en tanto que la conmutación asimétrica presenta una distribución diferente, o desigual del ancho de banda entre algunos puertos.

Un switch LAN asimétrico ofrece conexiones conmutadas entre puertos con diferente ancho de banda, como en el caso de combinaciones 10BaseT y 100BaseT. A este tipo de conmutación también se le llama *conmutación 10/100*. La conmutación asimétrica está optimizada para flujos de tráfico cliente servidor donde varios clientes se comunican con un servidor al mismo tiempo, lo que requiere más ancho de banda dedicado al puerto del servidor para evitar ahí un cuello de botella.

Un switch simétrico presenta conexiones conmutadas entre puertos con el mismo ancho de banda, como todos los 10BaseT y 100BaseT. La conmutación simétrica se optimiza para una carga de tráfico distribuida de manera razonable como sucede en un ambiente de escritorio entre equivalentes.

Un administrador de red debe evaluar la cantidad de ancho de banda que necesita para las conexiones entre dispositivos, para acomodar el flujo de datos de aplicaciones de red cuando decida seleccionar un switch asimétrico o simétrico

EL SWITCH LAN Y EL MODELO DE REFERENCIA OSI

Los switches LAN se categorizan de acuerdo con la capa OSI en la que filtran o envían o conmutan las tramas. Estas categorías son: Características de la Capa 2, de la Capa 2 con la Capa 3 o multicapa.

Un switch LAN de la Capa 2 es similar a un puente multipuerto desde el punto de vista operativo, pero tiene una capacidad mucho mayor y soporta muchas nuevas características, como la operación dúplex total. Un switch LAN de la Capa 2 desempeña conmutación y filtrado con base en la dirección MAC de la capa de enlace de datos de OSI (Capa 2). Como con los puentes, es completamente transparente a los protocolos de red y a las aplicaciones de usuario.

Un switch LAN de la Capa 2 con características de la Capa 3 puede tomar decisiones de conmutación con base en más información que solamente la dirección MAC de la Capa 2. Dicho switch debe incorporar algunas características de control del tráfico de la Capa 3, como la administración del tráfico de multidifusión y difusión, seguridad a través de listas de acceso y fragmentación IP.

Un switch multicapa toma decisiones de conmutación y filtrado con base en direcciones de la capa de enlace de datos de OSI (Capa 2) y direcciones de la capa de red de OSI (Capa 3). Este tipo de switch decide dinámicamente si conmutar (Capa 2) o rutear (Capa 3) el tráfico entrante. Un switch multicapa LAN conmuta un grupo de trabajo y rutea entre diferentes grupos de trabajo.

CAPÍTULO 17

X.25

ANTECEDENTES

X.25 es un estándar de protocolo del sector Estándares de la ITU-T (Unión Internacional de Telecomunicaciones) para las comunicaciones WAN, que define cómo se establecen y mantienen las conexiones entre los dispositivos de usuario y los dispositivos de red. Está diseñado para operar eficientemente sin tomar en cuenta el tipo de sistemas conectados a la red. En general se utiliza en las PSN (Redes de Conmutación de Paquetes) de los proveedores de servicios comunes, como las compañías telefónicas. A los suscriptores se les cobra según el uso que hagan de la red. El desarrollo del estándar X.25 fue iniciado por los proveedores de servicios en los años 70. En ese entonces, había una necesidad de protocolos WAN que pudieran ofrecer conectividad a través de las redes públicas de datos (las PDNs). En la actualidad, la ITU-T administra el X.25 como un estándar internacional. En este capítulo se estudian las funciones básicas y los componentes de X.25.

LA OPERACIÓN DEL PROTOCOLO Y LOS DISPOSITIVOS DE X.25

Los dispositivos de la red X.25 se pueden clasificar en tres categorías generales: DTE (Equipo Terminal de Datos), DCE (Equipo de Comunicación de Datos) y PSE (Intercambio de Conmutación de Paquetes). Los dispositivos del equipo terminal

de datos son sistemas terminales que se comunican a través de la red X.25. Por lo general son terminales, computadoras personales o anfitriones de red y están ubicados en las instalaciones de los suscriptores individuales. Los dispositivos que forman el equipo de comunicación de datos son dispositivos especiales de comunicaciones, como los módems y los switches de paquetes. Éstos ofrecen la interfase entre los dispositivos DTE y un PSE y, en general, se localizan en las instalaciones de la compañía que ofrece el servicio de transporte. Los PSEs son switches que componen el grueso de la red de la compañía de transporte. Los PSEs transfieren datos de un dispositivo DTE a otro a través de la PSN de X.25. La figura 17-1 muestra la relación entre los tres tipos de dispositivos de la red X.25.

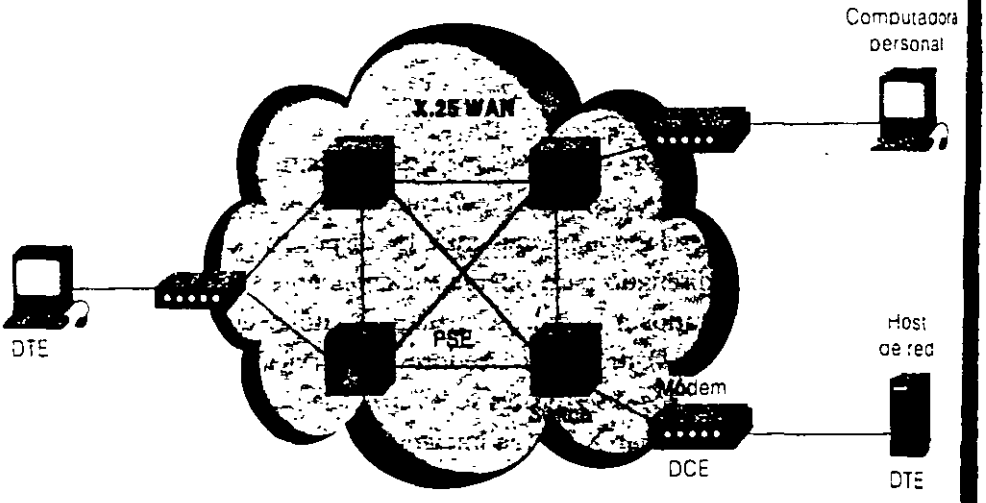


Figura 17–1
Los DTE, DCE y PSE conforman una red X.25.

Ensamblador/Desensamblador de Paquetes

PAD (Ensamblador/Desensamblador de Paquetes) es un dispositivo que comúnmente se encuentra en las redes X.25. Los PADs se utilizan cuando en un dispositivo DTE, por ejemplo una terminal en modo carácter, es muy fácil implementar la funcionalidad total de X.25. El PAD se ubica entre un dispositivo DTE y un dispositivo DCE, y desempeña tres funciones principales: el almacenamiento, el ensamblado y el desensamblado de paquetes. PAD almacena datos enviados

hacia o desde el dispositivo DTE. También ensambla datos salientes en paquetes y los envía al dispositivo DCE. (Esto incluye la adición de un encabezado de X.25); por último, el PAD desensambla los paquetes entrantes antes de enviar los datos hacia el DTE. (Esto incluye eliminar el encabezado X.25.) La figura 17-2 muestra la operación básica del PAD cuando se reciben paquetes de una WAN X.25.

