UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

" TELEFONIA DIGITAL Y RDSI
DISPOSITIVOS PARA LA TRANSMISION DE DATOS

TRABAJO DE SEMINARIO

QUE PARA OBTENER EL TITULO DE

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

CARLOS EMMANUEL GUTIERREZ ALANIS

ASESOR: ING. JOSE LUIS BARBOSA PACHECO

CUAUTITLAN IZCALLI, EDO. DE MEXICO JUNIO 2003

A

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS SUPERIORES-CUAUTITLAN
DEPARTAMENTO DE EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario:

Telefonía Digital y RDSI

"Dispositivos para la transmisión de datos"

que presenta el pasante: Carlos Emmanuel Gutierrez Alanis
con número de cuenta: 8560516-3 para obtener el título de :
Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXÁMEN PROFESIONAL correspondiente, otorgamos nuestro **VISTO BUENO**.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 18 de Junio de 2003.

MODULO	PROFESOR	FIRMA
1	Ing. José Luis Rivera López	
2	Ing. José Luis Barbosa Pacheco	
3	Ing. Victor Hugo Arroyo Hernández	

B

Dedicatorias

A mis Padres
Porque con su ejemplo, apoyo y amor incondicional logré alcanzar este sueño tan anhelado. Los amo.

A mis Hermanos
Porque sin su amor no podría haber logrado nada en la vida.

A Silvia
Porque con tú motivación y apoyo logré concluir este proyecto. Pero sobretodo porque sin ti no habría tenido sentido hacerlo. Te adoro.

A Carlitos y Silvita
Porque al mirarlos lloro hasta con las canciones de Molotov. Porque desde que llegaron a mi vida lucho incansablemente por convertirme en una mejor persona, alguien de quien puedan sentirse orgullosos.

Índice

Prólogo

Las redes de telecomunicaciones globales son el más grande y complejo sistema tecnológico que el hombre ha creado. Son también una parte fundamental de la infraestructura de las naciones y es un factor vital para el desarrollo de las mismas.

En los últimos años, el desarrollo en el campo de las telecomunicaciones ha evolucionado rápidamente. Dicho desarrollo ha establecido nuevas demandas de conocimientos y competencias para todo el mundo que tiene una participación activa en las telecomunicaciones modernas.

Para entender la estructura de las redes de telecomunicaciones es fundamental entender las demandas que los servicios básicos representan en la red. La transmisión de voz, datos y video pertenecen a esta categoría de servicios. Desde el punto de vista del servicio de voz, podemos decir que la red telefónica es equivalente a un traje hecho a la medida para proveer servicio telefónico a un costo razonable.

El extraordinario desarrollo en el campo de las telecomunicaciones se ha caracterizado por la integración de la red telefónica con otras redes que ofrecen servicios de datos y video. Este fenómeno se debe, en gran medida, a la creciente demanda de servicios de comunicación de datos que son, en comparación con la telefonía tradicional, mucho más variables y dinámicos. En este sentido, un campo que sin duda tendrá un crecimiento importante en el futuro inmediato, es el relacionado con los servicios multimedia, particularmente video en demanda y en línea. Prueba de ello son los servicios de video en línea a través de redes móviles, que en la actualidad están siendo utilizados por las grandes cadenas televisoras para cubrir noticias o sucesos que por razones de oportunidad, distancia o costo no podrían haber sido transmitidas en tiempo real.

La integración de redes significa que los servicios de voz, datos y video (TV por cable), que en la actualidad corren por redes independientes, podrán proveerse a través de una única red, basada en paquetes o celdas, de forma indistinta, garantizando los niveles de seguridad, retardo e integridad de la información que cada uno de los servicios demande. Por esta razón los operadores telefónicos están encaminando la evolución de sus redes (voz y datos) hacia la conformación de una sola y enorme red que integrará tantos servicios como sea posible, optimizando el uso de sus recursos e incrementando notablemente sus utilidades. Sin embargo, en la medida en que las redes antiguas predominen, el efecto en el corto plazo será complejo, ya que los sistemas centrales estarán obligados a manejar un gran número de redes bajo una sola plataforma de administración y control.

El presente documento pretende mostrar cuales son y como operan los dispositivos que hacen posible la integración o convergencia de las redes y cuales son las tecnologías, arquitecturas de red y protocolos que se han diseñado para este fin.

El Capítulo 1 describe, en términos generales, en que consiste una red y la interconexión de redes (*internetwork*), cuales son los tipos de redes y las topologías más utilizadas, cuales son los principales conceptos y terminologías que se manejan en el ámbito del

internetworking, cuales son los principales organismos encargados de regular, generar y publicar las especificaciones técnicas bajo las cuales todos los proveedores desarrollan sus productos y soluciones, y en que consiste el modelo de referencia OSI y cual es la función de cada una de las siete capaz que lo integran.

Los Capítulos 2 al 7 describen las características, modo de operación, alcance y aplicación de los principales dispositivos de red que permiten la interconexión de redes y usuarios. En dichos capítulos se revisa la función que desempeñan dispositivos sencillos como módems, repetidores y concentradores, al igual que aquellos más complejos como puentes, ruteadores, conmutadores y pasarelas. En el caso de estos últimos, se explica cuales son los protocolos que suelen utilizar para actualizar sus bases de datos, información que les permite tomar decisiones acerca de las trayectorias más adecuadas para enrutar el tráfico.

Al final de los capítulos se encuentran 4 apéndices. El primero contiene una breve explicación de los mecanismos de control de acceso al medio utilizados en las redes con medio compartido. El segundo describe la estructura de una red troncal o de soporte, sus ventajas y principales configuraciones. El tercero detalla los conceptos fundamentales de la pila de protocolos TCP/IP, pasando por el direccionamiento, el manejo de subredes y máscaras y la forma como se registran y controlan las direcciones IP. Y finalmente, el cuarto apéndice se refiere a los métodos para llevar a cabo la codificación de información analógica a digital y viceversa.

Capítulo 1 Introducción a las redes de datos

Qué es una red?

Una red no es más que un grupo de computadoras conectadas entre sí mediante cables o algún otro medio de transmisión. Sin embargo, la creación de una red no es nada simple. Cuando las computadoras son capaces de comunicarse entre sí, pueden trabajar de diferentes modos: compartiendo recursos con los demás, distribuyendo el procesamiento de una tarea en particular o intercambiando mensajes.

Algunas de las ventajas que las redes ofrecen son:

- Eficiente comunicación entre los usuarios de la red.
- Los usuarios pueden enviar y compartir información rápida y fácilmente, utilizando por ejemplo, e-mail.
- Los usuarios pueden compartir recursos, como impresoras y servidores Web.

Qué es una Internetwork?

Internetwork es una colección de redes individuales, conectadas entre sí por medio de uno o varios dispositivos de red, con la intención de que opere como una única y gran red de datos. El ejemplo por excelencia de una internetwork es Internet. Internetworking por su parte, se refiere a la industria, a los productos, y a los procedimientos necesarios para crear y administrar redes interconectadas. La Fig. 1.1 muestra algunas tecnologías de red que pueden ser interconectadas por medio de ruteadores (routers) o algún otro tipo de dispositivos de red.

Historia del Internetworking

El paradigma inicial de la computación compartida consistía en una gran computadora central (*mainframe*) a la cual se conectaban una serie de terminales, cada una de las cuales correspondía a un usuario diferente. A este paradigma se le denomina tiempo compartido, porque la computadora central divide los ciclos de reloj del procesador entre las terminales conectadas a aquella. En esta configuración las terminales son sólo dispositivos de comunicación: aceptan entradas de los usuarios a través del teclado y las envían a la computadora, la cual los analiza y devuelve un resultado, mismo que la terminal muestra en la pantalla o imprime en papel. A este tipo de terminales suele llamárseles *terminal simple*. Cada terminal se comunica con un único dispositivo, la computadora central. Las terminales nunca se comunican entre sí.

Conforme el tiempo pasaba y la tecnología progresaba, los ingenieros comenzaron a conectar computadoras que pudiesen comunicarse entre sí. Al mismo tiempo, las computadoras, se volvieron más pequeñas y más baratas. Las primeras redes utilizaban enlaces individuales, como las conexiones telefónicas, para unir dos sistemas. Tan pronto como la primera PC de IBM impactó en el mercado en 1980, fue rápidamente aceptada

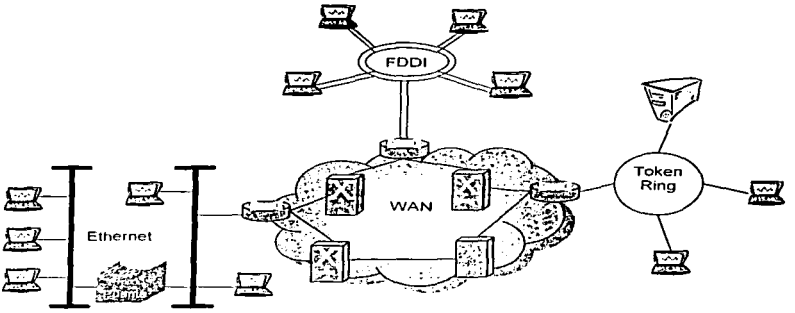


Figura 1.1. Una internetwork puede estar formada por la interconexión de diferentes tecnologías de red.

como herramienta de trabajo en las empresas, resultando obvias las ventajas de conectar estas pequeñas computadoras a la red en lugar de las terminales simples. En lugar de dotar a cada una con su propia impresora, una red podía compartir una única impresora. Cuando un usuario necesitaba entregar un archivo a otro usuario, la conexión a una red común eliminaba la necesidad de intercambiar disquetes. Sin embargo no era práctico ni rentable conectar, con enlaces individuales punto a punto, las computadoras de la empresa. Fue así como surgió una solución conocida como red de área local (*LAN, Local Area Network*).

Las LAN evolucionaron alrededor de la revolución de las PCs. Básicamente una LAN habilita la posibilidad de que múltiples usuarios, ubicados en un área geográfica relativamente pequeña, intercambien mensajes y archivos, así como acceso a recursos compartidos como pueden ser servidores e impresoras.

La evolución del Internetworking se enfocó en resolver tres problemas clave:

- El aislamiento de las redes LAN. Esta situación hacía que la comunicación electrónica entre oficinas o departamentos diferentes y remotos fuera imposible.
- Duplicidad de recursos. El mismo *hardware* y *software* tenía que ser suplido a cada oficina o departamento de una empresa, al igual que era necesario contar con grupos de soporte separados.
- La imposibilidad de gestionar a nivel red. No existía un método o mecanismo centralizado para administrar y resolver problemas técnicos de las redes LAN existentes.

Retos del Internetworking

Implementar una internetwork funcional no es una tarea fácil. Muchos retos deben ser resueltos, especialmente aquellos relacionados con la conectividad, confiabilidad, gestión de red y flexibilidad. Cada una de estas áreas es clave para asegurar que una internetwork sea eficiente y efectiva.

El gran reto cuando se desean conectar varios sistemas es soportar la comunicación a pesar de que cada uno de aquellos pudiera trabajar con tecnologías diferentes. Sitios diferentes, por ejemplo, pueden utilizar diferentes medios de transmisión con velocidades de operación variables, o pueden incluso manejar diferentes tipos de sistemas que necesitan ser comunicados.

Debido a que las compañías dependen enormemente de su comunicación de datos, las internetwork deben proveer cierto nivel de confiabilidad. Y ya que este es un mundo impredecible, muchas internetwork incluyen redundancia en su diseño para asegurar la comunicación incluso en caso de que se presente algún problema.

Además, la gestión de red debe proveer soporte centralizado y capacidad para realizar *troubleshooting* en la internetwork. La configuración, seguridad, desempeño, entre otros aspectos deben ser analizados adecuadamente para que la internetwork funcione sin problemas. La seguridad en una internetwork es esencial. Mucha gente piensa en la seguridad de las redes desde la perspectiva de proteger una red privada de ataques externos. Sin embargo, es igualmente importante protegerlas de ataques internos, ya que muchos de los problemas de seguridad vienen de adentro. Las redes también deben ser aseguradas con la intención de que la red interna no pueda ser utilizada como herramienta para atacar otros sitios externos.

Cobertura de las Redes

Redes de área Local (LAN)

Una *LAN (Local Area Network)* es un grupo de computadoras conectadas entre si mediante un medio de transmisión compartido, normalmente un cable. Compartiendo un único cable, cada computadora requiere una sola conexión para comunicarse con cualquier otra de la red. Una LAN está limitada geográficamente a un área local debido a las propiedades eléctricas de los cables utilizados para construirla, y al número, relativamente pequeño, de computadoras que pueden compartir un mismo medio de transmisión. Las LAN tienen, generalmente, acotada su zona de operación dentro de un único edificio o un campus de edificios adyacentes.

Algunas tecnologías como la fibra óptica, han extendido el rango de las LAN a varios kilómetros, pero de cualquier forma, no es posible utilizar una LAN para conectar computadoras en ciudades muy distantes. Ese es el terreno de las redes de área extensa *(WAN, Wide Area Network)*.

En la mayor parte de los casos, una LAN es una red de banda base con conmutación de paquetes.

Redes de Área Metropolitana (MAN)

Una MAN (*Metropolitan Area Network*) es una red más grande que una LAN pero más pequeña que una WAN. La superficie que usualmente abarca va de 5 a 50 kilómetros. El término MAN suele utilizarse para describir la interconexión de redes LAN dentro de una ciudad, convirtiendo a estas en una única y gran red.

Las MAN generalmente utilizan conexiones de fibra óptica de alta velocidad o algún otro medio digital, consiguiendo, con esto, alcanzar velocidades de transmisión de hasta 200 Mbps.

Redes de Área Amplia (WAN)

Una WAN (*Wide Area Network*) es una red sin limitaciones de distancia. Las WAN interconectan LAN y MAN de forma que los recursos de cualquier red individual están disponibles para todos los usuarios, a pesar de su ubicación geográfica. La interconexión entre WAN y LAN o MAN se realiza a través de puentes (*bridges*) o ruteadores (*routers*).

Para poner en servicio una WAN, circuitos de comunicación de empresas telefónicas deben ser rentados. Esto restringe las facilidades de comunicación, y la velocidad de transmisión, a aquellas que normalmente proveen dichas compañías. Así, Las WAN manejan velocidades de transmisión que van de 56 Kbps hasta 45 Mbps.

Redes e interconexión de redes

Originalmente las LAN se diseñaron para conectar un pequeño número de computadoras en lo que más tarde se llamaría *grupo de trabajo*. En lugar de invertir una gran cantidad de dinero en una computadora central y el soporte necesario para hacerla funcionar , las empresas se dieron cuenta de que, comprando unos pocos equipos y conectándolos entre sí, podían realizar la mayor parte del procesamiento que necesitaban. Conforme crecían las capacidades de las computadoras personales y sus aplicaciones, también progresaban las redes y la tecnología usada para construirlas.

Cableado y Topologías

La mayor parte de las LAN se construye mediante cables de cobre que usan corrientes eléctricas estándar para transmitir señales. Originalmente, la mayor parte de las LAN consistían en computadoras conectadas entre sí mediante cables coaxiales, pero al final resultó más popular el par trenzado utilizado en la telefonía.

Otra alternativa es la fibra óptica, que no usa en absoluto señales eléctricas, sino que utiliza pulsos de luz para codificar datos binarios. Otros tipos de infraestructura eliminan totalmente los cables y transmite los datos usando lo que se conoce como medios de transmisión libre, tales como ondas de radio, infrarrojos y microondas.

Las LAN conectan computadoras utilizando diferentes tipos de configuraciones de cableado llamadas *topologías* (ver Fig. 1.2) que dependen del tipo de cable y de los protocolos utilizados por los equipos. Las topologías más usuales son:

Topología Bus

Esta topología consiste en un cable que va desde una computadora hasta la siguiente como una guirnalda, asemejando una tira de luces de un árbol de Navidad. Cada señal transmitida por una computadora viaja a lo largo de la red en ambas direcciones hasta todas las demás.

Los dos extremos de la red en bus deben terminar en resistencias eléctricas que anulen los voltajes que lleguen a ellas, de modo que no vuelvan señales reflejadas en dirección opuesta.

La primera desventaja de la topología en bus es que, al igual que las luces de un árbol de navidad, un fallo del cable en cualquier punto divide la red en dos e impide que se comuniquen sistemas que estén en lados opuestos del punto de interrupción. Además, la falta de terminación apropiada en los extremos de las dos mitades impide que las computadoras que siguen conectadas se comuniquen correctamente. Encontrar una falla en una red grande de tipo bus puede ser problemático y llevar mucho tiempo.

La mayor parte de las redes de cable coaxial, como las originales LAN Ethernet, utilizan topología de bus.

Topología Estrella

La topología en estrella utiliza un cable distinto para conectar cada computadora a un nodo central llamado *hub* o concentrador. El concentrador propaga las señales que entran por cualquiera de sus puertos hacia todos los demás puertos, de modo que las señales transmitidas por cada computadora llegan a todas las demás. Los concentradores también amplifican las señales que propagan, permitiendo que viajen distancias más grandes sin degradarse.

Una red de estrella es más tolerante a fallas que una en bus porque una interrupción en un cable afecta solamente al dispositivo al que está conectado el cable, no a la totalidad de la red.

La mayor parte de los protocolos de red utilizados con cable de par trenzado, tales como Ethernet 10Base-T y 100Base-T usan topologías en estrella.

Topología Bus en Estrella

Esta topología es utilizada para expandir el tamaño de una LAN más allá de lo posible con una estrella única. En esta topología se unen varias redes en estrella usando un cable en bus para interconectar sus correspondientes concentradores. Nuevamente, toda computadora puede comunicarse con cualquier otra de la red porque cada uno de los concentradores transmite el tráfico entrante tanto al puerto conectado a un segmento de tipo bus como hacia los otros puertos conectados a segmentos de tipo estrella.

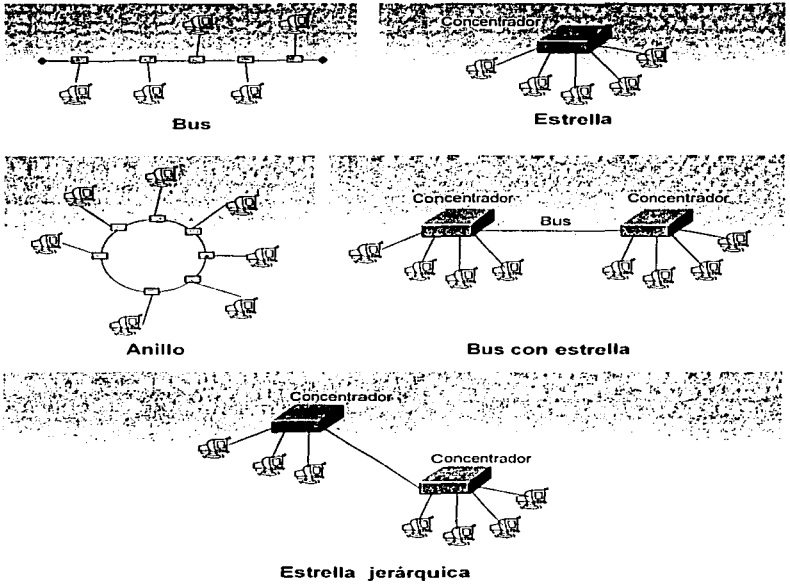


Figura 1.2. Topologías comunes de cableado

La red de bus en estrella, que se diseñó para expandir las redes Ethernet 10Base-T, se ve muy raramente hoy en día debido a las limitaciones de velocidad de las redes de bus con cable coaxial, que pueden convertirse en cuello de botella degradando el rendimiento de tecnologías más rápidas, como las redes en estrella Fast Ethernet.

Topología Estrella jerárquica

La topología en estrella jerárquica es el método más común para expandir una red en estrella más allá de la capacidad del concentrador original. Cuando todos los puertos del

concentrador están ocupados y es necesario conectar más computadoras a la red, se puede conectar un concentrador original a un segundo concentrador, usando un cable a un puerto especial diseñado para este propósito. El tráfico que llega a cualquier concentrador se propaga entonces hacia los demás concentradores, así como a las computadoras conectadas al concentrador. El número de concentradores que puede soportar una LAN depende del protocolo utilizado.

Topología Anillo

Esta topología es funcionalmente equivalente a una topología en bus con los dos extremos conectados entre sí, de modo que las señales viajan de una computadora a la siguiente en una propagación circular. Sin embargo, la comunicación en anillo no es un concepto físico, sino lógico. La red física está cableada en realidad utilizando una topología en estrella con un concentrador especial, llamado *Unidad de acceso multiestación* (*MAU, Multistation Access Unit*), el cual implementa el anillo lógico, transmitiendo cada señal entrante solamente al siguiente puerto del anillo, en lugar de a todos los puertos como ocurre en el concentrador de estrella. Cada computadora, al recibir la señal entrante, la procesa, si es pertinente, y la envía de vuelta al concentrador para que se transmita a la siguiente estación del anillo. Con esta disposición, los sistemas que transmiten las señales a la red deben eliminarlas después de que han atravesado todo el anillo.

Las redes configuradas con topología en anillo pueden utilizar diferentes tipos de cable. Las redes Token Ring, por ejemplo, usan cable de par trenzado, mientras que las redes FDDI utilizan fibra óptica.

Banda base vs. Banda ancha

Una red de banda base es aquella en la que el cable o cualquier otro medio de transmisión puede llevar una única señal cada vez. En contraparte, una red de banda ancha puede transportar múltiples señales simultáneamente, usando una fracción de la anchura de banda del cable para cada señal. El ejemplo más claro de una red de banda ancha es el servicio de televisión por cable. Aunque sólo llega un cable al televisor, nos proporciona docenas de canales de programación el mismo tiempo. Esto puede ser verificado de forma muy simple al conectar un segundo televisor a dicha señal utilizando un separador para llevar la señal a diferentes habitaciones. El hecho de que los televisores, conectados al mismo cable, puedan sintonizar diferentes programas al mismo tiempo, demuestra que el cable está proporcionando todo el tiempo una señal separada para cada canal.

Una red de banda base usa pulsos, aplicados directamente al medio de transmisión, para crear una única señal que transporta datos binarios codificados. En comparación con las tecnologías de banda ancha, las redes de banda base alcanzan distancias relativamente cortas porque están sujetas a la degradación debida a interferencias eléctricas y otros factores. La longitud máxima de un segmento de cable de banda base disminuye cuando aumenta la velocidad de transmisión. Por ese motivo, los protocolos de red de área local, como Ethernet, tienen estrictas especificaciones para la instalación de cable.