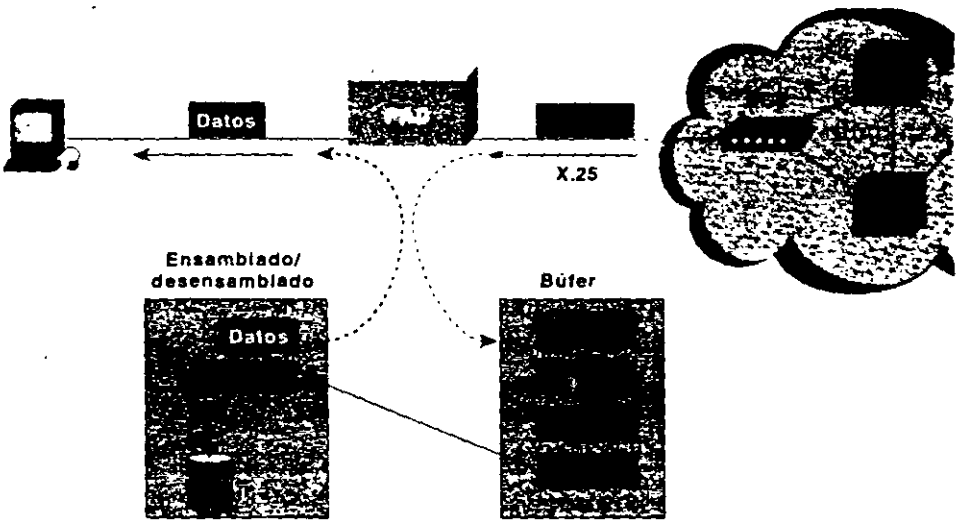


Figura 17-2
El PAD almacena, ensambla y desensambla los paquetes de datos.

Establecimiento de sesión en X.25

Las sesiones de X.25 se establecen cuando un dispositivo DTE se pone en contacto con otro para solicitar una sesión de comunicación. El dispositivo DTE que recibe la solicitud puede aceptar o rechazar la conexión. Si la solicitud es aceptada, los dos sistemas comienzan la transferencia de información dúplex total. Cualquiera de los dispositivos DTE puede finalizar la conexión. Una vez terminada la sesión, es necesario establecer una nueva sesión para cualquier comunicación adicional.

Circuitos virtuales X.25

Un circuito virtual es una conexión lógica creada para garantizar la comunicación confiable entre dos dispositivos de la red. Un circuito virtual denota la existencia de una trayectoria lógica bidireccional de un dispositivo DTE a otro a través de una red X.25. Físicamente, la conexión puede pasar por cualquier número de nodos intermedios, como dispositivos DTE y centrales de conmutación de paquetes. Los circuitos virtuales múltiples (conexiones lógicas) pueden ser multiplexados en un solo circuito físico (conexión física). Los circuitos virtuales se demultiplexan en el extremo remoto y los datos se envían a los destinos adecuados. La figura 17-3 muestra cuatro circuitos virtuales separados que se están multiplexando en un solo circuito físico.

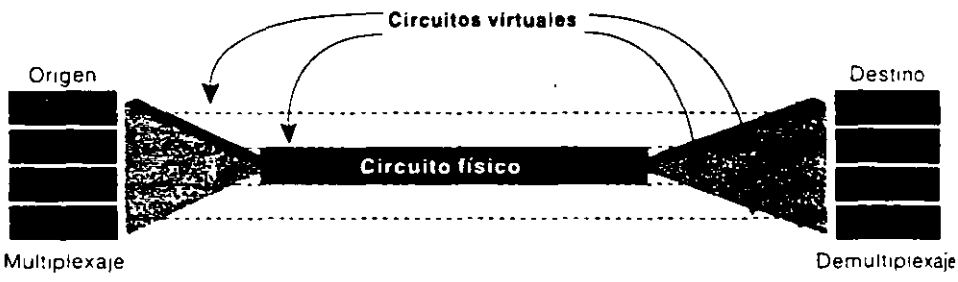


Figura 17–3 *Los circuitos virtuales pueden multiplexarse en un solo circuito físico.*

Hay dos tipos de circuitos virtuales X.25: conmutados y permanentes. Los SVCs (Circuitos Virtuales Conmutados) son conexiones temporales que se utilizan en las transferencias esporádicas de datos. Para que se establezcan es necesario que los dos dispositivos DTE establezcan, conserven y finalicen una sesión cada vez que los equipos necesiten comunicarse. Los PVCs (Circuitos Virtuales Permanentes) son conexiones establecidas de manera permanente, que se utilizan para transferencias de datos frecuentes y continuas, y no requieren que las sesiones se establezcan y finalicen. Por lo tanto, puesto que la sesión siempre está activa, los DTEs pueden comenzar a transferir datos en el momento que se requiera.

La operación básica de un circuito virtual X.25 empieza cuando el dispositivo DTE origen especifica el circuito virtual que se va a utilizar (en el encabezado

del paquete) y después envía el paquete a un dispositivo DCE conectado localmente. En este punto, el dispositivo DCE local analiza los encabezados del paquete para determinar qué circuito virtual debe utilizar y después manda los paquetes al PSE más cercano en la trayectoria de ese circuito virtual. Los PSE (switches) transfieren el tráfico al siguiente nodo intermedio en la trayectoria, que puede ser otro switch u otro dispositivo DCE remoto.

Cuando el tráfico llega al dispositivo DCE remoto, se analizan los encabezados de los paquetes y se determina la dirección de destino. Posteriormente, los paquetes se envían al dispositivo DTE destino. Si la comunicación se presenta a través de un SVC (Circuito Virtual Conmutado) y ningún dispositivo tiene más datos que transferir, el circuito virtual se da por terminado.

CONJUNTO DE PROTOCOLOS X.25

En el conjunto de protocolos X.25 se mapean las tres capas inferiores del modelo de referencia OSI. Por lo general, en las implementaciones X.25 se utilizan los protocolos siguientes: PLP (Protocolo de la Capa de Paquetes), LAPB (Procedimiento de Acceso al Enlace Balanceado) y, entre otras, varias interfases seriales de la capa física (como la EIA/TIA-232, EIA/TIA-449, EIA-530 y la G.703). En la figura 17-4 se mapean los protocolos X.25 más importantes con las capas del modelo de referencia OSI.

Protocolo PLP

PLP (*Protocolo de la Capa de Paquetes*) es el protocolo de la capa de red X.25 que administra el intercambio de paquetes entre los dispositivos DTE a través de circuitos virtuales. Los PLPs también pueden operar a través de implementaciones LLC2 (Control del Enlace Lógico 2) en las LANs y a través de interfases de la ISDN (Red Digital de Servicios Integrados) que corren el LAPD (Procedimiento de Acceso al Enlace sobre el canal D).

El PLP opera en cinco modos distintos: *establecimiento de la llamada, transferencia de datos, ocioso, liberación de la llamada* y *reinicio*.

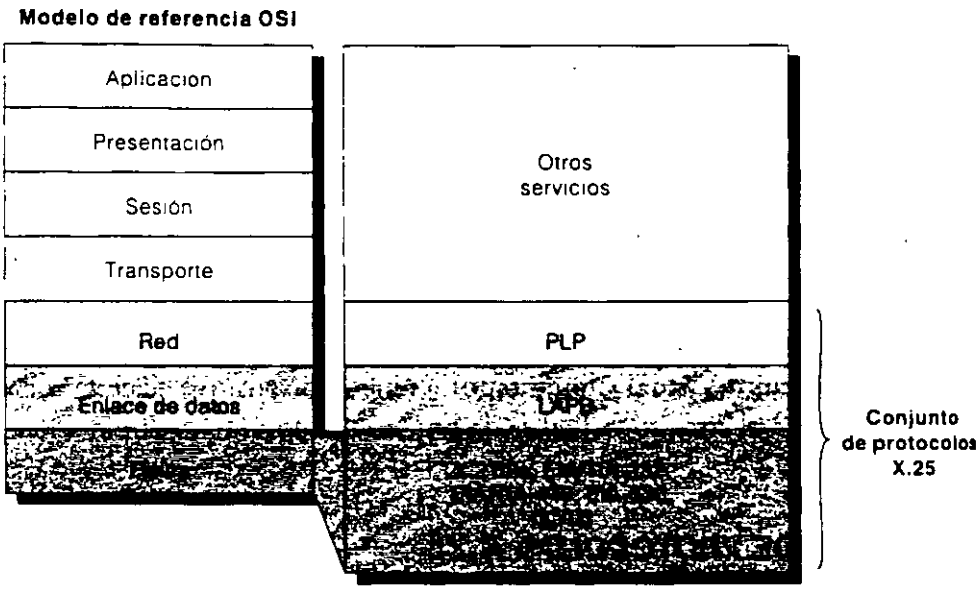


Figura 17–4 *Los protocolos clave de X.25 mapean las tres capas inferiores del modelo de referencia OSI.*

El modo de establecimiento de llamada se utiliza para establecer SVC entre dispositivos DTE. Un PLP utiliza el esquema de direccionamiento de X.121 para establecer el circuito virtual. Este modo es ejecutado en circuitos virtuales individuales, lo que significa que un circuito virtual puede estar en modo de establecimiento de llamada en tanto que otro está en el modo de transferencia de datos. Este modo sólo se utiliza con los SVCs, no con los PVCs.

El modo de transferencia de datos se utiliza para transferir datos entre dos dispositivos DTE a través de un circuito virtual. En este modo, el PLP maneja la segmentación y el reensamblado, el relleno con bits y el control de errores y de flujo. Este modo es ejecutado en circuitos virtuales individuales y se utiliza tanto con los PVCs como con los SVCs.

El modo de pausa se utiliza cuando se establece un circuito virtual pero no se presenta transferencia de datos. Es ejecutado en circuitos virtuales individuales y se utiliza solamente con los SVCs.

El modo de liberación de llamada se utiliza para finalizar sesiones de comunicación entre dispositivos DTE y para finalizar los SVCs. Este modo es ejecutado en circuitos virtuales individuales y se utiliza solamente con los SVCs.

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. Este capítulo se ocupa de las especificaciones y aplicaciones de Frame Relay en el contexto de los servicios WAN.

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 en 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 las 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 consorcio 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 de 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 ANSI (Instituto Nacional Americano de Estándares).

DISPOSITIVOS DE FRAME RELAY

Los dispositivos conectados a una WAN Frame Relay caen dentro de una 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.

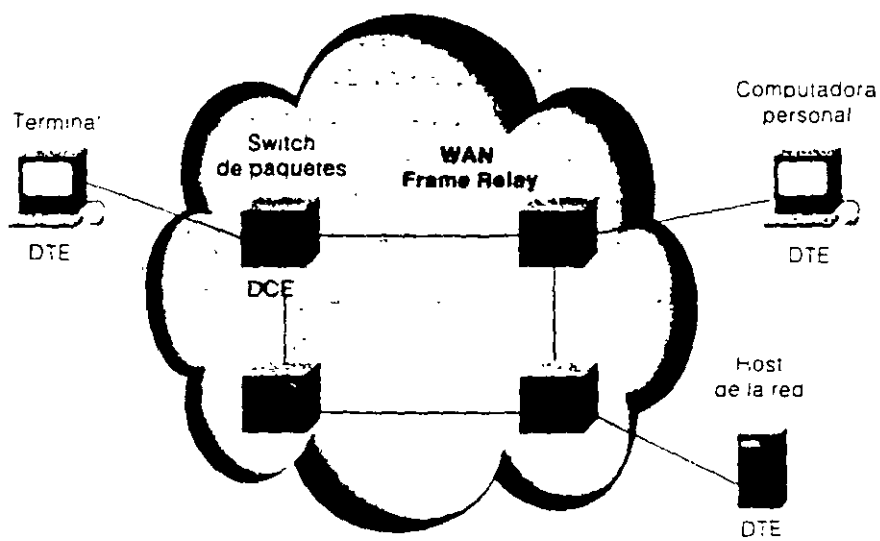


Figura 10–1
En general los DCE residen en las WAN, cuya operación está a cargo de una compañía de larga distancia.

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 este capítulo 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 implementa 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, poco 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 PVCs 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.

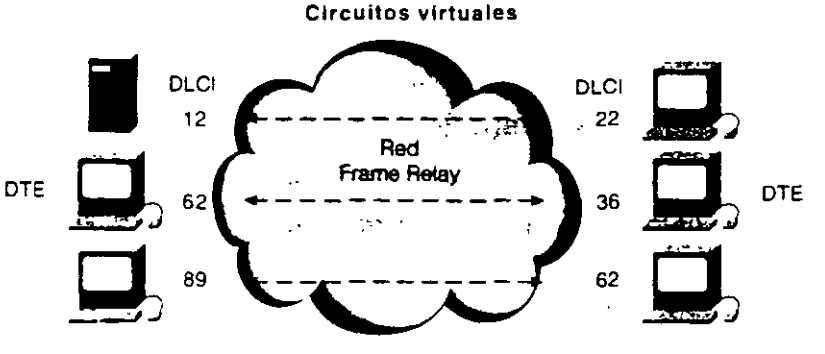


Figura 10–2
A un circuito virtual único Frame Relay se le pueden asignar diferentes DLCIs a cada extremo de un VC.

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 periodos 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 *extensiones*) 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 úni-

cas 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 Frame 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 56 K. En la figura 10-3 se muestra un ejemplo de una red simple Frame Relay.

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.