Control de acceso al medio

Cuando múltiples computadoras están conectadas al mismo medio de banda base, tiene que haber un mecanismo para controlar el acceso a dicho medio de transmisión compartido (*MAC, Media Access Control*), para impedir que distintos sistemas transmitan datos al mismo tiempo. El mecanismo de MAC es una parte fundamental de todos los protocolos de LAN que usan un medio de transmisión compartido. Los mecanismos de MAC más comunes son Acceso múltiple con detección de portadora y detección de colisiones (*CSMA/CD, Carrier Sense Multiple Access with Collision Detection*), que se usa en redes Ethernet, y el mecanismo Paso de testigo que se usa en redes Token Ring, FDDI y otros protocolos. Estos dos mecanismos son esencialmente diferentes, pero cumplen la misma función al proporcionar a cada sistema de la red la misma oportunidad de transmitir datos.

(Para mayor detalle sobre los mecanismos de control de acceso al medio, referirse al Apéndice A).

Conmutación de paquetes vs. Conmutación de circuitos

Se dice que las LAN son redes de conmutación de paquetes porque sus computadoras dividen los datos antes de transmitirlos, en pequeñas unidades separadas denominadas paquetes. Existe también una técnica similar, llamada conmutación de celdas, que difiere de la conmutación de paquetes solamente en que las celdas son siempre consistentes y de tamaño uniforme, mientras que los paquetes son variables. La mayor parte de las tecnologías de LAN, como Ethernet, Token Ring y FDDI (*Fiber Distributed Data Interface*), usan conmutación de paquetes. El modo de transferencia asíncrono (*ATM, Asynchronous Transfer Mode*) es el único protocolo LAN de conmutación de celdas de uso común.

La razón por la cual los datos se dividen de esta forma, es porque las computadoras de una LAN comparten un único cable; de otro modo, una computadora que transmitiese un flujo continuo de datos monopolizaría la red todo el tiempo. Cuando se examinan los datos transmitidos por una red de conmutación de paquetes, se puede ver que el flujo de datos consiste en paquetes generados por muchos sistemas diferentes, entremezclados en el cable. En este tipo de redes, es normal que paquetes que pertenecen al mismo mensaje tomen diferentes caminos hacia su destino e incluso lleguen al destino en un orden diferente al de partida. El sistema receptor debe disponer, por tanto, de un mecanismo para reensamblar los paquetes en el orden correcto y reconocer la ausencia de paquetes que se hayan perdido o paquetes que se hayan dañado por el camino.

Frente a la conmutación de paquetes está la conmutación de circuitos, en el que un sistema establece en canal de comunicación hasta el otro sistema antes de transmitir los datos. En la industria de comunicación de datos, se usa la conmutación de circuitos para ciertos tipos de tecnología de red de área extensa, como la Red Digital de Servicios Integrados (RDSI) y *Frame Relay*. El ejemplo clásico de la conmutación de circuitos es la red telefónica pública. Cuando se llama a otra persona, se establece un circuito físico ente los dos teléfonos. Este circuito permanece activo durante todo el transcurso de la llamada, de modo que nadie mas puede utilizarlo, incluso cuando no transporta datos, es decir, cuando nadie está hablando.

Tipos de comunicación

Con el reciente desarrollo de IPv6 (protocolo de Internet versión 6) se diseñaron cuatro tipos de comunicación para redes de datos: *difusión (broadcast), unienvío (unicast), multidifusión (multicast) y anycast*. IPv6 fue diseñado para reemplazar el antiguo estándar IPv4, más comúnmente conocido como TCP/IP. IPv6 representa muchas mejoras en la comunicación de Internet, incluyendo 128 bits de direccionamiento, mejores características en seguridad, soporte para comunicación en tiempo real, y capacidad de manejar otros tipos de comunicaciones.

Difusión Un mensaje de difusión (*broadcast*) es aquel que se envía simultáneamente a todo aquel usuario conectado a la red.

Unienvío El término dirección unienvío (*unicast*) se utiliza para distinguir una dirección física única asignada a una interfaz concreta. Por tanto, la comunicación del tipo unienvío es la que se realiza entre un sólo emisor y un sólo receptor. En la actualidad se utiliza también el término, comunicación punto-a-punto, que básicamente significa lo mismo que unienvío.

Multidifusión Un mensaje multidifusión (*multicast*) es aquel que se envía a un selecto grupo de estaciones de trabajo conectadas a una LAN, WAN o Internet. Por tanto, la multidifusión es la comunicación que se lleva a cabo entre un sólo emisor y múltiples nodos receptores de una red. Por ejemplo, un ruteador puede dirigir un mensaje asociado con una tabla de enrutamiento a un cierto número de otros ruteadores en una internetwork LAN.

Muchas compañías han descubierto que la multidifusión puede ser una manera mucho más eficiente de distribuir información internamente que el enviar mensajes separados a múltiples direcciones o saturando la red enviando mensajes de difusión (*broadcast*).

Anycast Es la comunicación entre un solo emisor y el más cercano grupo de receptores de este. Los mensajes *anycasting*, fueron diseñados para optimizar el proceso de actualización de las tablas de enrutamiento. IPv6 le permite a un *host* determinar cuales ruteadores están más cerca de él, y en consecuencia enviarles un mensaje como si se tratara de una comunicación unienvío. Ese ruteador, a su vez, asume la responsabilidad de transmitir la información de actualización hacia todos los demás ruteadores de su grupo vía un mensaje de multidifusión. Este acercamiento permite que la tarea de actualización de las tablas de enrutamiento se delegue y complete más eficientemente.

Direccionamiento

Para que los sistemas de una red con medio de transmisión compartido puedan comunicarse eficazmente, deben disponer de algún método para identificarse entre sí. Habitualmente algún tipo de dirección numérica. En la mayoría de los casos, la tarjeta de red (*NIC, Network Interface Card*), instalada en cada computadora, viene de fábrica con una

dirección codificada en el circuito, llamada *dirección MAC* o *dirección física o dirección hardware*, que identifica de un modo único la tarjeta entre las demás. Cada paquete que se transmite a la red contiene la dirección de la computadora emisora y la dirección del sistema al que el paquete está destinado.

Además de la dirección MAC, los sistemas pueden tener otras direcciones operando a otros niveles. Por ejemplo, el protocolo TCP/IP requiere que se asigne una dirección única IP a cada sistema, además de la dirección MAC que ya posee. Los esquemas de direccionamiento varían en función de la familia de protocolos y de la capa del modelo OSI en donde se esté trabajando. A nivel internetwork existen tres tipos de direccionamiento:

- Direccionamiento de la capa de enlace de datos.
- Control de acceso al medio (MAC, Media Access Control).
- Direccionamiento de la capa de red.

Direccionamiento de la capa de enlace de datos

Una *dirección de la capa de enlace de datos* únicamente identifica la conexión física a red de un dispositivo determinado. La dirección de enlace de datos suele utilizarse dentro de un espacio de direccionamiento plano y tiene una relación fija y preestablecida con un dispositivo específico.

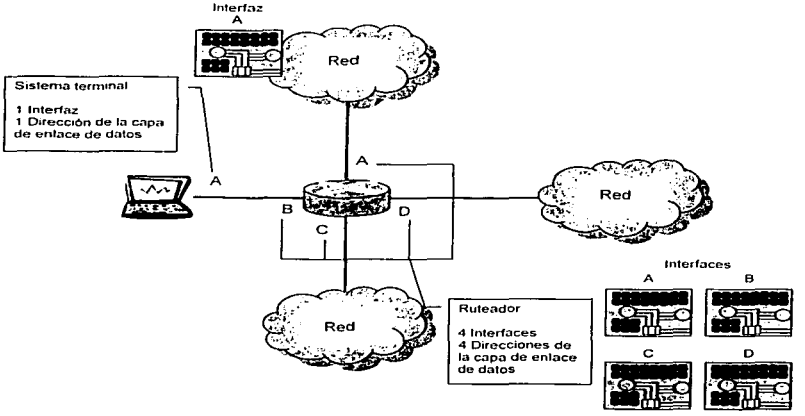


Figura 1.3. La interfaz de cada dispositivo se identificada de forma exclusiva con una dirección de la capa de enlace de datos.

Los sistemas terminales de una red generalmente cuentan con una sola conexión física a la red, por lo que, solo tienen una dirección de enlace de datos. Los ruteadores (routers) y otros dispositivos de internetwork suelen tener múltiples conexiones físicas a la red, por lo que cuentan con múltiples direcciones de enlace de datos. La Fig. 1.3 ilustra como cada interfaz de un dispositivo es identificado de forma única por una dirección de enlace de datos.

Direccionamiento MAC

La dirección de control de acceso al medio (MAC, Media Access Control) es una subcapa de las direcciones de enlace de datos. La dirección MAC identifica a los sistemas de una red LAN. Al igual que en la mayoría de las direcciones de enlace de datos, las direcciones MAC son únicas para cada interfaz de red. La Fig. 1.4 ilustra la relación entre dirección MAC, dirección de enlace de datos, y las subcapas de la capa de enlace de datos.

Figura 1.4. Las direcciones MAC, de enlace de datos y de las subcapas de la capa de enlace de datos de la IEEE, se relacionan entre si.

La dirección MAC tiene una longitud de 48 bits y está expresada como 12 dígitos en formato hexadecimal. Los primeros 6 dígitos, son administrados por la IEEE (*Institute of Electrical and Electronic Engineers*) e identifican al fabricante o vendedor por medio del *identificador organizativo único* (*OUI, Organizationally Unique Identifier*). Los últimos 6 dígitos comprenden el número serial de la interfaz, u otro valor administrado por el fabricante. La dirección MAC algunas veces llamada *dirección quemada (BIA, Burned-in Address)* es literalmente quemada en una memoria de sólo-lectura (*ROM, Read-Only Memory*) de la tarjeta interfaz de red. La Fig. 1.5 muestra el formato de la dirección MAC.

Figura 1.5. La dirección MAC contiene una identificación única de 12 dígitos en formato hexadecimal.

Direccionamiento de la capa de red

La dirección de la capa de red identifica a una entidad de la capa de red del modelo OSI. Las direcciones de red usualmente se utilizan dentro de un espacio de direcciones jerárquico y algunas veces es llamada dirección virtual o lógica. La relación entre una dirección de red y un dispositivo es lógica y no fija; típicamente está basada ya sea en características de la red física (el dispositivo se encuentra en un segmento particular de la red) o en agrupamientos que no tienen bases físicas. Las terminales requieren una dirección de red para cada protocolo de red que soporten (esto parte del hecho de que el dispositivo tiene una única conexión física a red). Los ruteadores y otros dispositivos de internetworking requieren una dirección de la capa de red por cada conexión a red física y para cada protocolo de red soportado. Por ejemplo, un ruteador con tres interfases, cada una de las cuales corriendo con *Apple Talk* (protocolo de red nativo de *Macintosh*), TCP/IP y OSI, debe tener tres direcciones de red por cada interfaz. Por lo tanto los ruteadores, tienen nueve direcciones de la capa de red. La Fig. 1.6 ilustra como cada interfaz de red debe ser asignada a direcciones de red para cada protocolo que soporte.

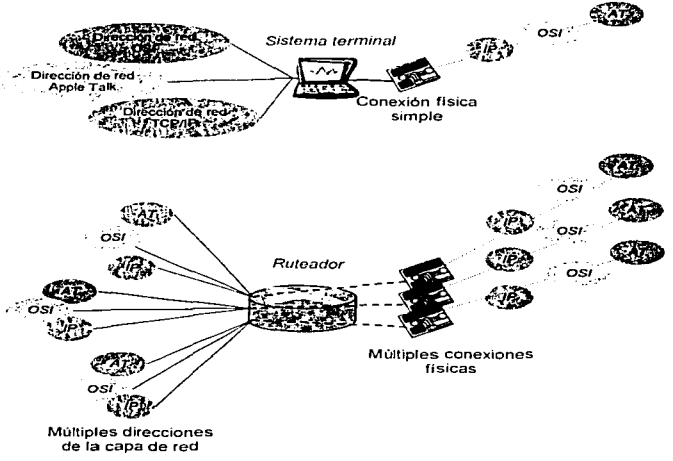


Figura 1.6. A cada interfaz de red se le debe asignar una dirección de red por cada protocolo que soporte.

Compaginación de direcciones

Debido a que las internetwork generalmente utilizan direcciones de red para enrutar el tráfico a través de la red, existe la necesidad de compaginar la dirección de red con la dirección MAC. Cuando la capa de red ha determinado la dirección de red de la estación de trabajo destino, debe reenviar la información sobre una red física utilizando la dirección MAC. Existen grupos de protocolos que utilizan diferentes métodos para realizar dicha compaginación, siendo el más popular el protocolo de resolución de direcciones (*ARP, Address Resolution Protocol*).

ARP es el método utilizado por TCP/IP. Cuando un dispositivo de red necesita enviar datos a otro dispositivo en la misma red, aquel conoce la dirección de red origen y destino para realizar dicha transferencia, por lo que debe de algún modo compaginar la dirección destino con la dirección MAC antes de reenviar los datos. Primero, la estación transmisora revisará su tabla ARP para verificar si cuenta con la dirección MAC de la estación destino. Si no es así, enviará un mensaje de difusión a la red con la dirección IP de la estación destino contenida en el encabezado del mensaje de difusión. Cada estación de la red recibe el mensaje de difusión y compara la dirección IP encapsulada con la suya propia. Sólo la estación con la dirección IP que coincida responderá a la estación transmisora con un paquete que contiene la dirección MAC de la estación. La primera estación, entonces añade esta información a su tabla ARP para futuras referencias y procede a transferir los datos. Cuando el dispositivo destino se encuentra en una red remota, más allá de un ruteador, el proceso es el mismo excepto que la estación transmisora envía la solicitud ARP con la dirección MAC de su propia pasarela (Gateway) predeterminada. La pasarela (Gateway) predeterminada reenviará la información sobre las redes que sean necesarias para entregar el paqueta a la red en la cual reside el dispositivo destino. El ruteador (router) de la red del dispositivo destino utilizará ARP para obtener la dirección MAC del dispositivo destino y entregará el paquete.

Además de ARP existe otro método comúnmente utilizado para la resolución de direcciones de red, conocido protocolo *Hello*. Este protocolo de la capa de red habilita la posibilidad de que los dispositivos conectados a la red identifiquen a otros e indiquen que aún están funcionando. Cuando, por ejemplo, un nuevo sistema se da de alta en la red, envía un mensaje de difusión *hello*, conteniendo su propia dirección MAC, hacia el resto de los usuarios a través de la red. Entonces, todos los dispositivos de la red responden al mensaje *hello* enviando sus respectivas direcciones MAC. Posteriormente, mensajes *hello* continúan siendo enviados a intervalos específicos para indicar que aún están conectados. Los dispositivos de red pueden aprender las direcciones MAC de otros dispositivos examinando los paquetes del protocolo *Hello*.

Espacio de direccionamiento jerárquico contra plano

El espacio de direccionamiento en una Internetwork puede ser: espacio de direccionamiento jerárquico o espacio de direccionamiento plano. Un espacio de direccionamiento jerárquico está organizado en numerosos subgrupos, cada uno de los cuales cuenta con una dirección específica hasta el punto de un dispositivo único. Un espacio de direccionamiento plano está organizado en un grupo simple. El direccionamiento jerárquico ofrece ciertas ventajas sobre el esquema de direccionamiento plano. La clasificación y llamado es simplificada

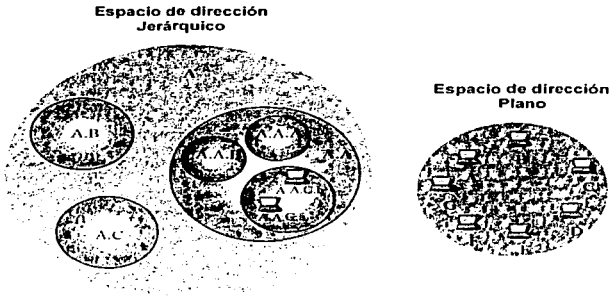


Figura 1.7. Comparación entre los espacios de direccionamiento Jerárquico y Plano.

utilizando operaciones de comparación. Por ejemplo, si la dirección destino de un paquete se encuentra en "Irlanda" se elimina a cualquier otro país como una posible localización. La Fig. 1.7 ilustra la diferencia entre el espacio de direccionamiento jerárquico y plano.

Asignación de dirección

Las direcciones asignadas a los dispositivos pueden ser: estáticas y dinámicas. Las direcciones estáticas son asignadas por el administrador de la red con base en un plan de direccionamiento preconcebido de Internetwork. Una dirección estática no cambia a menos que el administrador de la red lo haga manualmente. Las direcciones dinámicas las obtienen los dispositivos al conectarse a una red, por medio del proceso especificado por el protocolo en cuestión. Un dispositivo que utiliza una dirección dinámica a menudo tiene diferentes direcciones cada vez que se conecta a la red. Algunas redes utilizan un servidor para asignar las direcciones. Una vez que el usuario se desconecta de la red, las direcciones asignadas por el servidor son recicladas. Un dispositivo, por lo tanto, es probable que tenga diferentes direcciones cada vez que se conecta a la red.

Direcciones contra nombres

Los dispositivos de Internetwork tienen un nombre y una dirección asociada a ellos. Los nombres de internetwork normalmente son independientes de su ubicación y permanecen asociados con el dispositivo a donde quiera que el dispositivo se mueva (por ejemplo, de un edificio a otro). Las direcciones de Internetwork generalmente son dependientes de la ubicación y cambian cuando el dispositivo se mueve de lugar (aunque la dirección MAC es una excepción de esta regla). Al igual que las direcciones de red son compaginadas con las direcciones MAC, los nombres usualmente son compaginados a las direcciones de red por medio de algún protocolo. Internet utiliza el Sistema de nombres de dominio (*DNS, Domain Name System*) para compaginar el nombre de un dispositivo a su dirección IP. Por

ejemplo, resulta fácil recordar www.cisco.com en lugar de alguna dirección IP. Por lo tanto, una persona teclea www.cisco.com dentro de su *browser* cuando desea acceder al sitio Web de Cisco. Su computadora realiza una búsqueda DNS de la dirección IP del servidor Web de Cisco y entonces establece la comunicación utilizando la dirección de red correspondiente.

Formatos de la información

Los datos y la información de control que es transmitida a través de las internetworks tienen diferentes formatos. Los términos utilizados para referirse a dichos formatos no están consolidados en la industria del internetworking por lo que en ocasiones se utilizan indistintamente. Los formatos de información más comunes son:

- Tramas
- Paquetes
- Datagramas
- Segmentos
- Mensajes
- Celdas
- Unidades de datos

Una trama es una unidad de información cuyo origen y destino son entidades de la capa de enlace de datos. Está compuesta por un encabezado de la capa de enlace de datos y datos de capas superiores. El encabezado contiene información de control dirigida a la entidad de la capa de enlace de datos del sistema destino. Los datos de entidades de capas superiores son encapsulados (envueltos por un encabezado y en algunos casos por una cola) en la capa de enlace de datos. La Fig. 1.15 ilustra los componentes básicos de una trama de la capa de enlace de datos.

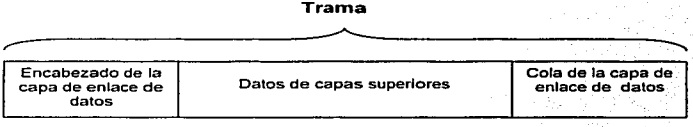


Figura 1.15. Los datos de entidades de capas superiores forman parte de la trama de la capa de enlace de datos.

Un paquete es una unidad de información cuyo origen y destino son entidades de la capa de red. Un paquete está compuesto por el encabezado de la capa de red y datos de capas superiores. El encabezado contiene información de control dirigida a la entidad de la capa de red en el sistema destino. Los datos para entidades de capas superiores son encapsulados (envueltos por un encabezado y en algunos casos por una cola) en la capa de red. La Fig. 1.16 ilustra los componentes básicos de un paquete de la capa de red.

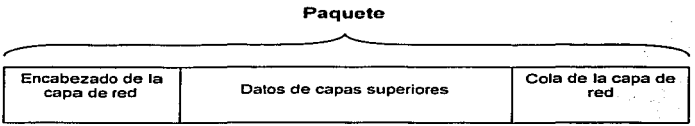


Figura 1.16. Tres componentes básicos integran un paquete de la capa de red.

El término *datagrama* generalmente se refiere a la unidad de información cuyo origen y destino son entidades de la capa de red que utilizan *protocolos sin conexión (connectionless)*.

El término *segmento* generalmente se refiere a la unidad de información cuyo origen y destino son entidades de la capa de transporte.

Un mensaje es una unidad de información cuyas entidades origen y destino existen encima de la capa de red (a menudo en la capa de aplicación).

Una celda es una unidad de información con tamaño fijo cuyo origen y destino son entidades de la capa de enlace de datos. Las celdas son utilizadas en ambientes conmutados, como el Modo de transferencia asíncrono (*ATM, Asynchronous Transfer Mode*) y redes de Servicios de datos multimegabit conmutados (*SMDS, Switched Multimegabit Data Service*). Una celda está compuesta por un encabezado y por la carga útil (*payload*). El encabezado contiene información de control dirigida a la entidad de la capa de enlace de datos destino y normalmente tiene una longitud de 5 bytes. El *payload* contiene datos de capas superiores que son encapsulados en el encabezado de la celda y normalmente tiene una longitud de 48 bytes.

La longitud del encabezado y de los campos de *payload* siempre son los mismos para todas las celdas. La Fig. 1.17 representa los componentes de una celda típica.

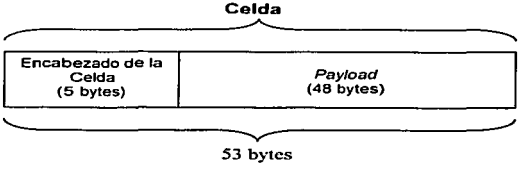


Figura 1.17. Una celda típica está compuesta por dos elementos

Las unidades de datos son un término genérico para referirse a una variedad de unidades de información. Algunos de las unidades de datos más comunes son unidad de datos de servicio (*SDU, Service Data Units*), unidad de datos de protocolo, y unidad de datos de protocolo de puente (*BPDU, Bridge Protocol Data Units*). Las SDU son unidades de información de protocolos de capas superiores que definen los requerimientos del servicio para los protocolos de capas inferiores. PDU es una terminología de OSI (*Open Systems Interconnection*) para paquetes. BPDU son utilizados por el algoritmo del árbol de expansión como mensajes *Hello* (ver capitulo 3).