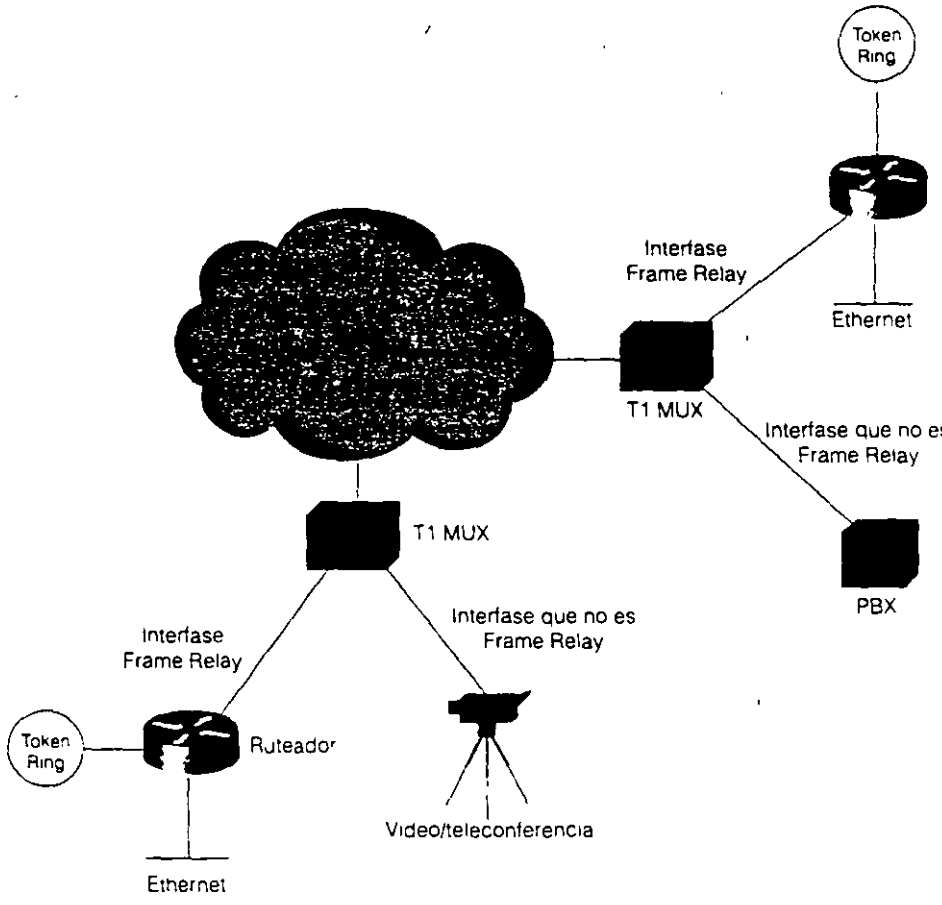


Figura 10–3
Una red sencilla Frame Relay conecta varios dispositivos a diferentes servicios a través de una red WAN.

En la sección siguiente se analizan 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 sucriptores 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 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.

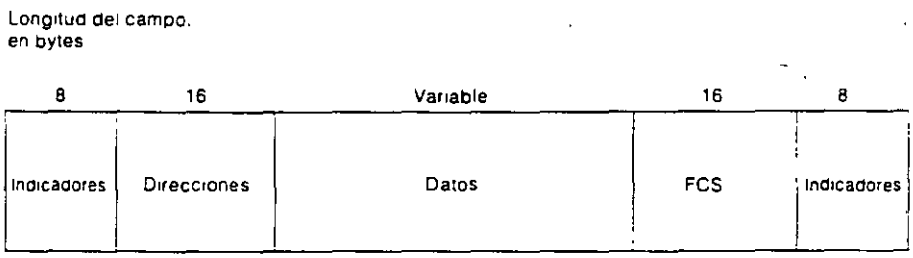


Figura 10–4 *La trama Frame Relay comprende cinco campos.*

- *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 dispositivo 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 Adelante) 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 el 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.

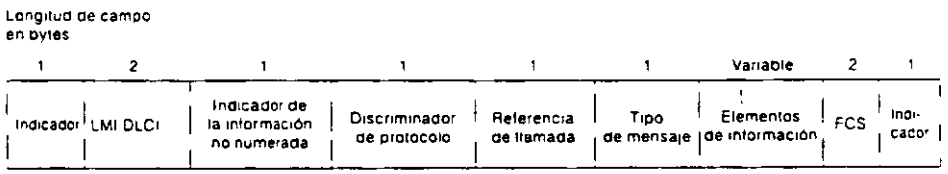


Figura 10–5 *El Frame Relay que constituye el formato LMI tiene nueve campos.*

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.

CAPÍTULO 18

Conmutación ATM

ANTECEDENTES

ATM (Modo de Transferencia Asíncrona) es un estándar de la ITU-T (Unión Internacional de Telecomunicaciones, Sector de Estándares en Telecomunicaciones), para la conmutación de celdas donde la información para múltiples tipos de servicios, como voz, video y los datos, se transporta en celdas pequeñas de tamaño fijo. El propósito de las celdas ATM es la conexión. Este capítulo presenta un resumen de los protocolos, servicios y operación de ATM. La figura 18-1 muestra una red ATM privada y una red ATM pública que transporta tráfico de voz, video y datos.

Estándares

ATM es producto de los esfuerzos del estándar de la BISDN (Red Digital de Servicios Integrados de Banda Ancha) de la ITU-T. Concebida originalmente como una tecnología de transporte a alta velocidad para voz, video y datos a través de redes públicas. El Foro de ATM amplió la visión de la ITU-T de ATM y planteó su uso en redes públicas y privadas. El Foro de ATM ha publicado trabajos en relación con las especificaciones siguientes:

- UNI (Interfase de Red de Usuario) 2.0
- UNI 3.0

- UNI 3.1
- P-NNI (Interfase de Nodo de la Red Pública)
- LANE (Emulación de LAN)

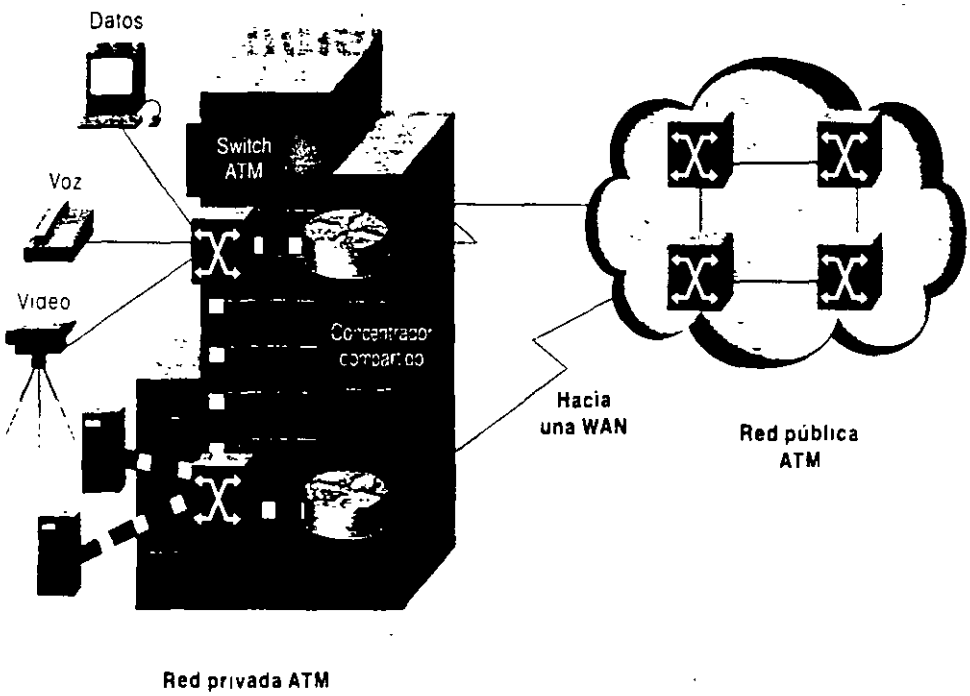


Figura 18–1
Una red privada ATM y una red pública ATM pueden transportar voz, video y tráfico de datos.