Redes de jerarquía ISO

Las redes grandes normalmente están organizadas en jerarquías. Una organización jerárquica provee ventajas tales como fácil administración, flexibilidad, y reducción de tráfico innecesario. Es por esto, que la Organización internacional de normalización (*ISO, International Organization for Standardization*), ha adoptado ciertos términos convencionales para identificar a las diferentes entidades que conforman una red. Términos como Sistema final (*ES, end system*), Sistema intermedio (*IS, intermediate system*), Sistema intermediario de frontera (*BIS, Boundary Intermediate System*), dominio de enrutamiento (*RD, Routing Domain*), Área, y Sistema autónomo (*AS, autonomous system*), son claves para entender las redes jerárquicas.

Un *ES*, es un dispositivo de red que no realiza enrutamiento u otras funciones de reenvío de tráfico. Tipicamente ES incluye dispositivos como terminales, computadoras personales e impresoras. Un *IS* es un dispositivo de red que realiza enrutamientos u otras funciones de reenvío de tráfico. Tipicamente un *IS* incluye dispositivos tales como ruteadores (router), conmutadores (Switch) y puentes (bridge).

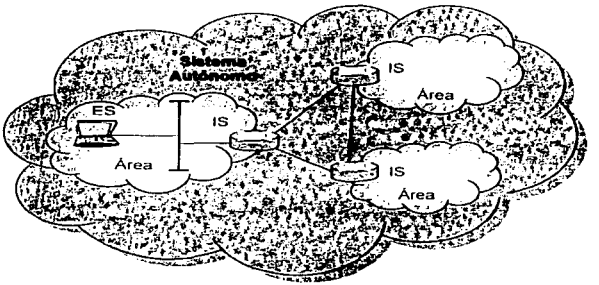


Figura 1.18. Componentes que integran las redes jerárquicas.

Existen dos tipos de redes IS: *IS intradominio* e *IS interdominio*. Un *IS intradominio* comunica sistemas dentro de un sólo sistema autónomo, mientras que un *IS interdominio* comunica sistemas dentro y entre sistemas autónomos. Un *Área* es un grupo lógico de segmentos de red y de sus dispositivos conectados. Las áreas son subdivisiones de sistemas autónomos (*AS, autonomous system*). Un *AS* es una colección de redes bajo una misma administración que comparten una estrategia de enrutamiento común. Los sistema s autónomos están subdivididos en áreas, y en algunas ocasiones los AS son llamados dominios. Un grupo de *ISs* conectados entre si, que participan con un mismo protocolo de enrutamiento intradominio forma un dominio de enrutamiento (*RD, Routing Domain*). Los *ISs* que participan en enrutamientos interdominio son llamados sistemas intermediarios de frontera (*BIS, Boundary Intermediate Systems*). La Fig. 1.18 ilustra una red jerárquica y sus componentes.

Protocolos con conexión y sin conexión

Hay dos tipos de protocolos que operan en la capa de red y de transporte: *protocolos con conexión (connection-oriented)* y *protocolos sin conexión (connectionless)*. El tipo de protocolo utilizado ayuda a determinar el resto de las funciones que se realizan en cada nivel. Un *protocolo con conexión* es aquel en que se establece una conexión lógica entre los sistemas de origen y de destino antes de que se transmitan datos de alto nivel. Durante el establecimiento de la conexión, los sistemas de origen y de destino pueden reservar recursos para la conexión, y tienen la posibilidad de negociar y establecer ciertos criterios para realizar la transferencia, como pudiera ser el tamaño de la ventana utilizada en conexiones TCP. Una vez que se establece la conexión, el sistema origen transmite los datos y el sistema destino confirma su recepción. La falta de recepción de la confirmación apropiada, le sirve al sistema emisor como señal de que se tienen que retransmitir los paquetes. Cuando la transmisión de datos se completa correctamente, los dos sistemas terminan la conexión. Al utilizar este tipo de protocolo, el sistema emisor puede saber con seguridad si los datos han llegado a su destino adecuadamente.

El costo de este servicio garantizado es el tráfico adicional producido en la red al establecer la conexión, realizar la confirmación y enviar mensajes de terminación, además de un encabezado (*overhead*) substancialmente más largo en cada paquete de datos que el del utilizado por los protocolos sin conexión.

Por su lado, los *protocolos sin conexión* pueden enviar datos sin la necesidad de establecer previamente una conexión, simplemente empaquetan los datos y los transmiten hacia su dirección de destino sin comprobar si el sistema destino está disponible ni esperar confirmación de recepción de los paquetes. En la mayor parte de los casos, se utilizan protocolos sin conexión cuando hay un protocolo de más alto nivel que proporciona servicios con conexión tales como entrega garantizada. Estos servicios adicionales pueden incluir también control de flujo, un mecanismo que regula la velocidad de transmisión de datos por la red, detección y corrección de errores.

La mayor parte de los protocolos de LAN que operan en el nivel de red, como IP e IPX, funcionan sin conexión. En ambos casos, hay diversos protocolos disponibles en el nivel de transporte para proporcionar, tanto servicios con conexión, como servicios sin conexión.

Cuando se utiliza un protocolo con conexión en cierto nivel, habitualmente no existe ningún motivo para hacer lo mismo en otro nivel. El objeto de la pila de protocolos es proporcionar el servicio que necesita cada aplicación, pero no más. A pesar de que IP es un protocolo sin conexión, dispone de un mecanismo de detección de errores a nivel de los campos del encabezado IP, dejando que sean otros protocolos de más alto nivel los que realicen comprobaciones de errores en el campo de datos.

Principios básicos del control de flujo

El control de flujo es, comúnmente, una de las funciones proporcionadas por los protocolos de transporte con conexión, cuyo objetivo es prevenir la ocurrencia de congestión y pérdida de datos en la red. En términos generales se trata de un mecanismo por medio del cual el sistema receptor puede notificar al emisor que disminuya su velocidad de transmisión para evitar saturación y pérdida de datos. Una computadora de alta velocidad, por ejemplo, puede generar tráfico más veloz del que la red puede transferir, o más veloz de lo que el sistema destino puede recibir y procesar. Los tres métodos comúnmente usados para manejar la congestión de red son *buffering, mensajes de extinción del origen* (*Source-quench messages*) y *ventana deslizante (windowing)*.

El Buffering, es utilizado por los sistemas receptores para almacenar, temporalmente en memoria, el exceso de datos recibidos hasta que estos puedan ser procesados. Eventualmente, el exceso de datos puede manejarse con facilidad por medio de *buffering*. Sin embargo, si un sistema emisor genera demasiados paquetes demasiado aprisa, el búfer del receptor se puede llenar y los paquetes que lleguen al sistema se descartaran hasta que exista nuevamente espacio en el búfer.

Los mensajes de extinción del origen son utilizados por los sistemas receptores como ayuda para prevenir la saturación de sus búferes. El sistema receptor envía mensajes de extinción del origen hacia el sistema transmisor, solicitando se disminuya la velocidad de transmisión. El proceso que sigue este mecanismo es el siguiente: Primero, el sistema receptor comienza a descartar paquetes debido a la saturación del búfer. Posteriormente, el sistema receptor inicia el envío de mensajes de extinción del origen hacia el sistema transmisor a razón de un mensaje por paquete descartado. El sistema transmisor recibe los mensajes de extinción del origen y disminuye la tasa de transmisión hasta que la recepción de dichos mensajes desaparezca. Finalmente, el sistema emisor incrementa gradualmente la velocidad de transmisión hasta el punto en que no se reciban nuevas solicitudes de extinción del origen.

La ventana deslizante es un esquema de control de flujo que, en esencia, le sirve al sistema receptor para indicar al emisor cuánto espacio disponible tiene en su búfer. Para conseguir esto, el sistema receptor envía mensajes de confirmación de recepción de paquetes al sistema emisor cada vez que recibe cierto número de paquetes, sin esta confirmación el sistema emisor no continuará con la transmisión de datos. Por ejemplo, con un tamaño de ventana de 3, el sistema emisor requiere un mensaje de confirmación después de haber enviado tres paquetes. El proceso que se sigue es el siguiente: Primero, el sistema emisor envía tres paquetes hacia el sistema destino. Enseguida, una vez que se han recibido dichos paquetes, el sistema destino envía un mensaje de confirmación hacia el sistema emisor. El

sistema emisor recibe el mensaje de confirmación y envía otros tres paquetes. Si el sistema destino no recibe uno o más de dichos paquetes por cualquier razón, como pudiera ser la saturación del búfer, no habrá recibido suficientes paquetes para enviar el mensaje de confirmación, en cuyo caso, el sistema emisor retransmitirá los paquetes a una velocidad de transmisión menor.

Principios básicos de la detección y corrección de errores

Los esquemas de detección de errores determinan si los datos transmitidos se han deteriorado o dañado durante el viaje hacia su destino. La función de detección de errores está implementada en varios niveles del modelo OSI, por lo que a continuación nos referiremos, brevemente, a los mecanismos de detección de errores más comúnmente usados en las capas de enlace de datos y de transporte.

La mayor parte de los protocolos de enlace de datos se diferencian de los protocolos de más alto nivel en que, además del encabezado, incluyen una cola a continuación del campo de datos. Esta cola contiene un campo denominado Secuencia de comprobación de tramas (*FCS, Frame Check Sequence),* que utiliza el sistema receptor para detectar errores ocurridos durante la transmisión. Con este fin, el sistema que transmite el paquete realiza un cálculo sobre la totalidad de la trama denominada Comprobación de redundancia cíclica (*CRC, Cyclic Redundancy Check*) e incluye el resultado en el campo FCS. Cuando el paquete alcanza su siguiente destino, el sistema receptor realiza el mismo cálculo y compara el resultado con el valor del campo FCS. Si los valores no coinciden, se deduce que el paquete se ha deteriorado durante el tránsito y se elimina.

El sistema receptor no realiza ninguna acción para que se vuelvan a transmitir los paquetes eliminados; esta tarea se deja a protocolos de más alto nivel. El proceso de detección de errores tiene lugar en cada salto durante el viaje del paquete hacia su destino.

Por otra parte, los protocolos de transporte con conexión, pueden realizar la detección y corrección de errores por cualquiera de los siguientes mecanismos:

- *Respuesta a errores señalados*
- *Detección y corrección de errores no señalados*

La respuesta a errores señalados, consiste en que el protocolo de transporte no tiene que detectar los errores de transmisión propiamente dichos, sino que utiliza la información de los errores detectados por otros protocolos de la pila, para corregirlos. Al recibir una notificación de un protocolo del nivel de red o de enlace de datos, informando que ha ocurrido un error y que determinados paquetes se han perdido o deteriorado. El protocolo de transporte sólo tiene que enviar un mensaje al sistema origen con la lista de paquetes, pidiendo su retransmisión.

La detección y corrección de errores no señalados, es el mecanismo más comúnmente implementado en el nivel de transporte. Consiste en la detección de errores no detectados por otros medios y su correspondiente corrección. A diferencia de los mecanismos de detección y corrección de errores utilizados por los protocolos de enlace de datos, en donde

operan en el ámbito de saltos individuales entre dos sistemas, el mecanismo de detección de errores del nivel de transporte proporciona comprobación de errores entre los dos sistemas terminales e incluye la capacidad de corregirlos, informando al emisor de los paquetes que hay que reenviar. Con este fin, la suma de comprobación que se incluye en el encabezado del protocolo de transporte, solamente se calcula sobre los campos que no se modifican en el viaje hasta el destino.

Protocolos y Estándares

Los primeros productos de red tendían a ser soluciones propietarias creadas por un único fabricante, pero, conforme el tiempo pasó, la interoperatividad se volvió cada vez más prioritaria y se crearon organizaciones para desarrollar y ratificar estándares de protocolos de red. En la actualidad existe gran variedad de organizaciones que contribuyen en la definición de dichos estándares, los cuales, a través de foros de discusión, convierten discusiones informales en especificaciones formales.

La mayoría de las organizaciones encargadas de desarrollar estándares utilizan procesos específicos: organizando ideas, discutiendo los diferentes enfoques, desarrollando estándares preliminares, votando por la totalidad o por ciertos aspectos de los estándares, y liberando, formalmente, estándares completos al público en general.

Hoy en día la mayor parte de los protocolos de uso común han sido estandarizados por estos organismos, algunos de los cuales son los siguientes:

International Organization for Standardization (ISO)

La organización Internacional de normalización (*ISO, International Organization for Standardization*) fue integrada como resultado de una reunión realizada en Londres en 1946, cuando delegados de 25 naciones decidieron crear una organización para desarrollar estándares internacionales. La nueva organización inició oficialmente sus funciones en 1947, sus oficinas centrales se encuentran en Génova y en la actualidad cuenta con 89 países miembros.

La contribución más conocida de este organismo son los estándares de la serie 9000, los cuales especifican los requerimientos que deben satisfacer los sistemas de calidad de las organizaciones. En muchas industrias y sectores, la certificación ISO 9000 se ha convertido en un requerimiento obligatorio. En el mundo de la comunicación de datos, ISO es conocido por el desarrollo del modelo de referencia de Interconexión de sistemas abiertos OSI y de su suite de protocolos.

American National Standards Institute (ANSI)

ANSI, fundada en 1918 y miembro de ISO, es un organismo coordinador de grupos voluntarios de estándares dentro de los Estados Unidos. Está integrado por compañías, agencias gubernamentales, instituciones y otras organizaciones del ámbito comunicaciones. Su principal responsabilidad es la estandarización de protocolos y códigos de transmisión en los Estados Unidos. Entre otros, ANSI desarrollo la interfaz de datos distribuidos por fibra (*FDDI, Fiber Distributed Data Interface*) y el código estándar americano para

intercambio de información (*ASCII, American Standard Code for Information Interchange*).

Electronic Industries Association (EIA)

La EIA especifica estándares para la transmisión eléctrica, incluyendo aquellas utilizadas en internetworking. La EIA desarrollo el ampliamente utilizado estándar EIA/TIA-232 (antes conocido como RS-232).

Institute of Electrical and Electronic Engineers (IEEE)

La IEEE surge en 1963 al fusionarse la *AIEE (American Institute of Electrical Engineers)* y la *IRE (Institute of Radio Engineers)*. Sin embargo el origen de esta organización data de 1884, fecha en que la AIEE fue fundada. La IEEE esta integrada por diversas asociaciones y consejos técnicos, y está enfocada en promover innovaciones tecnológicas en diversos campos, incluyendo ingeniería en computación y telecomunicaciones. Cualquier persona que trabaje en ingeniería o algún campo relacionado puede ser miembro de esta organización, de hecho, las membresías para estudiantes también están disponibles. La publicación más conocida de la IEEE es el grupo de trabajo 802, que incluye los estándares que definen las arquitecturas de red LAN (*Local Area Network*) y MAN (*Metropolitan Area Network*). Un ejemplo de ello son las especificaciones IEEE 802.3, más conocida como Ethernet, y la IEEE 802.14 para cable coaxial.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T)

Antiguamente conocida como el Comité Consultivo Internacional Telefónico y Telegráfico (*CCITT, Committee Consultative for International Telephone and Telegraph*) la ITU tiene sus oficinas generales en Génova. Fue establecida por las Naciones Unidas en 1865 como la Unión Telegráfica, obteniendo su nombre actual en 1947. Los miembros que integran ITU son representantes de gobierno de cada nación miembro y representantes de un amplio rango de corporaciones y organizaciones. La ITU se divide en tres principales secciones:

- Sector de estandarización de Telecomunicaciones (ITU-T)
- Sector de Radiocomunicaciones (ITU-R)
- Sector de desarrollo (ITU-D)

Los estándares que publica la ITU-T, son conocidos como recomendaciones, y cubren aspectos de comunicación de voz y datos. Está organizada en 15 grupos de estudio:

1. Descripción de Servicio.
2. Operación de la red.
3. Principios de Tarifación y Control.
4. Mantenimiento de la red.
5. Protección contra efectos ambientales electromagnéticos.
6. Planta externa.
7. Redes de datos y Comunicación de sistemas abiertos.
8. Equipo terminal y Protocolos para servicios de telemetría.
9. Transmisión de Sonido y Televisión.
10. Lenguajes para aplicaciones de telecomunicaciones.

11. Conmutación y señalización.
12. Desempeño de la transmisión punto-a-punto.
13. Aspectos de redes en general.
14. Módems y técnicas de transmisión para datos, telegrafía, y servicios de telemetría.
15. Sistemas y equipo de transmisión.

El trabajo de la ITU-T se realiza en ciclos de cuatro años. Cada cuatro años, se lleva a cabo una Conferencia mundial de estandarización de telecomunicaciones. El programa de trabajo para cada nuevo ciclo, se define en la asamblea en donde se someten las preguntas presentadas por los diferentes grupos de estudio, las cuales se basan en los requerimientos que dichos grupos de estudio recibieron por parte de sus miembros. La conferencia valora las preguntas, revisa el alcance de cada grupo de trabajo, crea nuevos grupos de trabajo o elimina grupos existentes, y asigna las preguntas a esos grupos.

Basados en esas preguntas, cada grupo de trabajo prepara un borrador de Recomendaciones. Dicho borrador puede que sea sometido durante la próxima conferencia, cuatro años más tarde, para su aprobación. Sin embargo, es cada día más frecuente, que las Recomendaciones sean aprobadas cuando estas están listas, sin tener que esperar hasta el final del periodo de estudio de cuatro años.

La ITU-T tiene un papel preponderante en los estándares internacionales de redes de área amplia (*WAN, Wide Area Network*). Es responsable de la publicación de las recomendaciones series V y X, que abarcan la comunicación de datos sobre redes telefónicas y redes de datos y la comunicación de sistemas abiertos. El protocolo X.25, es uno de los protocolos más conocidos desarrollados por la ITU-T.

La ITU-R es la responsable de coordinar el uso de las frecuencias de radio.

Y la ITU-D tiene dos funciones principales: promover el compromiso de la ITU para desarrollar proyectos en el área de las telecomunicaciones y administrar los proyectos financiados por las Naciones Unidas en países desarrollados.

Internet Engineering Task Force (IETF)

La IETF es una enorme comunidad internacional abierta de diseñadores de red, operadores, fabricantes, e investigadores interesados con la evolución de la arquitectura de Internet y su operación. Las membresías están disponibles para todo aquel interesado en el tema. El trabajo técnico de la IETF se realiza en grupos *ad hoc* de contribuidores y consultores que desarrollan y publican estándares para las tecnologías de Internet, incluyendo los protocolos TCP/IP.

La publicación de las especificaciones que realizan la IETF y su grupo directivo, la IESG (*Internet Engineering Steering Group*), tienen el formato de documentos Petición de comentarios (*RFC, Request For Comments*). Cualquiera puede escribir una RFC y someterla a la consideración de la IETF. Una vez que la RFC es aprobada, es editada y publicada. La RFC 1294, por ejemplo, especifica el Protocolo de resolución de dirección inverso (*Inverse ARP*).

Modelo de referencia OSI

El modelo de referencia de Interconexión de sistemas abiertos (*OSI, Open System Interconnection*) establece la forma mediante la cual la información de una aplicación de *software* de una computadora, se transfiere a través de la red, hacia una aplicación de *software* en otra computadora. El modelo de referencia OSI es un modelo conceptual compuesto por siete capas o niveles, cada una de las cuales establece funciones de red particulares. El modelo que hoy día conocemos, se basó en el desarrollo de dos modelos independientes, el primero de la Organización internacional de normalización (*ISO, International Organization for Standardization*) y el segundo del Comité consultivo internacional telefónico y telegráfico (*CCITT, Committee Consultative for International Telephone and Telegraph*). En 1984, dichos modelos se consolidaron en un solo documento que ISO publicó como ISO 7498 e ITU-T como X.200. Hoy día, el modelo de referencia OSI, es considerado el principal modelo arquitectónico para la comunicación entre computadoras.

Como ya se mencionó, el modelo OSI divide la tarea de transferir la información entre computadoras conectadas a una red, en siete grupos de trabajo más pequeños y manejables. Cada capa es razonablemente auto-contenida de forma tal que las tareas asignadas a cada una de ellas pueden ser implementadas de forma independiente. Esto permite que las soluciones ofrecidas por cualquiera de las capas, pueda ser actualizada sin afectar contraproducentemente al resto de ellas. Cada computadora de la red utiliza una serie de protocolos para realizar las funciones asignadas a cada nivel. El conjunto de niveles forma lo que se conoce como pila de protocolos. La Fig. 1.8 ilustra las siete capas del modelo de referencia OSI.

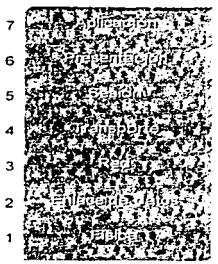


Figura 1.8. El modelo de referencia OSI contiene siete capas independientes

Características de las capas de OSI

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

Las capas superiores tratan asuntos relacionados con aplicaciones y generalmente están implementadas en *software*. La capa mas superior, la capa de aplicación, es la más cercana al usuario final. Tanto el usuario como los procesos de la capa de aplicación interactúan con aplicaciones de *software* que contienen componentes de comunicación. El término capa superior usualmente se refiere a cualquier capa por encima de otra dentro del modelo OSI.

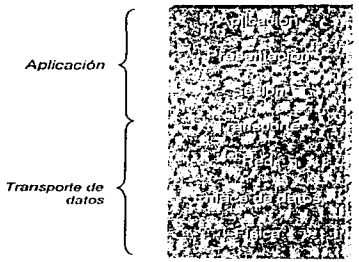


Figura 1.9. Dos grupos de capas componen las capas de OSI.

Las capas inferiores manejan aspectos de transporte de datos. La capa física y la de enlace de datos están implementadas tanto en *hardware* como en *software*. La capa más inferior, la capa física, es la más cercana al medio físico de la red (par de cobre, coaxial, fibra óptica, etc.) y es, de hecho, la responsable de poner la información en el medio. La Fig. 1.9 ilustra la división que existe entre las capas superiores e inferiores del modelo OSI.

Protocolos

El modelo OSI sólo provee un marco conceptual para la comunicación entre computadoras, por lo que, por sí mismo, no es un método de comunicación. Las comunicaciones actuales se realizan por medio del uso de protocolos de comunicación. En el contexto de redes de datos, un protocolo es un grupo formal de reglas y acuerdos que gobiernan la forma en que las computadoras intercambian información sobre la red. Un protocolo puede abarcar las funciones de una o más capas del modelo OSI.

Existe una gran variedad de protocolos de comunicación, entre los que encontramos protocolos para LAN y WAN, de red y de enrutamiento. Los protocolos LAN operan en la capa física y de enlace de datos y definen la comunicación sobre varios medios utilizados en redes LAN. Los protocolos WAN operan en las tres capas inferiores del modelo OSI y definen la comunicación entre varios medios de área amplia. Los protocolos de

enrutamiento son protocolos de la capa de red y son responsables por el intercambio de información entre ruteadores, de forma que, pueden seleccionar la trayectoria más adecuada para enviar el tráfico de red. Finalmente, los protocolos de red, son protocolos que involucran varias capas superiores y que forman parte de una suite de protocolos específica.

Comunicación entre sistemas

La información que es transferida desde una aplicación de *software* en un sistema de cómputo a una aplicación de *software* en otro sistema debe pasar a través de las capas de OSI. Por ejemplo, si una aplicación de *software* en el sistema A tiene información para transmitir a una aplicación de *software* en el sistema B, el programa de aplicación en el sistema A pasará su información a la capa de aplicación del sistema A (capa 7). Entonces la capa de aplicación pasará la información a la capa de presentación (capa 6), la cual transmitirá los datos a la capa de sesión (capa 5), y así hasta llegar a la capa física (capa 1). En la capa física, la información es puesta en el medio de red físico y enviada al sistema B a través del medio. La capa física del sistema B remueve la información del medio físico, y entonces su capa física pasa la información hacia arriba, a la capa de enlace de datos (capa 2), la cual la transfiere a la capa de red (capa 3), y así hasta alcanzar la capa de aplicación (capa 7) del sistema B. Finalmente, la capa de aplicación del sistema B pasa la información al programa de aplicación con lo que se completa el proceso de comunicación.

Comunicación horizontal

Para que dos computadoras se comuniquen por una red, los protocolos utilizados en cada nivel del sistema de transmisión deben estar duplicados en el sistema receptor. Cuando el paquete llega a su destino, el proceso por el que se crean los encabezados se invierte. El paquete pasa hacia arriba por la pila de protocolos y los encabezados se extraen y procesan sucesivamente por el protocolo correspondiente. Esencialmente, los protocolos que operan en los diversos niveles se comunican horizontalmente con sus homólogos en el otro sistema. Las conexiones horizontales entre los diversos niveles son lógicas; no hay comunicación directa entre ellas. La información que el sistema transmisor introduce en el encabezado de cada protocolo es un mensaje que se transfiere al mismo protocolo del sistema destino.

Comunicación vertical

Los encabezados que aplican los diversos protocolos implementan las funciones específicas llevadas a cabo por esos protocolos. Además de realizar una comunicación horizontal con el mismo protocolo del otro sistema, la información del encabezado permite también que cada nivel se comunique con los niveles inmediatamente por encima y por debajo. Por ejemplo, cuando un sistema recibe un paquete y lo pasa hacia arriba a través de la pila de protocolos, el protocolo del nivel de enlace de datos incluye un campo que identifica que protocolo del nivel de red debe utilizar el sistema para procesar el paquete. A su vez, el encabezado del nivel de red especifica un protocolo de los del nivel de transporte y el protocolo del nivel de transporte identifica la aplicación para la que los datos están finalmente destinados.

Interacción entre las capas del modelo OSI

Una capa dada del modelo OSI, generalmente se comunica con otras tres: la capa directamente arriba de ella, la capa directamente debajo de ella, y con su capa homóloga en el otro sistema de computo (sistema remoto). La capa del enlace de datos del sistema A, por ejemplo, se comunica con la capa de red del mismo sistema A, con la capa física también del sistema A, y con la capa de enlace de datos en el sistema B. La Fig. 1.10 ilustra este ejemplo.

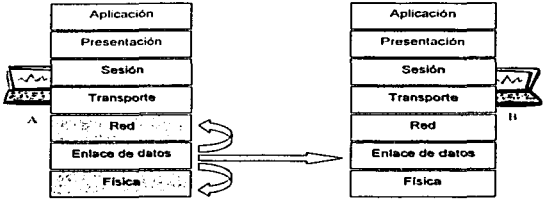


Figura 1.10. Las capas del modelo OSI se comunican entre sí

Servicios de las capas OSI

Una capa OSI se comunica con otra para hacer uso de los servicios suministrados por la segunda capa. Los servicios suministrados por capas adyacentes apoyan a una capa OSI dada a comunicarse con su capa homóloga en otro sistema. Tres elementos básicos están involucrados en los servicios de las capas: el usuario del servicio, el proveedor del servicio, y el punto de acceso al servicio (*SAP, Service Access Point*).

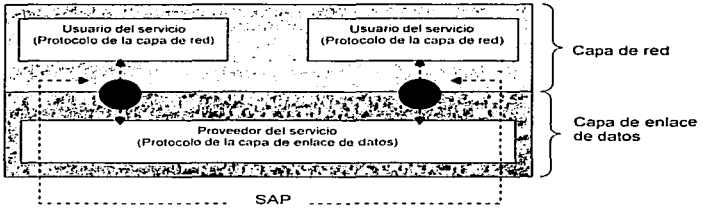


Figura 1.11. Usuarios de servicios, proveedores, y SAPs interactúan en las capas de red y de enlace de datos.

En este contexto, el usuario del servicio es la capa OSI que solicita servicios de la capa OSI adjunta. El proveedor del servicio es la capa OSI que provee el servicio a los usuarios del servicio. Las capas OSI pueden proveer servicios a múltiples usuarios. El punto de acceso al servicio es una ubicación conceptual a la que una capa puede solicitar los servicios de otra. La Fig. 1.11 ilustra como estos tres elementos interactúan en las capas de red y de enlace de datos.

Encapsulación de datos

Los protocolos que operan en los siete niveles funcionan conjuntamente para proporcionar una calidad de servicio unificada. Cada nivel proporciona un servicio a los niveles que están directamente por encima y por debajo del mismo. El tráfico saliente va adquiriendo, por etapas, la información de control necesaria para hacer el viaje hasta su destino, comenzando por protocolos más altos y bajando por la pila de protocolos hasta el medio de transmisión. Esta información de control toma la forma de encabezados (*header*), y en algunos casos de cola (*trailer*), que envuelven los datos recibidos del nivel inmediatamente superior, en un proceso llamada *encapsulación de datos*. La Fig. 1.12 muestra como el encabezado y los datos de una capa OSI cualquiera son encapsulados dentro del encabezado de la siguiente capa inferior.

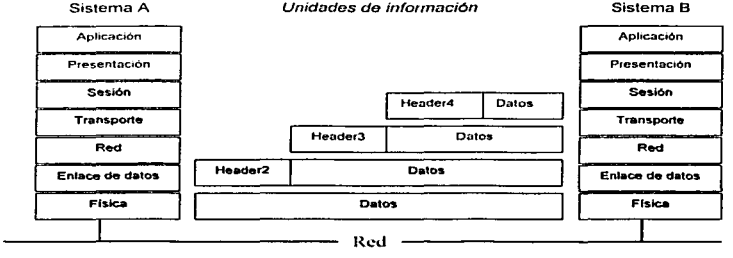


Figura 1.12. Encabezados y datos pueden ser encapsulados durante el intercambio de información

Los encabezados y la cola están compuestos por campos individuales que contienen la información de control necesaria para lograr que el paquete llegue a su destino. En cierto sentido, el encabezado y la cola forman el sobre que lleva el mensaje que proviene del nivel inmediatamente superior.

Los encabezados, las colas, y los datos son conceptos relativos que dependen de la capa OSI en la que se analice la unidad de información. En la capa de red, por ejemplo, una unidad de información consiste del encabezado de la capa 3 y de datos. En la capa de

enlace de datos, sin embargo, toda la información que baja de la capa de red (el encabezado de la capa 3 y los datos) es tratada como datos.

Proceso de intercambio de información

El proceso de intercambio de información ocurre entre capas OSI iguales (homólogas). Cada capa en el sistema fuente añade información de control a los datos. Y cada capa en el sistema destino analiza y remueva la información de control de esos datos.

Si el sistema A tiene datos de una aplicación de *software* para enviarlos al sistema B, los datos son transferidos a la capa de aplicación. Entonces, la capa de aplicación en el sistema A indica, por medio de la adición de un encabezado al principio de los datos, toda la información de control requerida por la capa de aplicación del sistema B. La unidad de información resultante (un encabezado con datos) se pasa a la capa de presentación, la cual añade al principio de aquella su propio encabezado conteniendo información de control dirigida a su capa homóloga en el sistema B. La unidad de información crece en tamaño a medida que cada capa antepone su propio encabezado (y, en algunos casos, una cola) que contiene información de control para ser utilizada por su capa homóloga en el sistema B. En la capa física, la unidad de información completa es puesta en el medio de transmisión.

La capa física en el sistema B recibe la unidad de información pasándola a la capa de enlace de datos. Entonces, la capa de enlace de datos del sistema B lee la información de control contenida en el encabezado antepuesto por la capa de enlace de datos del sistema A. El encabezado es entonces removido, y el resto de la unidad de información es pasada a la capa de red. Cada capa realiza las mismas acciones: lee el encabezado de su capa homóloga, lo remueve, y entrega el resto de la unidad de información a la inmediata capa superior. Después de que la capa de aplicación realiza estas acciones, los datos son pasados a la aplicación de *software* receptora en el sistema B, en la misma forma en la que fue transmitida por la aplicación del sistema A.

Capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de red en comunicación.

Las especificaciones de la capa física definen características como niveles de voltaje, tiempos de cambios de voltaje, tasa de transferencia de datos física, distancias de transmisión máximas, y conectores físicos. La implementación de la capa física puede ser catalogada como especificaciones LAN o WAN. La Fig. 1.13 ilustra algunas de las implementaciones más comunes de la capa física para LAN y WAN.

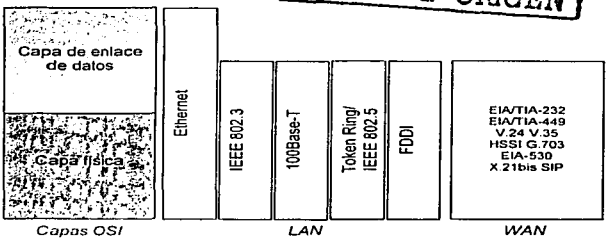


Figura 1.13. Las implementaciones de la capa física pueden ser especificaciones de LAN o WAN

El nivel físico codifica los datos binarios proporcionados por el nivel de enlace de datos, convirtiéndolos en voltajes eléctricos, pulsos de luz u otros impulsos adecuados para su transmisión por el medio físico de la red. El procedimiento de codificación de las señales viene determinado por el protocolo de enlace de datos que se utilice.

Capa de enlace de datos

La misión de la capa de enlace de datos es proveer tránsito fiable de los datos a través de un enlace físico de red. Un protocolo de enlace de datos incluye los siguientes tres elementos:

- El formato de la trama que encapsula los datos del nivel de red.
- El mecanismo que regula el acceso al medio de transmisión compartido.
- Especificaciones para la instalación del nivel físico de la red.

Las especificaciones de la capa de enlace de datos definen las características de red, como el direccionamiento físico, topología de red, detección de errores, secuencia de tramas, y control de flujo.

El direccionamiento físico, incluido en el encabezado del protocolo de enlace de datos, contiene la dirección de la computadora que envía el paquete y de la que lo tiene que recibir. La dirección utilizada en este nivel es la dirección MAC o dirección *hardware*. La topología de red consiste en las especificaciones que definen la forma en la cual los dispositivos están físicamente conectados entre sí, como es el caso de la topología en bus o en anillo. La detección de errores alerta a los protocolos de capas superiores de que un error de transmisión ha ocurrido, y la serie de tramas de datos y tramas vueltas a pedir están fuera de secuencia. Finalmente, el control de flujo modera la transmisión de datos de forma tal que el dispositivo receptor no es saturado con más tráfico del que puede manejar.

El Instituto de Ingenieros Eléctricos y Electrónicos (*IEEE, Institute of Electrical and Electronics Engineers*) ha subdividido la capa de enlace de datos en dos subcapas: Control

de enlace lógico (*LLC, Logical Link Control*) y Control de acceso al medio (*MAC, Media Access Control*). La Fig. 1.14 ilustra las subcapas de la capa de enlace de datos definidas por la IEEE.

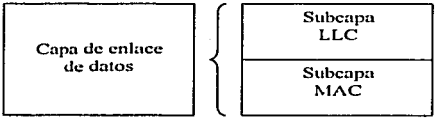


Figura 1.14. La capa de enlace de datos contiene dos subcapas

La subcapa de control de enlace lógico (LLC) maneja la comunicación entre dispositivos sobre un sólo enlace de red, y soporta tanto servicios con conexión como servicios sin conexión (*connection-oriented y connectionless*) utilizados por protocolos de capas superiores. La función de la subcapa LLC está definida en la especificación IEEE 802.2 y establece el número de campos que conforman las tramas de la capa de enlace de datos, habilitando la posibilidad de que múltiples protocolos de capas superiores compartan un solo enlace físico. La subcapa de control de acceso al medio (MAC) maneja el protocolo de acceso al medio físico de red, y define las direcciones *hardware* para identificar de forma inequívoca a múltiples dispositivos de la capa de enlace de datos.

Capa de red

El protocolo del nivel de red es el principal portador, desde el origen hasta el destino, de los mensajes generados en el nivel de aplicación, realizando las siguientes funciones:

- Direccionamiento.
- Enrutamiento.
- Fragmentación y reensamblaje de paquetes.
- Comprobación de errores, entre el sistema de origen y el de destino.
- Identificación del protocolo del nivel de transporte.

A diferencia del protocolo de enlace de datos que sólo se ocupa de que el paquete llegue a su próximo destino en la red local, de nivel de red es responsable del direccionamiento de todo el camino recorrido por el paquete, desde el sistema origen hasta el destino final.

Algunas implementaciones de la capa de red, como el protocolo de Internet (IP), definen direcciones de red en forma tal que la selección de una ruta puede ser determinada sistemáticamente por medio de la comparación de la dirección de red origen con la dirección de red destino y aplicando una mascara de subred.

Como los ruteadores pueden conectar redes que usan diferentes protocolos de enlace de datos, algunas veces es necesario que los sistemas intermedios dividan los datagramas en fragmentos para transmitirlos. Los datagramas o fragmentos de datagramas que son

fragmentados por los sistemas intermedios no se reensamblan hasta que alcanzan su destino final.

Capa de transporte

Una vez alcanzada la capa de transporte, el proceso de llevar los paquetes a su destino ha dejado de ser una preocupación. Los protocolos del nivel de transporte y superiores delegan completamente en los niveles de red y de enlace de datos los servicios de direccionamiento y transmisión. Los paquetes, al ser procesados en los sistemas intermedios, solamente suben hasta el nivel de red, de modo que los protocolos de transporte operan exclusivamente en los sistemas terminales.

Las funciones del nivel de transporte son:

- Identificación del proceso del nivel superior que generó (sistema origen) y que recibirá (sistema destino) el mensaje.
- Segmentación y reensamblaje.
- Control de flujo.
- Detección y corrección de errores.

Los protocolos de transporte de TCP/IP, por ejemplo, utilizan en su encabezado números de puerto para identificar servicios de niveles superiores. Los datos que el nivel de transporte recibe de la capa de sesión son fragmentados para ser transportados a través de la red. El control de flujo usualmente se lleva a cabo en esta capa, y consiste en administrar la transmisión de datos entre dispositivos de forma tal que, el dispositivo transmisor no envíe más datos de los que el receptor pueda procesar. El control de errores involucra la creación de diferentes mecanismos para detectar errores de transmisión, mientras que su corrección involucra acciones, como la solicitud de reenvío de paquetes de datos específicos, para resolver algún posible error.
La multiplexación permite que datos de varias aplicaciones sean transmitidos sobre un solo enlace físico. Los circuitos virtuales son establecidos, mantenidos, y terminados por la capa de transporte. Los protocolos de la capa de transporte utilizados por Internet son TCP y UDP.

Capa de sesión

La capa de sesión establece, administra, y concluye el diálogo entre computadoras. Los dos servicios más importantes atribuidos a esta capa son:

- Control de diálogo.
- Separación de diálogo.

El *control del diálogo* es el medio por el que dos sistemas inician un diálogo, intercambian mensajes y finalmente terminan el diálogo, asegurando que cada sistema ha recibido los mensajes que le correspondían. La *separación de diálogo* es el proceso de insertar un marcador, llamado *punto de comprobación*, dentro del flujo de datos que circula entre dos sistemas, de modo que se pueda evaluar el estado de las dos máquinas en el mismo instante.

Algunos ejemplos de los protocolos implementados en la capa de sesión incluyen el Protocolo de información de zona (*ZIP, Zone Information Protocol*), el Protocolo *Apple Talk* que coordina el proceso de vinculación de nombres; y el Protocolo de control de sesión (*SCP, Session Control Protocol*).

Capa de presentación

La capa de presentación provee una variedad de funciones de codificación y de conversión que son aplicadas a los datos de la capa de aplicación. Estas funciones aseguran que la información enviada por la capa de aplicación hacia un sistema determinado, sea entendible por la capa de aplicación de dicho sistema. Algunos ejemplos de esquemas de codificación y conversión de la capa de presentación incluyen los formatos de representación de datos, conversión de formato de representación de caracteres, esquemas de compresión de datos comunes, y esquemas de encriptamiento de datos comunes.

Los formatos de representación de datos comunes, o del uso de imágenes estándar, sonidos, y formatos de video, permiten el intercambio de datos de aplicación entre diferentes tipos de sistemas de cómputo. Los esquemas de conversión son utilizados para intercambiar información con sistemas por medio del uso de representaciones de datos y texto diferentes, como es el caso de EBCDIC y ASCII. Los esquemas de compresión de datos comunes permiten que datos que fueron comprimidos en el sistema origen sean adecuadamente descomprimidos en el destino. Los esquemas de encriptación de datos estándar habilitan la posibilidad de que los datos encriptados en el dispositivo origen sean correctamente desencriptados en el dispositivo destino.

Algunos de los estándares más conocidos para video incluyen *QuickTime* y *Motion Picture Experts Group* (MPEG). *QuickTime* es una especificación de *Apple Computer* para video y audio, y MPEG es un estándar para compresión de video y codificación.

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

Capa de aplicación

La capa de aplicación es, de las capas OSI, la más cercana al usuario final, lo que significa que tanto la capa de aplicación de OSI como el usuario interactúan directamente con el *software* de aplicación. Dicho de otra manera, el protocolo del nivel de aplicación es la interfaz entre la aplicación demandante de servicios de red, que se ejecuta en la computadora, y la torre de protocolos que convierte esta demanda en las señales transmitidas por la red. Todos los procesos analizados en las secciones previas son iniciados por una aplicación que demanda acceso a un recurso localizado en un sistema de la red.

Algunos ejemplos de implementaciones en la capa de aplicación incluyen *Telnet, File Transfer Protocol* (FTP), y *Simple Mail Transfer Protocol* (SMTP).

Capitulo 2 Repetidores y Concentradores (Hub)

Repetidores

Cuando una señal viaja por un cable, la resistencia natural del medio de transmisión provoca un debilitamiento gradual de aquella hasta que deja de ser viable su "interpretación". Cuanto más largo es el cable, mayor es el debilitamiento de la señal. Este debilitamiento es denominado atenuación, y es una condición que afecta a todos los tipos de cable en mayor o menor medida. El efecto de la atenuación depende del tipo de cable. El cable de cobre, por ejemplo, es mucho más propenso a la atenuación que la fibra óptica. Es una de las razones por las que los segmentos de cable de fibra óptica alcanzan longitudes mayores que los de cobre.

Cuando se construye una LAN, el estándar para el protocolo del nivel de enlace de datos que se pretende utilizar contiene, entre otras, las especificaciones para los tipos cables permitidos y las directrices para su instalación. Dichas directrices incluyen, entre otras cosas, las longitudes máxima y mínima para los cables que conectan las computadoras. La tasa de atenuación del cable es uno de los factores más importantes que afectan a su longitud máxima. Cuando se requiere tender un cable mas allá de la distancia máxima indicada por el estándar se puede utilizar un dispositivo, denominado repetidor, que amplifica la señal, lo que permite que alcance mayores distancias sin atenuarse hasta el punto que resulte ilegible para el sistema destino. En su configuración más sencilla, un repetidor es un dispositivo eléctrico utilizado en una red basada en cobre que recibe una señal por una conexión, la amplifica y la transmite por otra conexión.

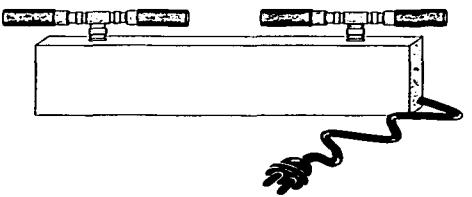


Figura 2.1. Repetidor de red coaxial.

Los repetidores se utilizaron inicialmente en redes de datos para aumentar la longitud de los segmentos de cable coaxial en redes Ethernet. En una red coaxial, como pudiera ser una red Ethernet gruesa o delgada, un repetidor aislado permite extender la longitud máxima del bus más allá de 185 metros, para Ethernet delgada, y 500 metros, para Ethernet gruesa. Este tipo de repetidor es, sencillamente, una pequeña caja con 2 conectores BNC y un cable de alimentación. Utilizando conectores en T y terminadores, como se muestra en la Fig. 2.1, se

conectan dos segmentos de cable al repetidor y este a una fuente de alimentación. Las señales que entran por cualquiera de los dos conectores se amplifican de inmediato y se transmiten por el otro conector.

En una red moderna no es habitual encontrar un repetidor aislado. En la mayoría de los casos, la función de repetición se incluye en otros dispositivos, como concentradores o conmutadores.

Puesto que su función es puramente eléctrica, este tipo de repetidores solamente trabaja en la capa física de la red. El repetidor no puede leer el contenido de los paquetes que viajan por la red: ni siquiera es capaz de saber que se trata de paquetes. El dispositivo amplifica las señales eléctricas que le llegan y la vuelve a enviar. Los repetidores tampoco son capaces de realizar ningún tipo de filtrado de los datos que viajan por la red. Como resultado, dos segmentos de cable unidos por un repetidor, forman un único dominio de colisiones y, por tanto, pertenecen a una misma red. La Fig. 2.2 muestra de forma esquemática la forma en que operan los repetidores.