DISPOSITIVOS ATM Y ENTORNO DE RED

ATM es una tecnología de conmutación de celdas y multiplexaje que reúne los beneficios de la conmutación de circuitos (garantizado: capacidad y retardo de transmisión constante) con los de la conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Proporciona un ancho de banda expandible desde algunos megabits por segundo (Mbps) hasta muchos gigabits por segundo (Gbps). Debido a su naturaleza asíncrona, ATM es más eficiente que las tecnologías síncronas como el TDM (*Multiplexaje por División de Tiempo*).

Con TDM, los usuarios son asignados a ranuras de tiempo, y ninguna otra estación puede enviar información en esa ranura de tiempo. Si una estación tiene muchos datos que enviar, lo puede hacer solamente cuando se presenta su ranura de tiempo, aunque todas las demás ranuras estén vacías. Por otro lado, si una estación no tiene información que enviar cuando se presente su ranura de tiempo asignada, dicha ranura de tiempo se manda vacía y, por lo tanto, se desperdicia. Como ATM es asíncrona, las ranuras de tiempo están disponibles bajo demanda, y hay información en el encabezado de cada celda ATM que identifica el origen de la transmisión.

Formato básico de la celda ATM

ATM transfiere la información a través de unidades de tamaño fijo llamadas *celdas*. Cada celda consta de 53 octetos o bytes. Los primeros 5 bytes contienen información del encabezado de la celda y los 48 bytes restantes contienen la "carga útil" (la información del usuario). Las celdas pequeñas de tamaño fijo son muy adecuadas para la transferencia de tráfico de voz y video, ya que dicho tráfico no tolera los retardos que surgen por tener que esperar a que un paquete grande de datos descargue su información, entre otras cosas. La figura 18-2 muestra el formato básico de una celda ATM.

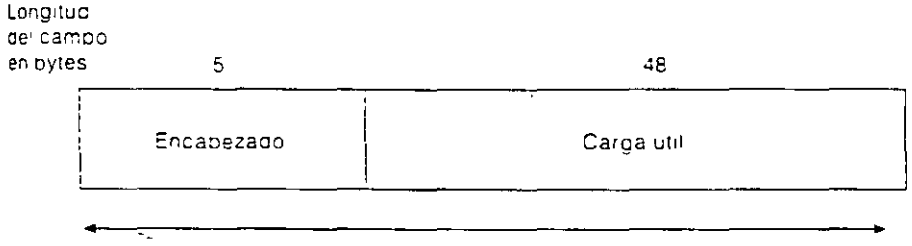


Figura 18–2 *Una celda ATM consta de un encabezado e información el usuario.*

Dispositivos ATM

Una *red* ATM está formada por un *switch* ATM y *puntos terminales* de ATM. Un switch ATM es responsable del transporte de celdas a través de una red ATM. El trabajo de un switch ATM está bien definido: Acepta la celda entrante de un punto terminal de ATM u otro switch ATM. Posteriormente, lee y actualiza la información contenida en el encabezado de la celda y, rápidamente, conmuta

la celda a una interfase de salida para enviarla a su destino. Un punto terminal de ATM (o sistema terminal) contiene un adaptador de interfase de red ATM. Algunos ejemplos de puntos terminales de ATM son las estaciones de trabajo, los ruteadores y las DSU (Unidades de Datos de Servicio), los switches LAN y los CODECs (Codificadores Decodificadores de Video). La figura 18-3 muestra una red ATM formada por switches ATM y puntos terminales de ATM.

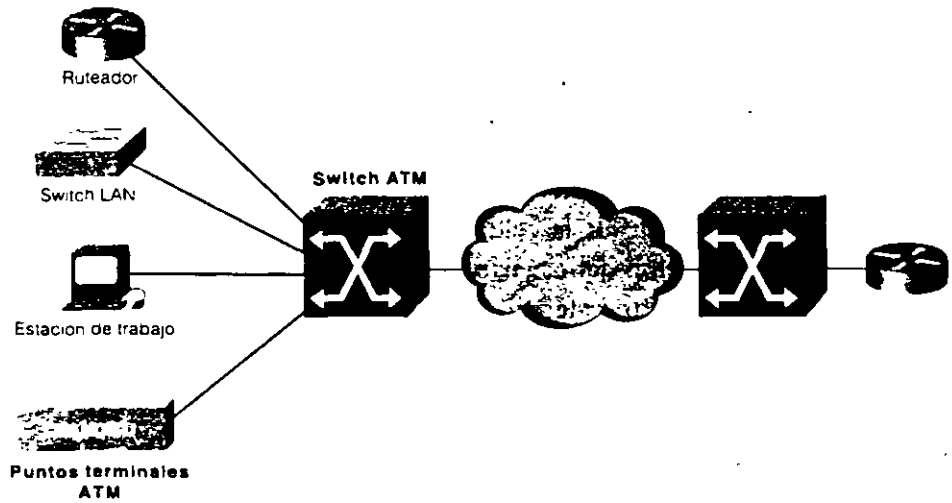


Figura 18–3 *Una red ATM está formada por switches ATM y puntos terminales.*

Interfases de red ATM

Una red ATM consta de un conjunto de switches ATM interconectados a través de enlaces o interfases punto a punto de ATM. Los switches ATM soportan dos tipos principales de interfases: la *UNI* (*Interfase de Red de Usuario*) y la *NNI* (*Interfase de nodo de red*). La UNI conecta los sistemas terminales de ATM (como los anfitriones y ruteadores) hacia un switch ATM. La NNI conecta dos switches ATM.

Si el switch es propiedad del cliente y está ubicado en sus instalaciones o es propiedad pública y es operado por una compañía telefónica, la UNI y la NNI se pueden subdividir en UNI y NNI públicas o privadas. Una UNI privada conecta un punto terminal de ATM y un switch ATM privado. Su equivalente públic

```
// Chaining message handlers
//////////
```

conecta un punto terminal de ATM o un switch privado con un switch público. Una NNI privada conecta dos switches ATM dentro de la misma organización privada. Una NNI pública conecta dos switches ATM dentro de la misma organización pública.

Una especificación adicional, la B-ICI (*Interconexión de Intercambio entre Prestadores de servicio en Banda Ancha*), conecta dos switches públicos de diferentes proveedores de servicio. La figura 18-4 muestra las especificaciones de la interfase ATM para las redes públicas y privadas.