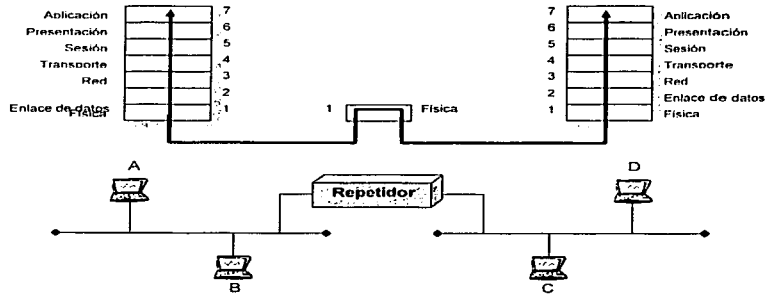


Figura 2.2. Si la estación A envía una trama a la estación B, todas las estaciones (incluyendo la C y D) recibirán la trama.

Concentradores (HUB)

Un concentrador (*Hub*) es un dispositivo que funciona como centro de cableado para una red con topología en estrella. Toda computadora está conectada por cable al concentrador central. La función de concentrador consiste en que el tráfico que llega a cualquiera de sus puertos se propague a través de los demás puertos. En función del medio utilizado en la red, un concentrador utilizará componentes eléctricos, ópticos u otra tecnología para difundir la

señal de entrada por los puertos de salida. Un concentrador de fibra óptica, por ejemplo, utiliza espejos para dividir los impulsos de luz.

El propio concentrador es una caja, independiente o montada en un bastidor, con cierto número de puertos a los que se conectan los cables. Los puertos pueden ser conectores RJ-45 estándar para redes de par trenzado, conectores ST para cable de fibra óptica o cualquier otro tipo de conector utilizado en una red de anillo. En muchos casos los concentradores también disponen de uno o varios LED para cada puerto que se ilumina cuando se conecta un dispositivo, cuando está circulando tráfico o cuando se produce una colisión.
El término concentrador se utiliza, principalmente, en redes Ethernet; el dispositivo equivalente en una red Token Ring se denomina unidad de acceso multiestación (*MAU, multistation access unit*). Los demás protocolos suelen utilizar uno de esos dos términos, en función del mecanismo de de control de acceso al medio (*MAC, media access control*) utilizado. El funcionamiento interno de los concentradores y de las MAU es muy diferente, pero tienen la misma finalidad: conectar un conjunto de computadoras y otros dispositivos en un mismo dominio de colisiones.

Tipos de concentradores

Concentradores pasivos

Al contrario de los repetidores independientes, que son esencialmente iguales, existen muchos tipos de concentradores con diferentes posibilidades. En su forma más sencilla, un concentrador proporciona conexiones de cable pasando a los demás puertos todas las señales que entran en el dispositivo por cualquiera de sus puertos. Esto se conoce como concentrador pasivo, ya que sólo opera en el nivel físico, no tiene inteligencia y no amplifica o modifica la señal de modo alguno. Este tipo de concentrador se utilizó en su día en las redes ARCnet, pero apenas se utiliza en la actualidad.

Concentradores repetidores

Los concentradores utilizados en las actuales redes Ethernet propagan las señales que reciben por cualquiera de sus puertos a través del resto de los puertos del dispositivo de forma simultánea. Esto crea un medio de red compartido y reúne a las computadoras de la red en un mismo dominio de colisiones y de difusión, de la misma forma que si estuvieran conectadas al mismo cable, como en una red Ethernet coaxial. Los concentradores de Ethernet, al igual que los repetidores, amplifican las señales de entrada mientras se propagan hacia los demás puertos. De hecho, los concentradores de Ethernet son en ocasiones conocidos como repetidores multipuerto. Al contrario de un concentrador pasivo, un concentrador activo, o repetidor, necesita una fuente de alimentación para amplificar la señal. Sin embargo, el dispositivo sigue operando en el nivel físico, ya que sólo se ocupa de las señales tal como viajan por los cables.

Algunos concentradores hacen algo más que repetir la señal y, a veces, también la vuelven a ajustar en el tiempo, para sincronizar las transmisiones a través de los puertos de salida. Dichos concentradores utilizan una técnica llamada almacenamiento y reenvío, que implica la lectura del contenido de los paquetes para retransmitirlo por puertos individuales si es

necesario. Un concentrador con estas capacidades puede disminuir el rendimiento de la red para los sistemas que se encuentran conectados a él, debido a los retardos por procesamiento. Sin embargo, se disminuye la pérdida de paquetes y se reduce el número de colisiones.

Otros concentradores de red pequeños incluyen módems en su diseño, lo que permite conectar las computadoras a una LAN y conectar dicha LAN a Internet utilizando un solo dispositivo. Los concentradores utilizados en redes grandes suelen estar diseñados para su apilamiento o para montarse en bastidores estándar de 19 pulgadas, los cuales ofrecen muchos más puertos, así como características para su administración. Sin embargo, la funcionalidad básica de estos concentradores sigue siendo la misma que la de los modelos pequeños.

Como ya se mencionó, un concentrador Ethernet conecta todas las computadoras a un mismo dominio de colisiones, lo que se convierte en un problema para redes pequeñas. Las redes mayores se componen de varios segmentos de red conectados por otros tipos de dispositivos como puentes, conmutadores y ruteadores. Puesto que un concentrador de Ethernet también trabaja como repetidor, cada uno de los cables que conecta al concentrador con una computadora puede tener la longitud máxima indicada por el estándar del protocolo que se esté empleando. Para Ethernet con cable UTP, la longitud máxima es de 100 metros.

En una misma LAN, es posible utilizar varios concentradores, conectados entre sí para formar una red jerárquica en estrella, como se muestra en la Fig. 2.3. Cuando se hace esto con concentradores repetidores estándar, todas las computadoras pertenecen al mismo dominio de colisiones, por lo que es necesario respetar las directrices de configuración del protocolo del nivel de enlace de datos utilizado en la red. Al igual que con los repetidores aislados no es posible conectar más de cuatro concentradores repetidores entre la trayectoria de dos máquinas cualesquiera de una red Ethernet a 10Mbps. Para el caso de redes Fast Ethernet (100Mbps), sólo se permiten 2 concentradores.

NOTA: Debido a que una red Fast Ethernet trabaja diez veces más rápido que una red Ethernet común, las limitaciones en la longitud total de la red son más restrictivas. Para una red Fast Ethernet, la temporización es crítica, ya que el mecanismo CSMA/CD debe ser capaz de operar correctamente en un ambiente en donde los paquetes son los mismos pero viajan a una velocidad diez veces mayor. Además de lo anterior, debemos considerar que los concentradores utilizados en este tipo de redes generan retardos a la señal. Por esta razón, la longitud máxima total de una red Fast Ethernet es de 205 metros, y el número máximo de concentradores en el trayecto entre dos nodos de red, son dos.

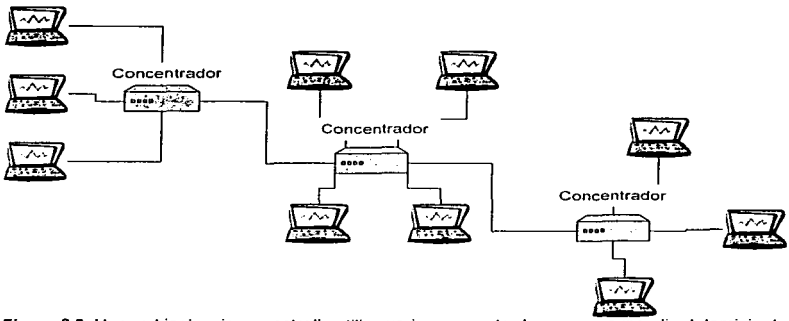


Figura 2.3. Una red jerárquica en estrella utiliza varios concentradores para expandir el dominio de colisiones.

Por ejemplo, si se cuenta con una pequeña red de trabajo en grupo 10Base-T que, llegado el momento, se supera la capacidad del concentrador existente, se puede agregar otro utilizando un cable UTP para conectar el puerto de enlace de subida (*uplink*) de cualquier de ellos con un puerto estándar del otro. Si la red crece aún más, se pueden sustituir los concentradores por modelos con mayor número de puertos o se puede dividir la red en dos LAN, o dos dominios de colisiones, utilizando otro tipo de dispositivos, como puentes, conmutadores o ruteadores.

MAU (Multistation Access Unit) de Token Ring

Las redes de Token Ring también utilizan concentradores, aunque ahí se denominen unidad de acceso multiestación, o MAU (Multistation Access Unit). Aunque una MAU, hacia el exterior realiza la misma función que un concentrador de Ethernet, internamente son muy diferentes. En lugar de pasar el tráfico de entrada a todos los demás puertos simultáneamente, como en un concentrador Ethernet, una MAU transmite un paquete entrante por cada puerto de salida por turno, uno cada vez. Después de transmitir un paquete a una estación de trabajo, la MAU espera hasta que el paquete regrese por el mismo puerto antes de enviarlo por el siguiente. Esto implementa la topología lógica en anillo de la que el protocolo ha tomado el nombre.

Las MAU contienen conmutadores que permiten excluir del anillo puertos específicos, en caso de una falla de cualquier tipo. Esto evita que un mal funcionamiento en una estación de trabajo perturbe la funcionalidad de todo el anillo. Las MAU también disponen de puertos *ring-in* (entrada anillo) y *ring-out* (salida anillo) que se pueden utilizar para extender la red en anillo conectando varias MAU.

Concentradores inteligentes

Los concentradores inteligentes son dispositivos que integran ciertas posibilidades de administración. Un concentrador repetidor básico es, esencialmente, un dispositivo eléctrico que propaga los paquetes de entrada a todos los puertos disponibles sin discriminación de ningún tipo. Los concentradores inteligentes hacen lo mismo, pero además, supervisan el funcionamiento de cada puerto.

Las posibilidades de administración varían enormemente de unos productos a otros, pero muchos concentradores inteligentes utilizan el Protocolo sencillo de administración de red (*SNMP, Simple Network Management Protocol*) para enviar información a una consola centralizada de administración de red, como *Open View*, de Hewlett-Packard. Otros modelos utilizan una terminal conectada directamente al concentrador o una interfaz HTML a la que se puede tener acceso con un navegador de Web desde cualquier punto de la red.

El propósito de estas características de administración consiste en proporcionar al administrador de red una fuente centralizada de información acerca de los concentradores y los sistemas conectados a ellos. Esto evita la necesidad de que el personal de mantenimiento de una red grande se la pase yendo y viniendo de un concentrador a otro para averiguar cual concentrador o sistema ha originado la falla. La consola de administración suele mostrar un modelo gráfico de la red y alerta al administrador cuando se presenta una falla o surge un problema en cualquiera de los sistemas conectados al concentrador.

En redes pequeñas, esta habilidad resulta innecesaria, pero cuando se administra una red empresarial con cientos o miles de nodos, una tecnología que pueda indicar con exactitud cual puerto de un concentrador funciona incorrectamente puede resultar muy útil. El grado de inteligencia incorporado en un concentrador varía enormemente de unos productos/marcas a otros. Existen en el mercado muchos dispositivos híbridos con la inteligencia suficiente para ir más allá de la definición de un concentrador, y proporcionan también funciones de puente, conmutador o ruteador.

Configuraciones de concentradores

Existen concentradores con una gran variedad de tamaños y con muchas características diferentes, desde dispositivos sencillos y pequeños, diseñados para dar servicio a un puñado de computadoras, hasta grandes configuraciones montadas en bastidores para grandes redes empresariales. Desde el punto de vista del diseño de los concentradores, se clasifican en tres categorías, como se muestra a continuación:

- Concentradores Aislados.
- Concentradores Apilables.
- Concentradores Modulares.

Concentradores Aislados

Un concentrador aislado es una caja pequeña, del tamaño de un libro, con un número de puertos que van desde 4 hasta 16. Como su nombre indica, el dispositivo es autosuficiente, dispone de su propia fuente de alimentación y se puede colocar fácilmente encima de un escritorio o debajo de él. Los mini-concentradores de 4 o 5 puertos son adecuados para redes domésticas y para pequeños grupos de trabajo o para proporcionar expansiones rápidas y a medida. Las unidades mayores además de contar con un mayor número de puertos, suelen disponer de LED para indicar la presencia de una señal de pulso de enlace en cada puerto y, posiblemente, la aparición de una colisión en la red.

A pesar del nombre, un concentrador aislado suele disponer de algún mecanismo de conexión a otros concentradores para expandir la red dentro del mismo dominio de colisiones.

Puerto de enlace de subida

Los cables utilizados en una red de pares trenzados se conectan de forma directa, lo que significa que cada una de las ocho terminales del conector RJ-45 de un extremo del cable está conectada con la misma terminal del otro extremo. Las redes UTP utilizan pares de hilos del cable independientes para transmitir y recibir datos. Sin embargo, para que funcione una conexión UTP entre dos computadoras, los contactos de transmisión de cada sistema deben conectarse a los contactos de recepción del otro. Por lo tanto, debe existir un cruce en algún punto de la conexión; tradicionalmente esto ocurre en el concentrador, como se muestra en la Fig. 2.4. Las terminales de cada uno de los puertos del concentrador se conectan a los demás puertos utilizando circuitos de cruce que transponen las señales transporte de datos (*TD, Transport Data*) y recepción de datos (*RD, Receive Data*). Sin este circuito de cruce, se conectarían entre sí los contactos de transmisión de dos sistemas, lo mismo ocurriría con los contactos de recepción, impidiendo cualquier tipo de comunicación.

Figura 2.4. Los concentradores de Ethernet contienen un circuito de cruce para que los cables de red se puedan conectar de forma directa.

Muchos concentradores disponen de un puerto que no posee el circuito de cruce y que se puede utilizar para conectar con otro concentrador. Este puerto se suele etiquetar como *Uplink* (enlace de subida) y a veces tiene un conmutador para seleccionar si el puerto es de cruce o directo. Si existe mas de un concentrador en un sistema, estos se conectan utilizando el enlace de subida de uno de ellos y un puerto estándar del otro. Si se conectan los puertos de enlace de subida de ambos concentradores, los dos circuitos de cruce se cancelarían entre sí y la conexión entre computadoras de un concentrador y una computadora del otro sería equivalente a una conexión directa. Si un concentrador no tiene

puerto de enlace de subida, aún es posible conectarlo a otro concentrador utilizando un puerto estándar y un cable de cruce, que es un cable con las terminales de transmisión de cada extremo conectadas directamente a las terminales de recepción del otro extremo.
El puerto de enlace de subida se suele utilizar para conectar concentradores cuando están a cierta distancia entre ellos y se desea utilizar el mismo tipo de cable en toda la red. A la hora de seleccionar un concentrador, es importante observar cuantos puertos están disponibles para conexión de estaciones de trabajo. Un concentrador que se anuncia con ocho puertos es posible que sólo disponga de siete puertos estándar para la conexión de computadoras y un puerto de enlace de subida sin conmutador. Independientemente del tamaño de la red, la adquisición del concentrador con unos pocos puertos más de los que se necesitan en la actualidad, para futuras expansiones, siempre es una buena idea.

Conexiones para red soporte (troncal)

Algunos concentradores aislados disponen de un puerto de interfaz de unidad de acoplamiento (*AUI, Attachment Unit Interface*) que se puede utilizar para crear una red soporte (troncal), esto es, un segmento de cable independiente que transporta el tráfico entre concentradores. Esta configuración se denomina topología en bus-estrella. Muchos concentradores 10Base-T baratos, por ejemplo, disponen de un conector BNC que se puede utilizar para conectarlo a un segmento de cable coaxial de Ethernet delgada, aunque el conector AUI quizá también admita Ethernet gruesa, cable de fibra óptica o cualquier otro medio. Ethernet delgada es poco utilizada en la actualidad para las nuevas instalaciones de red y no es posible utilizar la topología en bus-estrella en redes Fast Ethernet, ya que el cable coaxial sólo permite velocidades inferiores a 10Mbps.

(Para mayor información sobre Redes de Soporte o Troncales referirse al Apéndice B).

Cuando existen varios concentradores de Ethernet 10Base-T conectados en forma de estrella jerárquica, utilizando sus puertos de enlace de subida, cada fragmento de cable constituye un segmento independiente. Puesto que las directrices de Ethernet sólo permiten la existencia de cinco segmentos en el trayecto entre dos sistemas, conectados por cuatro concentradores. Cuando se conectan utilizando un bus de Ethernet delgada, como se muestra en la Fig. 2.5, sólo se agrega un segmento adicional. En el trayecto entre dos sistemas aparecen, como máximo, tres segmentos, ya que los datos viajan por el bus hacia todos los concentradores al mismo tiempo.

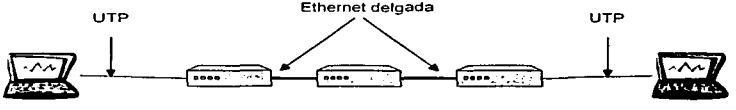


Figura 2.5. Puesto que los dos fragmentos del cable coaxial de Ethernet delgada de este ejemplo forman un único bus, el trayecto entre las dos estaciones de trabajo se compone de tres segmentos, no cuatro.

Cuando se expande aún más este tipo de redes puede aparecer otra limitación de Ethernet no mencionada. El bus que conecta los concentradores se conoce como segmento mixto, ya que a él se conectan más de dos dispositivos. Un segmento que sólo conecta dos dispositivos, como el cable UTP que conecta concentradores por medio del puerto de enlace de subida, se denomina segmento de enlace. De los cinco segmentos permitidos en una LAN 10Base-T, sólo tres pueden ser segmentos mixtos. Esta directriz, que indica que se pueden conectar hasta cinco segmentos utilizando cuatro concentradores y que no pueden ser segmentos mixtos más de tres de ellos, se conoce como la regla 5-4-3 de Ethernet.

Concentradores apilables

Los concentradores apilables ofrecen mayores posibilidades de expansión que los concentradores aislados. Como su nombre lo indica, estos concentradores disponen de carcasas diseñadas para apilar unos encima de otros, pero esa no es la única diferencia. Al contrario que los concentradores aislados, que pueden conectarse en habitaciones o plantas diferentes y estar conectados entre sí, los concentradores apilables suelen estar ubicados en un centro de datos o un armario de conexiones y se conectan entre sí por medio de cables cortos.

Cuando se conectan varios concentradores apilables, forman lo que, funcionalmente, es un único concentrador mayor. Los cables que conectan las unidades no constituyen segmentos independientes, por lo que se pueden interconectar más de cuatro concentradores. Además dichos dispositivos pueden compartir sus capacidades. Una misma unidad inteligente puede administrar sus propios puertos y también los de las demás unidades en conjunto.
Los concentradores apilables poseen su propia fuente de alimentación y pueden trabajar de forma independiente, proporcionando un entorno de mayor expansión u los concentradores aislados. Se puede iniciar con una unidad, sin incurrir en el importante gasto del chasis que utilizan los concentradores modulares, y conectar unidades adicionales a medida que crece la red.

Concentradores modulares

Los concentradores modulares están diseñados para soportar las redes más grandes y proporcionar la mayor flexibilidad y capacidad de expansión. Un concentrador modular consta de un chasis, denominado algunas veces carcasa de tarjetas, que suele ir montado en un bastidor de equipos estándar de 19 pulgadas y que contiene muchas ranuras para enchufar módulos individuales de comunicaciones. El chasis proporciona una alimentación común para todos los módulos, así como una placa posterior que les permite comunicarse entre ellos. Los módulos contienen los puertos a los que se conectan los cables de las computadoras. Cuando se enchufan varios módulos en el chasis, estos se comportan como un único concentrador mayor.

Los concentradores modulares casi siempre incluyen facilidades de administración y son extremadamente flexibles, ya que se pueden insertar en el mismo chasis módulos que admiten diferentes tecnologías. Utilizando diversos módulos se pueden mezclar medios como 100Base-TX y 100Base-FX en el mismo concentrador; mezclar protocolos, como Ethernet y Token Ring o insertar tarjetas de puentes, conmutadores o ruteadores. Algunos

productos modulares incluyen características adicionales de tolerancia a fallas, como ventiladores, fuentes de alimentación y baterías de reserva, así como la posibilidad de sustituir módulos en caliente en caso de que se presente una falla. Resulta fácil imaginar, que los concentradores modulares son los más costosos pero también los más adecuados para instalaciones grandes y permanentes.

En algunos casos, la línea divisoria entre los productos apilables y modulares resulta difícil de distinguir. Existen concentradores apilables con ranuras de expansión que aceptan módulos con puertos adicionales, posibilidades de administración o, incluso, soporte para otros medios, como una red soporte de fibra óptica.

Selección de un concentrador

Cuando se seleccionan concentradores para una red, se puede argumentar que el elemento más importante para tomar la decisión es la planificación de expansiones y crecimientos futuros. Debería adquirirse siempre un concentrador con algunos puertos más de los necesarios, teniendo en cuenta que quizá se desee conectar impresoras, además de estaciones de trabajo, directamente al concentrador. Debería prepararse también un plan de expansión de la red que vaya más allá de un único concentrador.

Planes de crecimiento de una red

Para redes pequeñas son suficientes los concentradores aislados y se pueden expandir conectando otro concentrador al puerto de enlace de subida, o aun puerto estándar utilizando un cable de cruce. Ésta es también una buena solución si se desea ubicar concentradores en lugares diferentes, ya que el cable de conexión entre dos concentradores puede tener una longitud de hasta 100 metros en una red Ethernet con UTP.

Sin embargo, hay que tener conciencia del límite en el número de repetidores impuesto por los estándares de Ethernet, así como la longitud máxima del cable. En una red LAN Ethernet 10Base-T sólo se permiten cuatro concentradores y dos en una 100Base-T Clase II. Si se tiene la sospecha de que una red va a crecer más de lo que esa configuración puede admitir, sería aconsejable adquirir un concentrador apilable para una futura expansión.

Los concentradores apilables constituyen una excelente elección para redes medianas, ya que pueden proporcionar gran parte de la flexibilidad de los concentradores modulares, con una inversión inicial relativamente modesta. Es posible adquirir una sola unidad para empezar y, posteriormente, agregar otras que proporcionen puertos adicionales o características nuevas, como funciones de administración de red o soporte para otros protocolos.

Puesto que los concentradores apilables se conectan formando una sola unidad, no hay que preocuparse de los límites de los repetidores de Ethernet a menos que existan varios conjuntos de concentradores en diferentes ubicaciones. Pero hay que tener en cuenta que los concentradores apilables no se pueden expandir hasta el infinito. Hay que averiguar el número máximo de unidades que se pueden interconectar, ya que este valor difiere enormemente de unos productos a otros.

Los concentradores apilables utilizan cables cortos para conectarse entre sí, por lo que todas las unidades deben estar juntas, normalmente en un armario de conexiones u otro lugar seguro. Este tipo de disposición requiere una mejor planificación que la que se requeriría para concentradores aislados, que se pueden colocar en cualquier sitio en donde se requieran puertos adicionales. Para los concentradores apilables hay que elegir una ubicación que sea, más o menos, equidistante a todas las estaciones de trabajo que se desea conectar y que se disponga de una fuente de alimentación confiable. Es importante tener en cuenta que si los concentradores dejan de trabajar, la red deja de funcionar, aunque las PC estén protegidas con fuentes de alimentación ininterrumpida (*UPS, Uninterruptible Power Supply*). Los concentradores apilables poseen también la ventaja de que se pueden trasladar con facilidad por la oficina, e incluso a un lugar completamente distinto.

Los concentradores modulares requieren la mayor planificación y la inversión inicial más elevada, ya que es necesario comprar un chasis y las tarjetas que se van a montar en él, con los puertos. Los concentradores modulares se suelen montar de forma permanente en un centro de datos o en un cuarto de conexiones, lo que significa que también hay que también hay que tomar en cuenta controles medioambientales y seguridad física para la ubicación de la unidad. La inversión en concentradores modulares suele ser un compromiso a largo plazo, ya que resultan adecuados para grandes redes que requieren una enorme flexibilidad y posibilidad de expansión. Se asume que la red crecerá d manera importante con el tiempo y que requerirá diversas tecnologías para lograr ese crecimiento. Hay que considerar escenarios como la posibilidad de que la empresa se fusione con otra y sea necesario combinar diferentes tipos de redes.

Planes de mejora de una red

La otra preocupación principal en lo que se refiere a la compra de concentradores en la actualidad es si se va a realizar una ampliación de velocidad en la red en un futuro cercano. Por ejemplo, si actualmente se cuenta con una red 10Base-T, quizá se desee pasar a algunas de las estaciones de trabajo a Fast Ethernet (100Base-T) en algún momento.

Los concentradores Ethernet pueden admitir 10Base-T, Fast Ethernet o ambos. Al contrario de las tarjetas de red, no todos los concentradores de Fast Ethernet son capaces de trabajar tanto a 10Mbps como a 100Mbps. Si se opta por concentradores de velocidad única, es necesario disponer de segmentos de red diferentes para los equipos que trabajan a cada una de las velocidades, y de dos NIC (*Network Interface Card*) en las computadoras que tengan acceso a las dos redes. Si se decide gastar un poco más y adquirir concentradores de dos velocidades, cada uno de los puertos del concentrador negocia de forma automática la mejor velocidad posible con la computadora a la que está conectando.

Los concentradores de velocidad dual trabajan manteniendo un segmento lógico independiente dentro de la unidad para cada velocidad y a veces utilizan un conmutador de dos puertos para pasar los datos entre segmentos, de forma que sólo pasen los datos destinados al otro segmento. En algunas configuraciones de concentradores apilables, el conmutador se encuentra en un concentrador "maestro" que da servicio a todos los demás concentradores "clientes" de la pila. Esto ahorra dinero al hacer posible la conmutación

entre los segmentos de los concentradores interconectados sin tener que pagar circuitos de conmutación redundante para cada unidad.

Los concentradores de dos velocidades también simplifican la migración entre Ethernet estándar y Fast Ethernet. No es necesario contar con dos NIC en los servidores y otros sistemas compartidos, ya que el concentrador proporciona una ruta entre los dos segmentos de red. Tampoco es necesario cambiar ninguna de las NIC de las estaciones de trabajo cuando se instala el concentrador. Una vez que el dispositivo está en su lugar, los sistemas 10Base-T siguen funcionando normalmente. Posteriormente se pueden reemplazar las NIC 10Base-T por un modelo 100Base-T en aquellas estaciones de trabajo que se desee. De forma tal que, al arrancar la estación de trabajo, la nueva NIC se conectará con el concentrador a 100Mbps agregándose al segmento de alta velocidad.

Por supuesto que los concentradores de dos velocidades son significativamente más caros que los modelos que manejan una sola velocidad. Por lo que la decisión de adquirir uno u otro modelo, dependerá en que etapa del proceso de migración nos encontremos. Por ejemplo, si gran parte de la red ya maneja Fast Ethernet y sólo quedan unas pocas estaciones a 10Mbps, invertir gran cantidad de dinero extra en concentradores de dos velocidades probablemente no se justifique cuando se podría instalar Fast Ethernet en las estaciones faltantes en tan sólo un fin de semana. Por el contrario, si aún se trabaja con 10Base-T en toda la red y la migración a Fast Ethernet aún se encuentra en la fase de planificación, los concentradores de dos velocidades pueden resultar la solución ideal.

Capitulo 3 Puentes (Bridge)

Descripción

Un puente (bridge) es un dispositivo utilizado para conectar segmentos de cable LAN, pero a diferencia de los concentradores, opera en el nivel de enlace de datos del modelo OSI y es selectivo respecto a los paquetes que pasan a través de él. Los Puentes y los concentradores están diseñados para propagar, a través de todos los segmentos de cables a los que están conectados, todo el tráfico de red que reciben.

Un puente posee dos o más interfaces de red, con sus propias direcciones MAC, con sus puertos conectados a distintos segmentos de cable y operando en modo promiscuo, es decir, las interfaces reciben todos los paquetes transmitidas por los segmentos a los que están conectados. Cuando un paquete entra en el puente, el dispositivo lee su dirección destino de la cabecera del protocolo del nivel de enlace de datos, y si se trata de un paquete para un sistema en otro segmento, lo reenvía hacia dicho segmento. Si el sistema destino del paquete se encuentra en el mismo segmento por el que ha llegado, el puente descarta el paquete, pues ya habrá llegado a su destino. Este proceso se denomina filtrado de paquetes. El filtrado de paquetes es uno de los principios fundamentales utilizados por los dispositivos de conexión de red para regular el tráfico en la red.

En este caso, el filtrado de paquetes se realiza en el nivel de enlace de datos, pero también puede ocurrir en los niveles de red y de transporte.

La posibilidad de leer el contenido de la cabecera de un paquete eleva al puente por encima del nivel de un concentrador o repetidor, los cuales sólo se ocupan de señales individuales. Sin embargo, al igual que con un concentrador o un repetidor, el puente no realiza ningún tipo de modificación en el paquete y desconoce por completo el contenido de la trama de enlace de datos. Por lo que no es necesario tomar en cuenta los protocolos del nivel de red y superiores al momento de seleccionar un puente.

Al utilizar el filtrado de paquetes, el puente reduce la cantidad de tráfico de la red, ya que no propaga los paquetes de forma innecesaria. Sin embargo, los mensajes de difusión se reenvían a todos los segmentos conectados, permitiendo la utilización de protocolos que se basan en la difusión, como NetBEUI, sin tener que realizar una configuración manual del sistema. Al contrario de un concentrador o repetidor, un puente no retransmite datos a los segmentos conectados hasta que recibe todo el paquete. Recuérdese que los concentradores y repetidores trabajan con señales, mientras que los puentes trabajan con paquetes. Por este motivo, dos sistemas en segmentos separados por un puente pueden transmitir de forma simultánea sin que se produzca una colisión. Por lo anterior, podemos establecer que un puente conecta segmentos de red de tal forma que les mantiene en el mismo dominio de difusión pero en diferentes dominios de colisiones. Sin embargo, se puede considerar que los segmentos forman parte de la misma LAN.

Si, por ejemplo, se cuenta con una LAN en la que se detecta una disminución en su desempeño debido a un elevado nivel de tráfico, se puede dividir en dos segmentos

colocando un puente en un punto intermedio de dicha LAN. Esto hará que el tráfico local generado en cada segmento, permanezca en dicho segmento y sólo el tráfico de difusión y el tráfico con destino al otro segmento, pasen a través del puente. En una red Ethernet, la reducción del tráfico de esta forma también reduce el número de colisiones, lo que incrementa considerablemente el desempeño de la red. Los puentes también proporcionan las mismas funciones de repetición que un concentrador, lo que permite extender la longitud del cable.

Modo de operación

Existen dos principales modelos de operación utilizados por los puentes, los cuales fueron diseñados para satisfacer los requerimientos de los dos "principales mercados del Mundo", el americano y el resto del Mundo. Sin embargo, ambos productos cumplen con las mismas funciones, es decir, filtrar y reenviar paquetes. Lo que cambia es el método que utilizan para realizar dichas funciones. Dichos modelos son:

- Puentes transparentes
- Puentes con enrutamiento en origen

Puentes transparentes

Para filtrar de forma efectiva los paquetes que le llegan, un puente tiene que conocer que sistemas están conectados en cada segmento de red y así decidir que paquetes debe reenviar y cuales descartar. El puente almacena esta información en una tabla de direcciones interna. Inicialmente, los administradores de red tenían que crear la tabla de direcciones de un puente de forma manual, pero los puentes actuales recopilan la información de la tabla de direcciones de forma automática, un proceso denominado puentes transparentes.

Tan pronto como un puente transparente, conocido también como puente aprendiz, se conecta a los segmentos de red, comienza a compilar su tabla de direcciones. Leyendo las direcciones origen de los paquetes que le llegan y anotando la interfaz por la que llegan, el puente puede construir una tabla de direcciones de nodo para cada segmento al que está conectado.

Imaginemos una red compuesta de tres segmentos, A, B y C, todos ellos conectados a un puente local, como se muestra en la Fig. 3.1. Cuando el puente se activa por primera vez, recibe un paquete del Nodo 1 por la interfaz de Red A y destinado al Nodo 2 de la Red B. Puesto que ahora ya sabe que el Nodo 1 pertenece a la Red A, crea una entrada en su tabla para la Red A que contiene la dirección MAC del Nodo 1.

En este momento, el puente no posee información del Nodo 2 ni el segmento en el que se encuentra, por lo que transmite el paquete a las Redes B y C, esto es, a todos los segmentos excepto por el que ha llegado el paquete. Éste es el comportamiento de un puente cuando recibe un paquete destinado a un sistema que no aparece en sus tablas. Transmite el paquete a los demás segmentos para asegurarse de que llega a su destino.

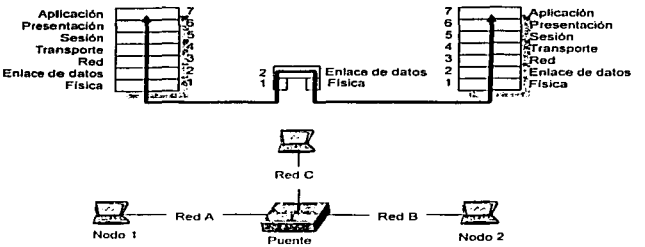


Figura 3.1. Un puente transparente reenvía los paquetes en función de la tabla de direcciones que compila a partir de los paquetes transmitidos previamente.

Cuando el Nodo 2 recibe el paquete, transmite una respuesta al Nodo 1. Puesto que el Nodo 2 se encuentra en la Red B, su paquete de respuesta llega al puente por una interfaz diferente. Ahora el puente puede agregar una nueva entrada a su tabla para la Red B que contiene la dirección MAC del Nodo 2. Al examinar el paquete, el puente busca la dirección destino en su tabla, y descubre que pertenece al Nodo 1, en Red A. A continuación, el puente transmite el paquete exclusivamente por la interfaz de la Red A.

A partir de este momento, cuando cualquier otro sistema de la red A transmite un paquete para el Nodo 1, el puente sabe que tiene que descartarlo sin pasarlo a los demás segmentos. Sin embargo, el puente sigue utilizando esos paquetes para agregar la estación transmisora a su tabla de direcciones para Red A.

Al final, el puente dispondrá, en su tabla de direcciones, de las entradas para todos los nodos de la red y podrá dirigir todos los paquetes que le lleguen a los puertos de salida adecuados.

Bucles de puentes

Cuando los segmentos de una red se conectan utilizando puentes, el fallo o mal funcionamiento de un puente puede resultar catastrófico. Por este motivo, los administradores suelen conectar los segmentos de red con puentes redundantes, para garantizar que todo nodo puede tener acceso a toda la red aunque falle uno de los puentes.

En la Fig. 3.2 aparecen tres segmentos conectados por dos puentes. Si uno de los puentes falla, uno de los segmentos quedaría aislado del resto de la red. Para remediar este problema y proporcionar tolerancia frente a fallos se puede agregar un tercer puente que conecte los dos segmentos de los extremos, como se muestra en la Fig. 3.3.

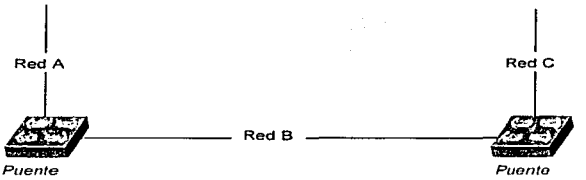


Figura 3.2. Cuando los segmentos se conectan entre sí utilizando un puente, se crea un punto de fallo único.

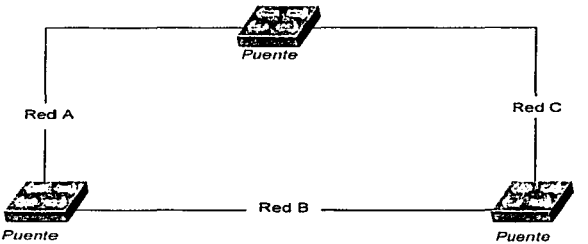


Figura 3.3. La conexión de cada uno de los segmentos a dos puentes, proporciona tolerancia a fallas.

De esta forma, todo sistema cuenta con dos rutas posibles para acceder a los demás segmentos.

La instalación de puentes redundantes es una buena idea, pero provoco lo que pudiera convertirse en un serio problema. Cuando una computadora, Nodo 1, se encuentra en un segmento conectado a dos puentes, como se muestra en la Fig. 3.4, ambos puentes recibirán el primer paquete que transmita el sistema y agregarán la dirección de la máquina a su tabla para ese segmento, Red A. Ambos puentes transmitirán, a continuación, el mismo paquete al otro segmento, Red B. Como consecuencia ambos puentes recibirán el paquete reenviado por el otro puente.

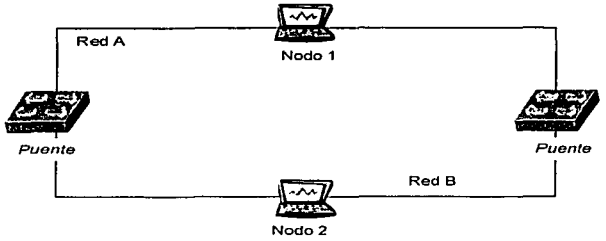


Figura 3.4. Los puentes redundantes proporcionan tolerancia frente a fallos, pero también pueden crear bucles y tormentas de difusión.

La cabecera del paquete seguirá mostrando la dirección del Nodo 1 como origen, pero ahora los puentes han recibido el paquete por la interfaz de Red B. Como resultado, los puentes quizá modifiquen sus tablas de direcciones para registrar que el Nodo 1 pertenece a la Red B, no a la Red A. Si esto ocurre, cualquier transmisión posterior desde el Nodo 2, en red B, dirigida al Nodo 1 se descartará, pues los puentes piensan que le Nodo 1 pertenece a la Red B, cuando de hecho, se encuentra en la Red A.

El resultado es una pérdida de datos, ya que los puentes descartan tramas de forma incorrecta, y una degradación de rendimiento de la red. Al final, las entradas incorrectas de la tabla de direcciones de los puentes expiraran o se modificarán, pro, mientras tanto, el Nodo 1 no estará accesible para los sistemas de los demás segmentos de red.

Si este problema no fuera suficientemente malo, lo que ocurre cuando el Nodo 1 transmite una difusión es mucho peor. Ambos puentes reenvían el paquete a la Red B, donde, como ya se explicó, lo recibe el otro puente, reenviándolo de nuevo. Puesto que los puentes siempre reenvían los paquetes de difusión sin filtrarlos, ente los dos segmentos circularían varias copias del mismo mensaje por tiempo indefinido, siendo reenviados constantemente por los dos puentes. Esto es conocido como tormenta de difusión y puede impedir que el resto del tráfico de la red llegue a su destino.

Algoritmo del árbol de expansión

Para tratar de resolver el problema de los bucles sin fin y las tormentas de difusión en redes con puentes redundantes, *Digital Equipment Corporation* ideó el algoritmo del árbol de expansión *(SPA, SPanning tree Algorithm)*, que mantiene la tolerancia frente a fallos proporcionada por los puentes adicionales y evita los bucles sin fin.

El *Institute of Electrical and Electronic Engineers (IEEE)* revisó posteriormente el SPA y lo normalizó en la especificación 802.1d.

El algoritmo del árbol de expansión funciona seleccionando un solo puente de cada segmento de red que dispone de varios de ellos. Este puente es el responsable de todas las tareas de filtrado de paquetes y reenvío para el segmento. Los demás permanecen inactivos, pero preparados para tomar el control si el puente designado falla.

Durante el proceso de selección, a cada puente se le asigna un identificador único, utilizando una de las direcciones MAC del puente más un valor de prioridad, al igual que a cada puerto individual de cada puente, utilizando la dirección MAC del puerto. Cada uno de los puertos se asocia también con un costo de trayecto, que indica el costo de transmitir un paquete por la LAN utilizando dicho puerto. Los costos de trayecto son establecidos por el administrador cuando existe una razón para preferir un puerto antes que otro, o se pueden dejar los valores predeterminados.

Una vez identificados todos los componentes, el puente con menor identificador se convierte en puente raíz para toda la red. Cada uno de los puentes restantes determina, a continuación, cual de los puertos puede alcanzar el puente raíz con el menor costo, lo que se denomina costo de trayecto raíz, y lo designa como puerto raíz para ese puente.
Por último, para cada segmento de red se selecciona un puente designado, así como un puerto designado en ese puente. Sólo el puerto designado del puente designado puede filtrar y reenviar los paquetes para ese segmento de red. Los demás puentes de ese segmento, puentes redundantes, se mantienen "pasivos", para tomar eventualmente el control en caso de que le puente designado falle. En el momento en que sólo opera un puente en cada segmento, se pueden reenviar los paquetes sin que se formen bucles.

Para realizar los cálculos, los puentes tienen que intercambiar mensajes entre ellos, utilizando un formato de mensaje definido por el estándar 802.1d, como se muestra en la Fig. 3.5. Dichos mensajes se conocen como unidades de datos del protocolo de puentes (*BPDU, Bridge Protocol Data Unit*) y contienen los siguientes datos:

Campo	Long. [bytes]	Descripción
Identificador de protocolo	2	Siempre contiene el valor 0
Versión	1	Siempre contiene el valor 0
Tipo de mensaje	1	Siempre contiene el valor 0
Banderas	1	Contiene dos banderas de un bit, utilizando los siguientes valores: Bit 1 Cambio de topología. Indica que se envía el mensaje para solicitar una modificación en la topología de red. Bit 2 Confirmación de cambio de topología. Utilizado como acuse de recibo de un mensaje con el bit de cambio de topología activado.
Identificación Raíz	8	Indicar el puente raíz especificando su valor de prioridad de 2 bytes seguido de su dirección MAC de 6 bytes

Costo de trayecto raíz	4	Indica el costo de trayecto desde el puente que envía el mensaje BPDU hasta el puente raíz
Identificación de puente	8	Identifica al puente que envía el mensaje, especificando su valor de prioridad de dos bytes seguido de su dirección MAC de 6 bytes
Identificación de puerto	2	Indica el puerto por el que se envía el mensaje
Edad del mensaje	2	Indica el tiempo transcurrido desde que el puente raíz transmitió el mensaje que originó el mensaje actual
Edad máxima	2	Indica la edad a la que debe eliminarse el mensaje
Tiempo de saludo	2	Indica el intervalo de tiempo entre los mensajes de configuración del puente raíz
Retardo de reenvío	2	Indica el intervalo de tiempo que deberían esperar los puentes para completar el algoritmo del árbol de expansión después de una modificación de la topología de red. Las transiciones de estado prematuras pueden originar la formación de bucles si algunos puentes no han terminado el algoritmo

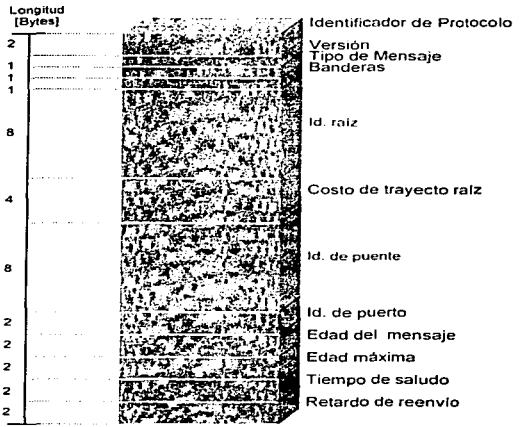


Figura 3.5. Formato del mensaje de unidad de datos del protocolo de puente utilizado durante los cálculos del algoritmo del árbol de expansión.

Los mensajes BPDU se encapsulan en tramas estándar del protocolo del nivel de enlace de datos utilizando el valor *SAP (Service Advertising Protocol)* 01000010 y se dirigen a la dirección de multidifusión "todos los puentes". Los puentes generan los mensajes de forma autónoma, pero no los reenvían a otras redes. Por lo tanto, todas las BPDU intercambiadas por puentes se quedan en los segmentos de red conectados directamente a los puertos.

NOTA: El Protocolo de anuncio de servicios (*SAP, Service Advertising Protocol*) sirve para recopilar información acerca de otros equipos conectados a la red, como es el caso de puentes, ruteadores multiprotocolo, servidores de archivos, servidores de impresión, servidores de pasarela, etc.