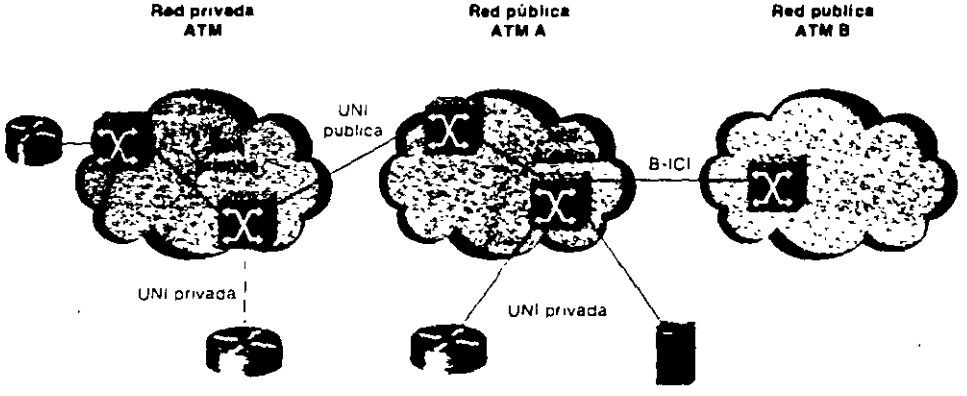


Figura 18–4 *Las especificaciones de la interfase ATM difieren para las redes públicas y privadas.*

FORMATO DEL ENCABEZADO DE CELDA ATM

Un encabezado de celda ATM puede tener uno de dos formatos: *UNI* o *NNI*. El encabezado UNI se utiliza para la comunicación entre puntos terminales de ATM y switches ATM en las redes ATM privadas. El encabezado NNI se utiliza para la comunicación entre switches ATM. La figura 18-5 describe el formato básico de celda ATM, el formato del encabezado UNI y el del encabezado NNI de la celda ATM.

A diferencia del encabezado UNI, el encabezado NNI no incluye el campo GFC (Control de Flujo Genérico). Además, el encabezado NNI tiene un VPI (Identificador de Trayectoria Virtual) que ocupa los primeros 12 bits, y permite que haya troncales más grandes entre switches públicos ATM.

```
// CMainFrame message handlers
//////////
```

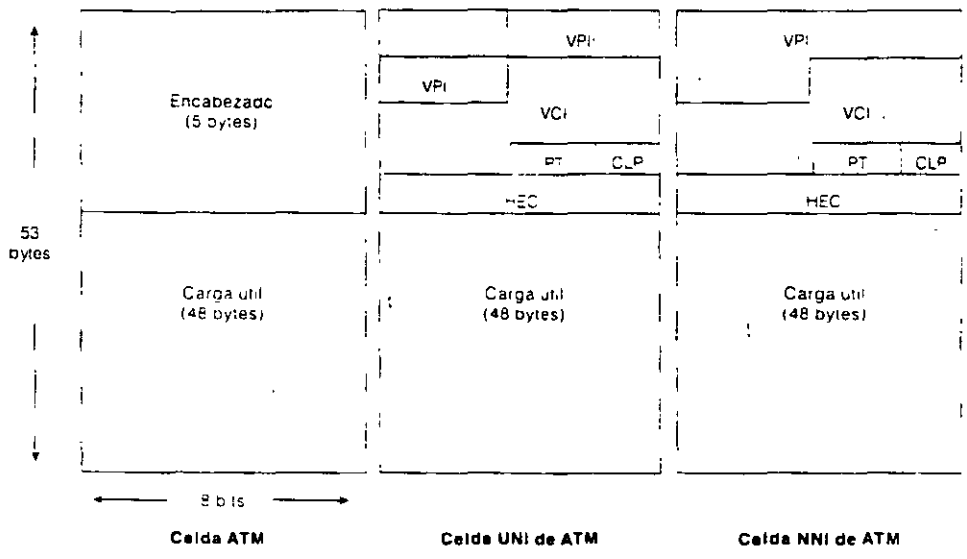


Figura 18–5 *Las celdas ATM, UNI de ATM y NNI de ATM contienen, cada una, una "carga útil" de 48 bytes.*

Campos del encabezado de la celda ATM

Además de los campos del encabezado de GFC y VPI, se utilizan otros campos del encabezado de la celda ATM. Las descripciones siguientes se refieren a los campos del encabezado de la celda ATM que se muestran en la figura 18-5:

- *GFC* (*Control de Flujo Genérico*) — Proporciona funciones locales como la identificación de múltiples estaciones que comparten una sola interfase de ATM. En general este campo no se utiliza y se fija en su valor predeterminado.
- *VPI* (*Identificador de Trayectoria Virtual*) — En conjunto con el VCI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en camino hacia su destino.
- *VCI* (*Identificador del Canal Virtual*) — En conjunto con el VPI, identifica el siguiente destino de una celda conforme ésta pasa a través de una serie de switches ATM en ruta a su destino.

- *PT* (*Tipo de Carga Útil*) — Indica en el primer bit si la celda contiene datos del usuario o datos de control. Si la celda contiene datos del usuario, el segundo bit indica si hay saturación y el tercer bit indica si la celda es la última de una serie de celdas que representan una sola trama AAL5.
- *CLP* (*Prioridad de Pérdida de Saturación*) — Indica si la celda se debiera eliminar al encontrar un alto grado de saturación a su paso por la red. Si el bit CLP es igual a 1, la celda se deberá eliminar para dar preferencia a las celdas cuyo bit CLP sea igual a cero.
- *HEC* (*Control de Errores del Encabezado*) — Calcula la suma de verificación sólo en el encabezado mismo.

SERVICIOS ATM

Hay tres tipos de servicios en ATM: PVC (*Conexiones Virtuales Permanentes*), SVC (*Conexiones Virtuales Conmutadas*) y *servicio sin conexión* (muy parecido a SMDS).

Una PVC permite la conectividad directa entre sitios. De esta forma, una PVC es similar a una línea privada. Una de las ventajas de una PVC es que garantiza la disponibilidad de una conexión y no requiere los procedimientos asociados con el establecimiento de llamada entre switches. Las desventajas de lass PVCs son, entre otras, la conectividad estática y el establecimiento manual.

Una SVC se genera y libera dinámicamente y permanece en uso sólo mientras se lleva a cabo la transferencia de datos. En este sentido, es similar a una llamada telefónica. El control dinámico de la llamada requiere un protocolo de señalización entre el punto terminal de ATM y el switch ATM. Entre las ventajas de las SVCs se cuentan la flexibilidad de la conexión y el establecimiento de llamada que puede manejarse automáticamente por medio de un dispositivo de red. Algunas desventajas son el tiempo extra y el gasto indirecto que se requiere para establecer la conexión.

CONEXIONES ATM

ATM soporta dos tipos de conexiones: punto a punto y punto a multipunto.