Al igual que ocurre con el proceso de aprendizaje, el algoritmo del árbol de expansión comienza tan pronto como se conectan los puentes a la red y se encienden. Inicialmente, todos los puentes asumen que serán un puente raíz y utilizan un costo de trayecto 0, pero a medida que reciben mensajes BPDU de los demás puentes del segmento comparan la información de dichos mensajes y deciden que puente resulta más adecuado para realizar las tareas de puente para el segmento. El algoritmo para tomar esa decisión se basa en los valores de los criterios siguientes, por orden:

- Identificación raíz
- Costo de trayecto raíz
- Identificación de puente
- Identificación de puerto

Para todos los criterios, un valor menor es mejor que un valor mayor. Si un puente recibe un mensaje BPDU con valores mejores que los de sus propios mensajes, deja de transmitir las BPDU por el puerto por el que ha llegado, reconociendo la responsabilidad del puente más adecuado para el trabajo. El puente utiliza también los valores de esa BPDU de entrada para volver a calcular los campos de los mensajes que enviará por los demás puertos.
Una vez que el algoritmo del árbol de expansión designa un puente para cada segmento de red, tiene que seguir supervisando la red de forma que el proceso pueda comenzar de nuevo cuando algún puente falle o se quede fuera de línea. Todos los puentes de red almacenan las BPDU recibidas de los demás puentes y consultan su edad. Cuando un mensaje exceda la edad máxima permitida se descarta y comienza de nuevo el intercambio de mensajes del árbol de expansión.

Además, a intervalos periódicos especificados por el valor del campo Tiempo de saludo, el puente raíz transmite una nueva BPDU con un valor 0 de edad de mensaje. Esto hace que los demás puentes de la red actúen de la misma forma. Si uno de los puentes de un segmento de red no transmite mensajes BPDU, los demás realizan de nuevo todo el algoritmo para seleccionar un nuevo puente designado para el segmento. Un mensaje de 4 bytes de cambio de topología indica a los demás puentes que comiencen de nuevo el algoritmo. Este mensaje sólo contiene los campos identificador de protocolo, Versión y Tipo de mensaje del formato de BPDU, con el valor 0 para los dos primeros campos y el valor 128 para el campo Tipo de mensaje.

Puentes con carga compartida

En el caso de puentes remotos que conectan segmentos de red utilizando enlaces WAN, no tiene sentido pagar una línea alquilada redundante o cualquier otro enlace de telecomunicaciones caro para que permanezca sin utilizar como resultado del algoritmo del árbol de expansión. Para afrontar este problema, existen en el mercado puentes de carga compartida que pueden utilizar el enlace WAN de reserva para transportar datos sin que se produzcan bucles indefinidos ni tormentas de difusión.

Puentes con enrutamiento en origen

Los puentes con enrutamiento en origen son una alternativa para los puentes transparentes desarrollada por IBM para redes Token Ring multisegmento y normalizada en IEEE 802.5. En una red que utiliza puentes transparentes, los puentes designados por el algoritmo del árbol de expansión determinan la ruta que toma un paquete hacia su destino en otro segmento. En los *puentes con enrutamiento en origen*, es la estación de trabajo la que determina la ruta hacia el sistema destino y la incluye en cada paquete individual.

Para descubrir las posibles rutas a través de la red hacia un determinado destino, un sistema Token Ring transmite una trama de difusión hacia todos los anillos (*ARB, All Rings Broadcast*), y todos los puentes la reenvían a los anillos a los que están conectados. Cuando un puente procesa la trama agrega, al paquete, su indicador de trayecto (*RD, Route Designator*), indicando el puente y puerto. Leyendo la lista de RD, los puentes evitan los bucles, pues no envían el paquete al mismo puente dos veces.

Si existe más de una ruta hacia el sistema destino, llegarán varias ARB conteniendo información acerca de las diferentes rutas recorridas. El sistema destino transmite, a continuación, una respuesta por cada una de las ARB que recibe, utilizando la lista de RD para enrutar el paquete hacia el emisor.

Cuando el emisor original de las ARB recibe las respuestas, selecciona la mejor ruta, en función de uno o varios de los siguientes criterios:

- El intervalo de tiempo necesario para que la trama de exploración regrese al emisor.
- El número de saltos entre origen y destino.
- El tamaño de trama que puede utilizar el sistema.

Después de seleccionar una de las rutas, el sistema genera los paquetes de datos e incluye la información de enrutamiento en la cabecera de trama de Token Ring.

El formato de un paquete ARB y de un paquete de datos con información de enrutamiento es el mismo que el de una trama IEEE 802.5 estándar, excepto que el primer bit del campo dirección origen, denominado *indicador de información de enrutamiento* (*RII, Route Information Indicator*) tiene el valor 1, lo que indica que el paquete contiene información de enrutamiento. Dicha información, que consiste en una lista con los puentes que utilizará el paquete al viajar por la red, aparece en *el campo información de enrutamiento* (*RIF,*

Routing Information Field), que forma parte del campo de información, a continuación del campo *dirección origen* de la trama (ver Fig. 3.6).

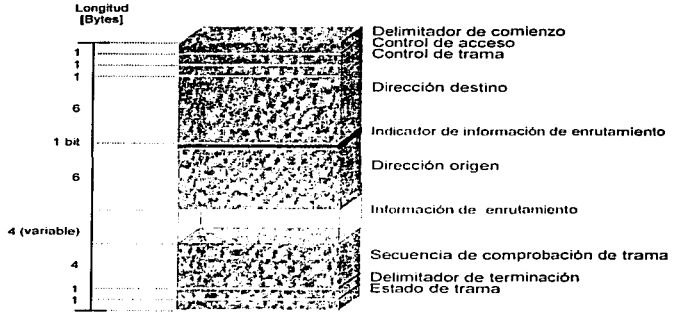


Figura 3.6. Indicador de información de enrutamiento y campo de información de enrutamiento utilizados en los puentes con enrutamiento en origen, dentro de una trama Token Ring estándar.

El RIF consta de una sección de control de enrutamiento, de 2 bytes, y una serie de secciones de 2 bytes de indicador de trayecto, como se muestra en la Fig. 3.7. La sección de control de enrutamiento contiene los siguientes campos:

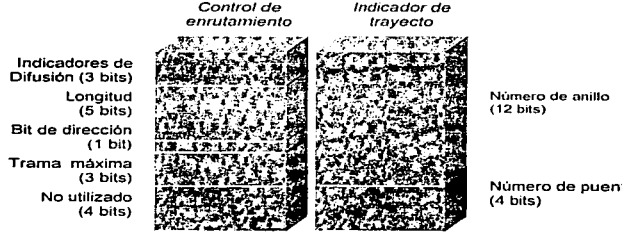


Figura 3.7. El campo información de enrutamiento indica que puentes utilizará el paquete en su recorrido a través de la red.

Campo	Long. [bits]	Descripción
Indicadores de difusión	3	Indica el tipo de enrutamiento utilizado por la trama, de acuerdo a los valores siguientes: 000 – No difusión Indica que el paquete contiene una ruta específica hacia el destino, en las secciones de indicador de trayecto del campo RIF. 100 – Difusión a todas las rutas Indica que el paquete debería enrutarse a través de todos los puentes de la red, sin atravesar dos veces el mismo puente, y que cada uno de los puentes debería agregar una sección de indicador de trayecto al campo RIF indicando el puente y el puerto por el que lo reenvía. 110 – Difusión de ruta única Indica que el paquete debería enrutarse exclusivamente a través de los puntes designados por el *algoritmo del árbol de expansión* [ver nota] y que cada uno de los puentes debería agregar una sección de indicador de trayecto al campo RIF indicando el puente y el puerto por el que lo reenvía.
Longitud	5	Indica la longitud total del campo RIF, entre 2 y 30 bytes.
Bit de dirección	1	Especifica en que dirección viaja el paquete. El valor de este bit indica al nuevo nodo transmisor si debería leer las secciones de indicador de trayecto del campo RIF de izquierda a derecha (0) o de derecha a izquierda (1).
Trama máxima	3	Indica el tamaño máximo de trama que es posible transportar por la ruta, denominado *unidad máxima de transferencia* (*MTU, Maximum Transfer Unit*). Establecida inicialmente por el sistema emisor, un puente reduce su valor si reenvía el paquete a un segmento que sólo admite tramas menores. Los valores permitidos son los siguientes: 000 Indica una MTU de MAC de 552 bytes. 001 Indica una MTU de MAC de 1.064 bytes. 010 Indica una MTU de MAC de 2.088 bytes. 011 Indica una MTU de MAC de 4.136 bytes. 100 Indica una MTU de MAC de 8.232 bytes.
No utilizado	4	
Número de anillo	12	Indica de forma única el segmento de red (anillo).
Número de puente	2	Identifica un puente específico en la red, utilizando un valor que tiene que ser único entre los puentes conectados a ese segmento de red (anillo).

NOTA: El algoritmo del árbol de expansión que utilizan los puentes con enrutamiento en origen para la difusión de ruta única no es igual al algoritmo del mismo nombre utilizado por los puentes transparentes.

Los puentes con enrutamiento en origen son un método relativamente poco eficiente, debido a que se apoyan demasiado en las transmisiones de difusión que se propagan a través de todos los segmentos de la red. Además de que cada una de las estaciones de trabajo debe mantener su propia información de enrutamiento a cada uno de los sistemas con los que desea comunicarse. Esto puede representar para un sistema destino el procesamiento de una gran cantidad de tramas ARB antes de ver siquiera el primer byte de los datos de aplicación.

Tipos de Puentes

Existen tres tipos básicos de puentes, que son:

Locales. Un puente local proporciona servicios de filtrado de paquetes y repetición para segmentos de red del mismo tipo. Este tipo de dispositivos son conocidos como puentes de nivel MAC, ya que los datos que llegan al puente sólo tienen que subir, en la pila de protocolos, hasta el subnivel de control de acceso al medio (MAC, Media Access Control), es decir, el subnivel inferior de los dos que forman el nivel de enlace de datos, siendo el otro el subnivel de control del enlace lógico (*LLC, Logical Link Control*). Se trata del tipo de puente más sencillo, ya que no se requiere almacenar o traducir los paquetes. El dispositivo, sencillamente, propaga los paquetes que llegan a los puertos adecuados o los descarta.

De traducción. Un puente de traducción proporciona las mismas funciones que un puente local, excepto que cuenta con la capacidad de conectar segmentos de cable que utilizan velocidades o protocolos diferentes. Se puede, por ejemplo, utilizar un puente de traducción para conectar Ethernet con Token Ring, 10Base-T con 100Base-T o 100Base-TX con 100Base-T4.
En este tipo de puente, los paquetes que llegan suben por la pila de protocolos hasta el subnivel MAC, donde se les quita la cabecera del protocolo del nivel de enlace de datos y se pasan al subnivel LLC. Entonces, el protocolo adecuado encapsula los datos para cada uno de los puertos por los que se transmitirán los paquetes de salida. Esta traducción agrega un grado de complejidad y de costo, al propio puente y un retardo en la propagación de los datos por la red, pero sin duda constituye una solución efectiva para unir redes dispares en un mismo dominio de difusión.

Remotos. Un puente remoto conecta segmentos de red en ubicaciones diferentes, utilizando un enlace de red de área extensa (*WAN, Wide Area Network*), a través de un MODEM o una línea alquilada. Los enlaces WAN suelen ser más lentos y más caros que las conexiones LAN, y un puente conserva su valioso ancho de banda, minimizando la cantidad de tráfico que pasa por el enlace, a la vez que proporciona a ambos segmentos acceso completo a toda la red. Debido a la diferencia de velocidad entre el enlace local y de área extensa, un puente remoto suele contar con un búfer interno en donde

almacena los datos que recibe de la LAN mientras espera a transmitirlos al sitio remoto.

Puentes en redes Ethernet y Token Ring

En general, las redes Ethernet utilizan puentes transparentes, y las redes Token Ring utilizan puentes con enrutamiento en origen. Por tanto ¿Qué ocurre cuando se desea conectar un segmento Ethernet con un segmento Token Ring utilizando un puente? La respuesta es compleja, ya que la tarea presenta cierta cantidad de obstáculos importantes y porque aún no existe un estándar bien definido que proporcione una solución.
Algunas de las incompatibilidades fundamentales de los dos protocolos del nivel de enlace de datos son las siguientes:

Orden de bits Los sistemas Ethernet consideran que el primer bit de una dirección MAC es el bit de menor peso, mientras que los sistemas Token Ring tratan el primer bit como el de mayor peso.

Tamaño de MTU Las tramas Ethernet tienen un tamaño de unidad máxima de transferencia de 1,500 bytes, mientras que las tramas Token Ring pueden ser mucho mayores. Los puentes no son capaces de fragmentar paquetes para transferirlos a un segmento con MTU menor y volver a reensamblarlos en el destino, como hace los ruteadores. Un paquete demasiado largo que llega a un puente destinado a un segmento con una MTU menor se descarta.

Características exclusivas de Token Ring Las redes Token Ring utilizan bits de estado de trama, indicadores de prioridad y otras características que no tienen equivalente en Ethernet.
Además, los dos métodos para puentes poseen sus propias incompatibilidades. Los puentes transparentes no entienden la función especial de los mensajes ARB que se utilizan en los puentes con enrutamiento en origen y no pueden utilizar el campo RIF de los paquetes de Token Ring. Por otra parte, los puentes con enrutamiento en origen no entienden los mensajes del algoritmo del árbol de expansión generados por los puentes transparentes y no saben que hacer cuando reciben tramas sin información de enrutamiento.
Existen dos métodos básicos para resolver estas incompatibilidades, pero ninguno de ellos constituye una solución ideal. Dichos métodos son:

- Puentes de traducción.
- Puentes transparentes con enrutamiento en origen.

Puentes de traducción

En *los puentes de traducción*, un puente especial traduce las tramas del nivel de enlace de datos entre los formatos de Ethernet y Token Ring. No existe ningún estándar para éste proceso, por lo que los métodos utilizados por los fabricantes de productos individuales pueden variar enormemente. Es necesario llegar a un compromiso en el proceso de traducción, ya que no existe ninguna forma de implementar por completo todas las características de cada uno de los protocolos y de trasladar esas características al otro.

Algunas de las técnicas utilizadas en diversos puentes de traducción para solventar las incompatibilidades se describen a continuación.

Una de las funciones básicas del puente consiste en realizar una correspondencia entre los campos de la trama Ethernet y la trama Token Ring, y viceversa. El puente invierte el orden de bits de las direcciones origen y destino de los paquetes que pasan por los segmentos y pueden hacer algo o no hacer nada en función de los valores de los bits estado de trama, prioridad, reserva y monitor de un paquete de Token Ring. Puede que los puentes, sencillamente, descarten esos bits al traducir de Token Ring a Ethernet y que establezcan para ellos valores predeterminados cuando traducen de Ethernet a Token Ring.

Para enfrentarse a la diferencia de tamaño de MTU de los segmentos de red, un puente de traducción puede establecer como valor máximo de trama en el campo RIF de los paquetes de Token Ring la MTU de la red Ethernet (1,500 bytes). Siempre que las implementaciones de Token Ring de las estaciones de trabajo lean este campo y, en consecuencia, ajusten su tamaño de trama, no debería presentarse ningún problema, pero cualquier trama mayor que la MTU de los segmentos Ethernet se descartará en el puente que conecta las dos redes.
La mayor diferencia entre los dos tipos de puentes es que en Ethernet la información de enrutamiento se almacena en los puentes, mientras que el las redes Token Ring se almacena en las estaciones de trabajo. Para que el puente de traducción admita los dos tipos de redes, tiene que parecer un puente transparente hacia el lado Ethernet y uno con enrutamiento en origen hacia el lado Token Ring.

Para la red Token Ring, el puente de traducción posee un número de anillo y un número de puente, igual que cualquier puente con enrutamiento en origen estándar. Sin embargo, el número de anillo representa a todo el dominio Ethernet, no sólo al segmento conectado al puente. A medida que pasan a través del puente los paquetes de la red Token Ring, se elimina la información de los campos RIF y se almacena en caché en el puente. A partir de ese momento, los puentes transparentes estándar llevan los paquetes a su destino en la red Ethernet.

Cuando un paquete generado por una estación Ethernet tiene como destino un sistema de la red Token Ring, el puente de traducción busca el sistema en su caché de información RIF y agrega un campo RIF al paquete que contiene una ruta hacia la red, si es posible. Si no dispone de ninguna ruta en la caché o si el paquete es de difusión o multidifusión, el puente lo transmite como una difusión de ruta única.

Puentes transparentes con enrutamiento en origen

IBM también ha propuesto un estándar que combina las dos principales tecnologías de puentes, denominado puentes *transparentes con enrutamiento en origen* (*SRT, Source Route Transparent*). Esta tecnología se ha normalizado en el apéndice C del documento IEEE 802.1d. Los puentes SRT pueden enviar paquetes con origen en redes con puentes con enrutamiento en origen o con puentes transparentes, utilizando un algoritmo del árbol de expansión común a ambos. El algoritmo del árbol de expansión estándar utilizado por las redes Token Ring para los mensajes de difusión de ruta única no es compatible con el

algoritmo utilizado por Ethernet, definido en la especificación 802.1d. Este apéndice compagina ambos.

Los puentes SRT utilizan el valor del bit RII para determinar si un paquete contiene información RIF y, por tanto, se debería utilizar puentes con enrutamiento en origen o transparentes. Sin embargo, la mezcla de ambas tecnologías no es perfecta y puede resultar más sencillo para los administradores de red conectar los segmentos Ethernet y Token Ring por medio de un conmutador o ruteador en lugar de un puente de traducción o SRT.

Capitulo 4 Ruteadores (Router)

Descripción

Como ya vimos, los repetidores, concentradores y puentes conectan segmentos de red en los niveles físicos y de enlace de datos del modelo OSI, creando una LAN de mayores dimensiones con un único dominio de colisiones. El siguiente paso en el proceso de expansión de redes consiste en conectar dos LAN completamente independientes en el nivel de red.

Ésa es la labor de un ruteador (router). Los ruteadores son más selectivos que los puentes con relación al tráfico que circula entre las redes y son capaces de seleccionar de forma inteligente la ruta más eficiente hacia un destino determinado. Debido a que trabajen en el nivel de red, los ruteadores ofrecen la posibilidad de conectar redes distintas. Por ejemplo, es posible conectar una red Ethernet con una Token Ring, ya que a los paquetes que entran en el ruteador se les quita la cabecera del protocolo del nivel de enlace de datos a medida que asciende por la pila de protocolos hacia el nivel de red. Esto deja una unidad de datos del protocolo (*PDU, Protocol Data Unit*) encapsulada utilizando el protocolo de nivel de red que se ejecute en la computadora (Ver Fig. 4.1). Después de procesarla, el ruteador encapsula la PDU en una nueva cabecera del nivel de enlace de datos utilizando el protocolo con el que trabaja la otra red conectada al ruteador.

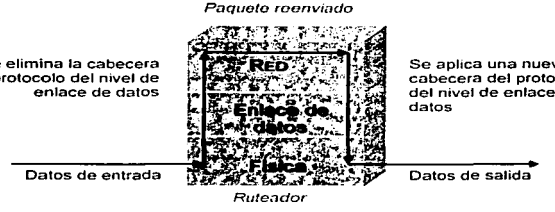


Figura 4.1. Los ruteadores pueden conectar redes de diferentes tipos porque desechan la cabecera del protocolo del nivel de enlace de datos de un paquete antes de procesarlo y le aplican una nueva antes de transmitirlo.

Los ruteadores son específicos del protocolo, tienen que soportar el protocolo de nivel de red utilizado por cada paquete. Con mucho, el protocolo de nivel de red utilizado con mayor frecuencia actualmente es el Protocolo de Internet (*IP, Internet Protocol*), que es la base de Internet y de la mayor parte de las redes privadas. En muchos casos, cuando se habla de un ruteador se está haciendo referencia a un ruteador IP. Sin embargo, algunas redes privadas utilizan el protocolo de *Intercambio de paquetes entre redes* (*IPX, Internetwork Packet Exchange*), de Novell, en el nivel de red. Una computadora conectada a dos o más redes se conoce como sistema multihospedado.

Los servidores de Novell NetWare con dos o más tarjetas de red (*NIC, Network Interface Card*) instalados, siempre han sido capaces de trabajar como ruteadores IPX, y ahora el producto incluye *software* de enrutamiento multiprotocolo que también admite IP. Los sistemas Windows multihospedados también pueden trabajar como ruteadores. Los sistemas servidores con Windows XP, 2000 y NT también disponen de posibilidades de enrutamiento multiprotocolo que admiten IP e IPX. Las estaciones de trabajo con Windows 95, 98, Me y XP pueden enrutar IPX de manera predeterminada, pero no IP. Sin embargo, la instalación de la característica Compartir Conexión a Internet (*ICS, Internet Connection Sharing*), que ahora se incluye en muchas versiones de Windows, proporciona servicios de enrutamiento IP entre una LAN y una conexión de acceso telefónico a Internet. El protocolo NetBEUI, en rigor, no es enrutable, pero todos los sistemas con Windows permiten el acceso telefónico a redes utilizando NetBEUI.

No obstante la mayoría de los ruteadores que se utilizan en grandes redes son dispositivos independientes; en esencia, computadoras dedicadas a las funciones de enrutamiento. Existen ruteadores de diferentes tamaños, desde unidades pequeñas que conectan una red de trabajo en grupo a una red soporte, hasta dispositivos grandes y modulares montados en bastidores, que cuestan mucho dinero. Sin embargo, aunque los ruteadores varían en sus posibilidades, como el número de redes a las que se conectan, los protocolos que admiten y la cantidad de tráfico que pueden manejar, sus funciones básicas son, esencialmente, las mismas.

Aplicaciones de los ruteadores

Aunque la función primaria de un ruteador es conectar redes y pasar tráfico entre ellas, los ruteadores pueden asumir diferentes papeles en los diseños de red. El tipo de ruteador utilizado para una función específica determina su tamaño, costo y posibilidades. La arquitectura de enrutamiento más sencilla aparece cuando es necesario conectar dos LAN que se encuentran a cierta distancia, utilizando una conexión de red de área extensa (*WAN, Wide Area Network*). Una sucursal de una gran empresa, por ejemplo, quizá disponga de una conexión WAN con las oficinas centrales de la corporación, en otra ciudad (ver Fig. 4.2).

Figura 4.2. Los ruteadores permiten utilizar conexiones de área extensa pera unir dos LAN

Para que sea posible establecer las comunicaciones entre las redes de ambas oficinas, cada una de las oficinas tiene que conectar su LAN a un ruteador, y los dos ruteadores se unen a través de la conexión WAN. La conexión WAN puede ser una línea telefónica alquilada, una conexión RDSI o DSL o, incluso, una conexión de acceso telefónico por MODEM. La tecnología utilizada para conectar las dos redes es irrelevante, siempre que los ruteadores de ambas oficinas estén conectados. En este ejemplo se requieren ruteadores porque las tecnologías de LAN y WAN son fundamentalmente incompatibles. No es posible disponer de una conexión Ethernet entre dos ciudades ni utilizar líneas telefónicas alquiladas para conectar cada una de las estaciones de trabajo con el servidor de archivos de la habitación de al lado.