Las conexiones punto a punto conectan dos sistemas terminales de ATM y pueden ser unidireccionales (comunicación solamente en una dirección) o bidireccionales (comunicación en ambas direcciones). Las conexiones punto a multipunto conectan un sistema terminal de un solo origen (conocido como nodo raíz) hacia múltiples terminales de destino (conocidas como hojas). Dichas conexiones son solamente unidireccionales. Los nodos raíz pueden transmitir hacia las hojas, sin embargo, las hojas no pueden transmitir hacia la raíz o entre ellas en la misma conexión. La duplicación de celdas se lleva a cabo dentro de la red ATM a través de los switches ATM, donde las conexión se divide en dos o más ramas.

Algo muy útil sería que las redes ATM tuvieran conexiones multipunto a multipunto bidireccionales. Dichas conexiones son análogas a las características de multidifusión y de difusión de las LANs de medio de transmisión compartido como Ethernet y Token Ring. La característica de difusion es fácil de implementar en las LANs de medio compartido, donde todos los nodos conectados a un solo segmento de LAN deben procesar todos los paquetes que se envían a través de ese segmento. Desafortunadamente, una característica multipunto a multipunto no se puede implementar utilizando AAL5, que es la AAL (Capa de Adaptación ATM) más común para transmitir datos a través de la red ATM. A diferencia de la AAL3/4, con su campo MID (Identificador de Mensajes), la AAL5 no ofrece un modo dentro de su formato de celda de entrelazar celdas de diferentes paquetes AAL5 en una sola conexión. Esto significa que todos los paquetes AAL5 enviados hacia un destino particular a través de una conexión particular se deben recibir en secuencia; de otra forma, el proceso de reensamblado del destino no podrá reconstruir los paquetes. Ésta es la razón por la que las conexiones punto a multipunto de la AAL5 de ATM sólo pueden ser unidireccionales. Si un nodo de hoja transmitiera un paquete AAL5 en la conexión, por ejemplo, sería recibido por el nodo raíz y por todos los demás nodos hoja. En estos nodos, el paquete enviado por la hoja puede estar entrelazado con los paquetes enviados por la raíz y, posiblemente, por otros nodos hoja, impidiendo el reensamblado de cualquiera de los paquetes entrelazados.

CAPÍTULO 45

Monitoreo remoto

ANTECEDENTES

RMON (*Monitoreo Remoto*) es una especificación de monitoreo estándar que permite que varios monitores de red y sistemas de consola intercambien datos sobre el monitoreo de la red. RMON ofrece a los administradores de red mayor libertad al seleccionar sensores y consolas para el monitoreo de red con características que satisfagan sus necesidades particulares de conectividad. Este capítulo presenta un breve panorama de la especificación RMON, enfocándose en los grupos RMON.

La especificación RMON define un conjunto de estadísticas y funciones que se pueden intercambiar entre los administradores de consola que cumplen con RMON y los sensores de red. Como tales, el RMON proporciona a los administradores de red información muy completa acerca del diagnóstico de fallas de red, planeación y puesta a tono del sistema.

RMON fue definido por la comunidad de usuarios con ayuda de IETF (Fuerza de Trabajo de Ingeniería de Internet). En 1992 se convirtió en un estándar propuesto como RFC 1271 (para Ethernet). Después, en 1995, pasó a ser un estándar en borrador como el RFC 1757, con lo cual el RFC 1271 se hizo obsoleto.

La figura 45-1 muestra un sensor RMON capaz de monitorear un segmento Ethernet y transmitir información estadística de regreso a la consola para RMON.

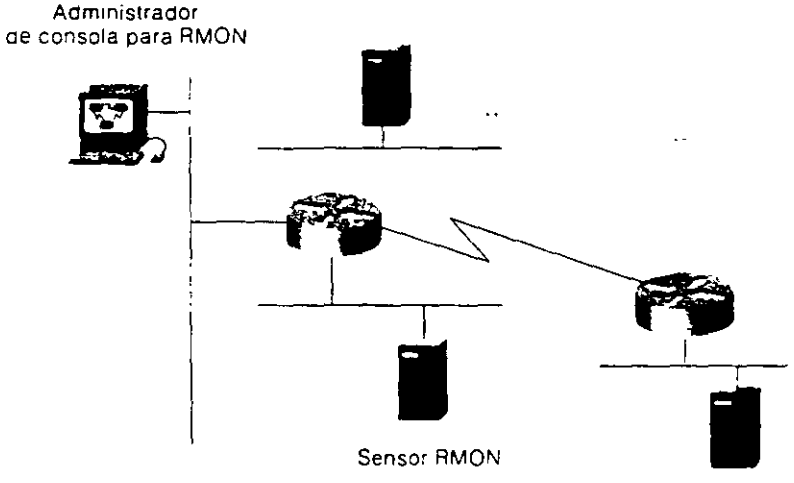


Figura 45-1
El sensor RMON puede enviar información estadística a una consola RMON.

GRUPOS RMON

RMON entrega información en nueve *grupos* RMON de elementos de monitoreo; cada uno de ellos proporciona conjuntos específicos de datos para cumplir con los requerimientos comunes de monitoreo de la red. Cada grupo es opcional, por lo que los proveedores no necesitan soportar todos los grupos dentro de una MIB (Base de Información de Administración). Algunos grupos RMON necesitan soporte de otros grupos RMON para funcionar adecuadamente. La tabla 45-1 muestra los nueve grupos de monitoreo especificados en el RFC 1757 Ethernet RMON MIB.

Tabla 45-2 *Grupos de monitoreo de RMON.*

ON	Función	Elementos
ıs	Contiene estadísticas tomadas por el sensor de cada interfase monitoreada en este dispositivo.	Paquetes eliminados, paquetes enviados, bytes enviados (octetos), paquetes de difusión, paquetes multidifundidos, errores de CRC, enanos, gigantes, fragmentos, parlanchines, colisiones y contadores de paquetes que van de 64-128, 128-256, 256-512, 512-1024 y 1024-1518 bytes.
	Periódicamente toma muestras estadísticas de una red y las guarda para utilizarlas más adelante.	Periodo de muestra, número de muestras, artículos muestreados.
	Cada cierto tiempo toma muestras estadísticas de las variables en el sensor y las compara con los niveles previamente configurados. Si la variable monitoreada cruza un umbral, se genera un evento.	Incluye la tabla de alarmas y requiere la implementación del grupo de eventos. Tipo de alarma, intervalo, umbral de comienzo y umbral de final.
	Contiene estadísticas asociadas con cada anfitrión descubierto en la red.	Las direcciones de anfitriones, paquetes y bytes recibidos y transmitidos, así como los paquetes de difusión, multidifundidos y de error.
J	Prepara tablas que describen a los anfitriones que están al principio de la lista ordenada por una de sus estadísticas. Las estadísticas disponibles son muestras de una de sus estadísticas base en un intervalo especificado por la estación de administración; por lo tanto, estas estadísticas se basan en la tasa.	Estadísticas, host(s), periodos de inicio y final de las muestras, tasa base, duración.
	Almacena estadísticas de conversaciones entre conjuntos de dos direcciones. A medida que el dispositivo detecta una nueva conversación, crea un nuevo parámetro en su tabla.	Pares de direcciones origen y destino, y paquetes, bytes y errores por cada par.

Continúa

Tabla 45–2 *Continuación*

RMON Grupo	Función	Elementos
Filtros	Permiten la comparación de los paquetes a una ecuación de filtro. Estos paquetes comparados forman una ráfaga de datos que se debe capturar o generar nuevos eventos.	Tipo de filtro bit (con o sin máscara), expresión del filtro (nivel de bit), expresión condicional (y, o, no) hacia otros filtros.
Captura de paquetes	Permite la captura de paquetes después de que han fluido a través de un canal.	Tamaño del búfer para los paquetes capturados, status total (alarma), número de paquetes capturados.
Eventos	Controla la generación y notificación de eventos de este dispositivo.	Tipo de evento, descripción, última vez que se envió el evento.

CAPÍTULO 46

Protocolo SNMP

ANTECEDENTES

SNMP (Protocolo Simple de Administración de Red) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte del conjunto de protocolos TCP/IP (Protocolo de Control de la Transmisión/Protocolo Internet). SNMP hace posible que los administradores de red administren el desempeño de la misma, encuentren y resuelvan problemas en ella y planeen su crecimiento.

Hay dos versiones de SNMP: SNMPv1 (Versión 1 de SNMP) y SNMPv2 (Versión 2 de SNMP). Ambas tienen una serie de características comunes; sin embargo, SNMPv2 presenta mejoras, como las operaciones adicionales de protocolos. La estandarización de otra versión del SNMP, el SNMPv3 (Versión 3 de SNM), está pendiente. En este capítulo se describen las operaciones de los protocolos SNMPv1 y SNMPv2. La figura 46-1 muestra una red básica administrada por el protocolo SNMP.

El comando de captura es utilizado por los dispositivos administrados para reportar eventos al NMS de manera asíncrona. Cuando se presenta determinado tipo de eventos, un dispositivo administrado envía una captura a NMS.

NMS utiliza las operaciones transversales para determinar qué variables soporta un dispositivo administrado y reunir secuencialmente información en tablas de variables, como sería una tabla de ruteo.

MIB DE SNMP

MIB (*Base de Información de Administración*) es la información organizada de manera jerárquica. Los MIBs se accesan por medio de un protocolo de administración de la red como SNMP. Se componen de objetos administrados y son identificados por identificadores de objetos.

Un objeto administrado (a menudo llamado objeto MIB, un objeto o un MIB) es una de las características específicas de un dispositivo administrado. Los objetos administrados se componen de una o más instancias de objetos, esencialmente variables.

Hay dos tipos de objetos administrados: *escalares* y *tabulares*. Los objetos escalares definen una sola instancia del objeto. Los objetos tabulares definen múltiples instancias de objetos relacionados que están agrupados en tablas MIB.

Un ejemplo de objeto administrado es *atInput*, que es un objeto escalar que contiene una sola instancia de objetos, el valor entero que indica el total de paquetes AppleTalk de entrada en una interfase del ruteador.

Un identificador de objetos (o ID del objeto) identifica de manera única un objeto administrado en la jerarquía del MIB. La jerarquía del MIB puede ser descrita como un árbol con una raíz sin nombre, cuyos niveles son asignados por diferentes organizaciones. La figura 46-3 muestra el árbol MIB.

Los IDs de objetos de alto nivel en MIB pertenecen a las diferentes organizaciones de estándares, en tanto que los IDs de objetos de nivel inferior son asignados por organizaciones asociadas.

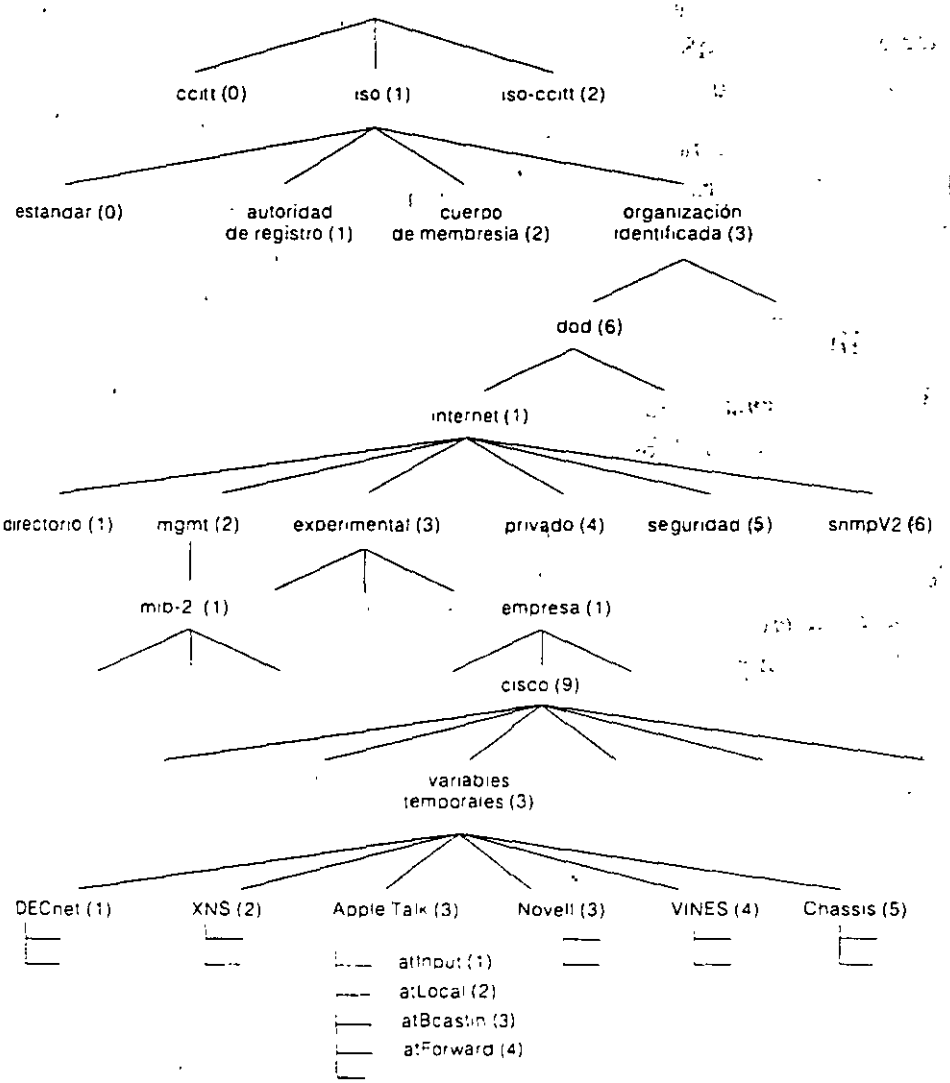


Figura 46–3
El árbol MIB muestra las diferentes jerarquías asignadas por diversas organizaciones.

Los proveedores pueden definir ramificaciones privadas que incluyan objetos administrados para sus propios productos. En general, los MIBs que no han sido estandarizados están ubicados en la rama experimental.