En una configuración un poco más complicada, un sitio con una red de interconexión mayor puede disponer de muchas LAN, cada una de las cuales se conecta a una red soporte utilizando un ruteador (Ver Fig. 4.3). Aquí se necesitan los ruteadores porque una misma LAN quizá no sea capaz de soportar el número de estaciones de trabajo necesarias. Además, las LAN individuales pueden encontrarse en otros lugares del edificio o en otros edificios del mismo campus, y quizá se necesite un tipo de red diferente para conectarlas. Las conexiones entre edificios de un campus, por ejemplo, necesitan un medio de red adecuado para exteriores, como cable de fibra óptica, mientras que las LAN de cada edificio pueden utilizar cable de cobre, más barato. Existen ruteadores que pueden conectar esos tipos de redes, independientemente del protocolo que utilicen.

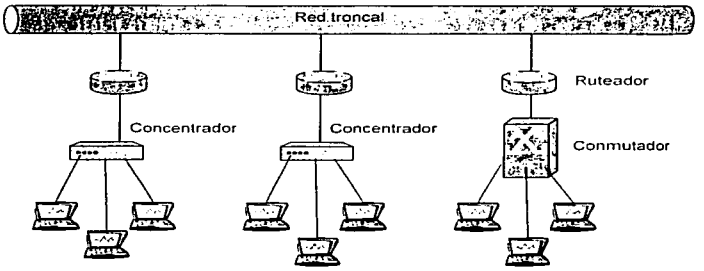


Figura 4.3. Los ruteadores también pueden conectar LAN a una red de soporte

Con frecuencia se combinan esos dos ejemplos de ruteadores. Una gran red de interconexión corporativa que utiliza una red soporte para conectar varias LAN, es más que probable que necesite una conexión a Internet. Esto significa que se necesita otro ruteador para admitir cierto tipo de conexión WAN a un proveedor del servicio Internet (*ISP, Internet Service Provider*). Los usuarios de cualquier lugar de la red corporativa podrán, entonces, tener acceso a los servicios de Internet.

Ambos escenarios utilizan ruteadores para conectar un número relativamente pequeño de redes, que se quedan pequeñas en comparación con Internet, que es una red de interconexión ruteada, compuesta por miles de redes de todo el mundo.

Para que los paquetes puedan viajar a través de esa maraña de ruteadores con una eficiencia razonable, existe una jerarquía de ruteadores desde los ISP locales más pequeños hasta los proveedores regionales, los cuales, a su vez, obtienen el servicio de los grandes proveedores nacionales (Ver Fig. 4.4). El tráfico generado por un sistema que utiliza un pequeño ISP sube por el árbol virtual hasta una de las redes de soporte principales, atraviesa los niveles superiores de la red vuelve a bajar hacia su destino.

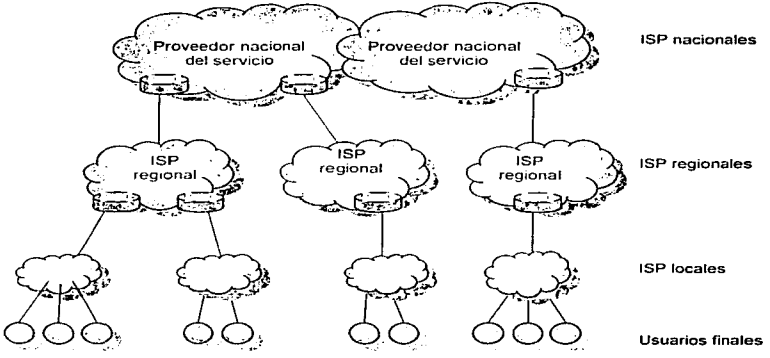


Figura 4.4. Internet utiliza una jerarquía de ruteadores para enviara el tráfico a cualquier lugar.

Se puede ver la ruta seguida por los paquetes desde una computadora a través de Internet hasta un destino concreto mediante la utilidad de seguimiento de rutas, denominada *traceroute* en los sistemas Unix y *tracert.exe* en los sistemas Windows. Esta utilidad de la línea de comandos toma la dirección IP o el nombre del DNS especificado y utiliza mensajes del protocolo de mensajes de control de Internet (*ICMP, Internet Control Message Protocol*) para mostrar los nombres y direcciones de todos los ruteadores intermedios en la ruta hasta el destino. Una pantalla típica de seguimiento de rutas, generada en este caso por un sistema Windows XP, tiene el siguiente aspecto:

C:\Documents and Settings\Carlos>tracert www.ericsson.se

Traza a la dirección www.ericsson.se [193.180.17.140] sobre un máximo de 30 saltos:

Saltos				Nombre del ruteador	Dirección IP del ruteador
1	338 ms	472 ms	353 ms	ipt-lj08.proxy.aol.com	[205.188.195.101]
2	336 ms	341 ms	340 ms	we3-dtc-G4-0-2.proxy.aol.com	[205.188.195.124]
3	336 ms	669 ms	340 ms	pop1-dtc-P0-0.atdn.net	[66.185.140.1]
4	335 ms	853 ms	353 ms	bb2-dtc-P13-0.atdn.net	[66.185.140.6]
5	388 ms	643 ms	354 ms	bb2-vie-P3-0.atdn.net	[66.185.152.119]
6	574 ms	365 ms	355 ms	bb2-nyc-P4-0.atdn.net	[66.185.152.200]
7	350 ms	354 ms	340 ms		[66.185.151.67]
8	349 ms	366 ms	669 ms	nyk-bb1-pos4-0-0.telia.net	[213.248.82.217]
9	415 ms	657 ms	431 ms	kbn-bb1-pos3-0-0.telia.net	[213.248.64.109]
10	479 ms	458 ms	446 ms	s-bb1-pos4-0-0.telia.net	[213.248.65.26]
11	494 ms	458 ms	445 ms	s-b3-pos5-0.telia.net	[213.248.66.2]
12	440 ms	432 ms	828 ms	fre-b1-pos3-2.telia.net	[213.248.67.62]
13	457 ms	945 ms	469 ms	fre-c3-pos2-0.se.telia.net	[194.22.190.90]
14	756 ms	469 ms	447 ms	hy-d4-geth6-1.se.telia.net	[213.64.62.162]
15	469 ms	445 ms	432 ms	eriesson-hy.k.telia.net	[213.64.82.162]
16	441 ms	433 ms	946 ms	C0A80004.ipt.aol.com	[192.168.0.4]
17	456 ms	958 ms	457 ms	www.eriesson.com	[193.180.17.140]

Traza completa.

Funciones de un ruteador

La función básica de un ruteador consiste en evaluar todo paquete que llega de una de cualquiera de las redes a las que está conectado y enviarlo hacia su destino a través de otra red. . su objetivo es, para cada paquete, seleccionar la red que proporciona la mejor ruta hacia el destino. Cada uno de los ruteadores en la ruta de un paquete se conoce como salto (*hop*); el objetivo es que el paquete llague a su destino con el menor número de saltos. En una red privada, un paquete quizá necesite realizar tres o cuatro 8° más) saltos para llegar a su destino. En Internet, es fácil que un paquete se encuentre con más de 20 ruteadores en su camino.

Un ruteador, por definición, se conecta a dos o más redes. El ruteador tiene información directa acerca de cada una de ellas y de los protocolos que admiten. Si, por ejemplo, una estación de trabajo de Red 1 (Ver Fig. 4.5) transmite un paquete a un sistema en Red 2, el ruteador que conecta Red 1, Red 2 y Red 3 puede decidir directamente cuál de las dos redes, Red 2 o Red 3, contiene el sistema destino y por lo tanto reenviar el paquete adecuadamente.

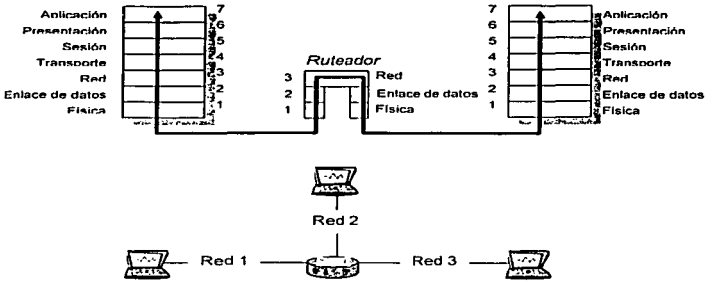


Figura 4.5. Los ruteadores tienen información directa acerca de las redes a las que se conectan

Tablas de enrutamiento

El ruteador reenvía paquetes manteniendo una lista de redes y *hosts*, denominada tabla de enrutamiento. Par que las computadoras se comuniquen en red, toda máquina debe tener una dirección propia. Sin embargo, además de identificar una computadora, la dirección tiene que identificar la red en la que se encuentra. En redes TCP/IP, por ejemplo, la dirección estándar de 32 bits se compone de un identificador de red y de un identificador de *host*. Una tabla de enrutamiento contiene entradas con el identificador de red de cada una de las redes conectadas o, en algunos casos, los identificadores de red y de *host* para computadoras específicas. Cuando el ruteador recibe un paquete destinado a una estación de trabajo de Red 3, mira el identificador de red de la dirección destino del paquete, lo compara con la tabla de enrutamiento y lo envía a la red que posee el mismo identificador.
Se trata de una tarea bastante sencilla, siempre que el ruteador esté conectado a todas las LAN de la internetwork, si embargo cuando la internetwork es mayor y utiliza varios ruteadores, ninguno de ellos conoce todas las LAN. Supongamos que el ruteador A está conectado a Red 1, 2 y 3 (ver Fig. 4.6), y posee en sus tablas los identificadores de dichas redes, pero no conoce a Red 4, que está conectada a otro ruteador.

Entonces, ¿cómo sabe el ruteador A hacia dónde enviar los paquetes destinados a una estación de trabajo en una red distante? La respuesta es que los ruteadores mantienen en sus tablas de enrutamiento información acerca de otras redes, además de aquellas a las que están conectados directamente. Una tabla de enrutamiento puede contener información acerca de muchas redes diferentes situadas por toda la empresa. En una internetwork privada, no resulta raro que todos los ruteadores tengan entradas para todas las redes conectadas. Sin embargo, en Internet existen tantas redes y ruteadores que ninguna tabla de enrutamiento podría contener a todos ellos y funcionar de forma eficiente. Por tanto, un ruteador conectado a Internet envía paquetes al ruteador que cree posee mejor información acerca de la red a la que va destinado el paquete.

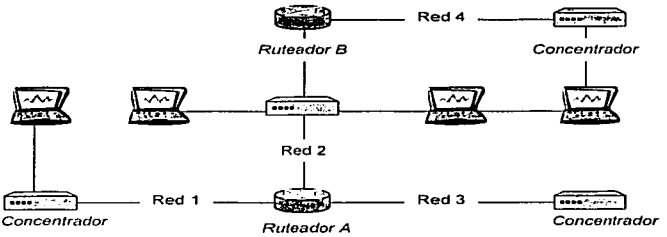


Figura 4.6. El ruteador A no conoce a la Red 4 de forma directa, ya que está conectada a otro ruteador.

Tablas de enrutamiento en Windows

Toda computadora de una red TCP/IP posee una tabla de enrutamiento, incluso aunque sólo esté conectada a una red. Como mínimo, la tabla de enrutamiento indica la puerta de enlace (Gateway) predeterminada del sistema y contiene instrucciones sobre como manejar el tráfico que se envía a la red local y a la dirección de red de bucle (127.0.0.0). Una tabla de enrutamiento típica para un sistema Windows tiene el siguiente aspecto:

C:\Documents and Settings\Carlos>netstat -nr

Rutas activas:

Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	172.141.3.157	172.141.3.157	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
172.141.3.157	255.255.255.255	127.0.0.1	127.0.0.1	50
172.141.255.255	255.255.255.255	172.141.3.157	172.141.3.157	50
200.52.49.38	255.255.255.255	172.141.3.157	172.141.3.157	1
205.188.68.80	255.255.255.255	172.141.3.156	172.141.3.157	1
224.0.0.0	240.0.0.0	172.141.3.157	172.141.3.157	1
255.255.255.255	255.255.255.255	172.141.3.157	0.0.0.0	1

Puerta de enlace predeterminada: 172.141.3.157

Rutas persistentes: Ninguna

Dirección de red — Indica la dirección de red para la que se proporciona la información de enrutamiento. Aunque la mayor parte de las entradas poseen direcciones de red en este campo, también es posible proporcionar

	información de enrutamiento para una dirección de *host*. Esto se denomina *ruta de host*.
Máscara de red	Indica la máscara de subred utilizada para determinar cuales de los bits de la dirección de red funcionan como identificador de red.
Puerta de enlace	Indica la dirección IP de la puerta de enlace o ruteador que debería utilizar el sistema para enviar paquetes a la dirección de red. Cuando la entrada es para una red a la que el sistema se encuentra conectado directamente, este campo contiene la dirección de la interfaz de red del sistema.
Interfaz	Indica la dirección IP de la interfaz de red que debería utilizar el sistema para enviar tráfico a la dirección de puerta de enlace.
Métrica	Indica la distancia entre el sistema y la red destino, normalmente expresado como el número de saltos necesarios para que el tráfico llegue a la dirección de red.

El sistema que utiliza esta tabla de enrutamiento sólo cuenta con una dirección IP, la 172.141.3.157. Esto se obtiene a partir de la tercera entrada, que contiene una ruta de *host* dirigiendo esa dirección al adaptador de buele (127.0.0.1). La entrada 0.0.0.0 representa la puerta de enlace predeterminada del sistema, que utiliza para el tráfico destinado a las redes que no aparecen en la tabla. Como el sistema está conectado a Internet a través de un MODEM, los campos Puerta de enlace e Interfaz de la entrada 0.0.0.0 contienen la dirección asignada a la conexión MODEM por el servidor de la red del ISP. En este caso el módem funciona como interfaz de red, igual que una NIC, y posee su propia dirección IP.
Si el sistema perteneciera a una LAN y esta estuviera conectada a Internet a través de un ruteador, el campo Puerta de enlace contendría la dirección IP de dicho ruteador.

Las dos últimas entradas definen rutas para mensajes de difusión y multidifusión. La RFC (*Request For Comments) "Assigned Numbers*" contiene direcciones de red Clase D asignadas a grupos específicos de multidifusión, todos los cuales se encuentran en la red 224.0.0.0. La entrada 255.255.255.255 es la dirección de difusión estándar.

(Para mayor información acerca de la asignación y manejo de las direcciones de IP, referirse al Apéndice C).

Otros sistemas operativos, como pudiera ser el caso del Unix, muestran la tabla de enrutamiento ligeramente diferente y puede que incluyan otra información, pero los elementos y funciones básicos de la tabla son los mismos.

Por lo tanto volviendo a red que se muestra en la Fig. 4.6, el ruteador A posee entradas en su tabla de enrutamiento para todas las LAN de la internetwork, que especifican como transmitir los paquetes a cada una de ellas. Las entradas para las redes a las que el ruteador está conectado directamente indican la interfaz a la que están conectadas, y las entradas para redes distantes indican la dirección de otro ruteador. Cuando los paquetes llegan al ruteador indicado se repite en mismo proceso y puede que los datos se transmitan de nuevo a otro ruteador. En Internet este proceso se puede repetir docena de veces. Ningún ruteador conoce el trayecto completo que seguirá un paquete desde el origen hasta el destino; cada cual es tan sólo responsable del siguiente salto. De hecho, cuando una transferencia de

archivos consta de varios paquetes, las condiciones de la red, siempre cambiante, pueden hacer que cada uno de los paquetes tome una ruta distinta hacia el mismo destino.

Análisis sintáctico de la tabla de enrutamiento

Ya sea que un sistema trabaje o no como ruteador, la responsabilidad de un protocolo del nivel de red, como IP, consiste en determinar donde debería transmitirse a continuación cada uno de los paquetes. La cabecera IP de cada paquete contiene la dirección del sistema que es el último destino, pero antes de pasar cada paquete al protocolo del nivel de enlace de datos, IP utiliza la tabla de enrutamiento para determinar cual debería ser la dirección destino del nivel de enlace de datos para el siguiente salto del paquete. Esto es así debido a que un protocolo del nivel de enlace de datos, como Ethernet, sólo puede dirigir un paquete a un sistema de la red local, que puede ser o no su destino final. Para tomar esa dirección, IP lee la dirección destino de cada paquete que procesa, y busca la entrada correspondiente en la tabla de enrutamiento, utilizando el siguiente procedimiento:

1. IP recorre primero la tabla de enrutamiento buscando una ruta de *host* que corresponda exactamente a la dirección de IP destino del paquete. Si existe, el paquete se transmite a la puerta de enlace especificada en la entrada de la tabla de enrutamiento.
2. Si no existe la ruta de *host* correspondiente, IP utiliza la máscara de subred para determinar la dirección de red del paquete y busca en la tabla de enrutamiento una entrada que corresponda a esa dirección.
   Si IP encuentra una correspondencia, el paquete se transmite a la puerta de enlace especificada -si el sistema no está conectado directamente a la red destino- o a la interfaz de red especificada –si el destino está en la red local.
3. Si no existe la dirección de red correspondiente en la tabla de enrutamiento, IP busca la ruta predeterminada (o 0.0.0.0) y transmite el paquete por la puerta de enlace especificada.
4. Si la tabla no contiene una ruta predeterminada, IP devuelve un mensaje de "destino no alcanzable" al origen del paquete, ya sea la aplicación que lo generó o el sistema que lo transmitió.

Enrutamiento estático y dinámico

Un sistema puede generar entradas para la puerta de enlace predeterminada, la red local y las direcciones de difusión y multidifusión, ya que posee toda la información necesaria para crearlas. Sin embargo, para redes a las que el ruteador no está conectado directamente, es necesario crear las entradas de la tabla de enrutamiento por medio de un proceso externo. Los dos métodos básicos para crear entradas en la tabla de enrutamiento se denominan *enrutamiento estático*, que es la creación manual de entradas, y *enrutamiento dinámico*, que utiliza un protocolo externo para obtener información acerca de la red.

En una red estable, relativamente pequeña, el enrutamiento estático es una alternativa práctica, ya que sólo es necesario crear una vez las entradas en las tablas de los ruteadores. No es necesario configurar de forma manual la tabla de enrutamiento en las estaciones de trabajo, ya que suelen disponer solamente de una interfaz de red y tener acceso a la red a

través de una puerta de enlace predeterminada. Sin embargo, los ruteadores disponen de varias interfases de red y suelen tener acceso a varias puertas de enlace. Tienen que conocer, por tanto, que ruta utilizar para transmitir a una determinada red.

Para crear entradas estáticas en la tabla de enrutamiento de una computadora se utiliza un programa suministrado con el sistema operativo. La herramienta estándar para hacerlo en los sistemas Unix y Windows es una utilidad basada en caracteres llamada *route* (en Unix) y *route.exe* (en Windows). Para crear una entrada nueva en una tabla de enrutamiento de una computadora con Windows, por ejemplo, se utiliza un comando como el siguiente:

```
ROUTE ADD 192.168.5.0 MASK 255.255.255.0 192.168.2.1 METRIC 2
```

Este comando le indica al sistema que, para llegar a la red con dirección 192.168.5.0, el sistema tiene que enviar los paquetes a una puerta de enlace (ruteador) con la dirección 192.168.2.1 y que la red destino está a dos saltos de distancia.

En algunos casos existen utilidades gráficas que puede realizar la misma tarea de una forma más amigable.

Las rutas estáticas creadas de esta forma se mantienen en la tabla de enrutamiento hasta que se modifican o eliminan de forma manual, y esto puede representar un problema. Si falla una puerta de enlace especificada en una ruta estática, el sistema continúa enviándole paquetes, sin sentido. Es necesario reparar la puerta de enlace o modificar las rutas estáticas de toda la red que la tienen como referencia, para conseguir que los sistemas vuelvan a funcionar correctamente.

En redes mayores, el enrutamiento estático llega a ser impracticable, no sólo debido a la enorme cantidad de entradas de la tabla de enrutamiento involucradas, sino también porque las condiciones de la red pueden modificarse con demasiada frecuencia para que los administradores de red pueden mantener actualizadas las tablas de enrutamiento de todos los sistemas. En lugar de eso, en dichas redes, se utiliza el enrutamiento dinámico, donde protocolos de enrutamiento especializados comparten información acerca de los demás ruteadores de la red y, en consecuencia, modifican la tabla de enrutamiento. Una vez configurado, el enrutamiento dinámico apenas necesita mantenimiento por parte de los administradores de la red, ya que el protocolo puede crear, modificar o eliminar entradas de la tabla de enrutamiento en función de las condiciones de la red. Internet depende por completo del enrutamiento dinámico, ya que se modifica constantemente y sería imposible afrontar esos cambios con un proceso manual.

Selección de la ruta más eficiente

Muchas intercedes, incluso algunas relativamente pequeñas, se diseñan con varios ruteadores que proporcionan trayectos redundantes hacia un destino determinado. Por tanto, aunque sería posible crear una internetwork compuesta por varias LAN unidas en serie, la mayoría suele utilizar una topología que se asemeja a una malla, como se muestra en la Fig. 4.7. De seta forma, si alguno de los ruteadores falla, todos los sistemas pueden seguir enviando tráfico entre sí.

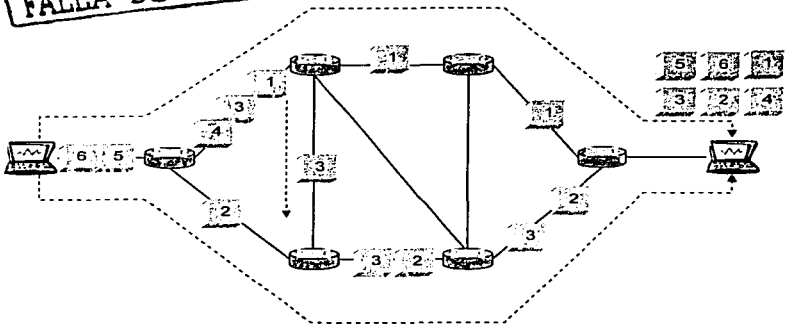


Figura 4.7. Al interconectar los ruteadores, los paquetes de una estación de trabajo pueden viajar a un destino en otra red por rutas diferentes.

Cuando se diseña una internetwork de esta forma, una parte importante del proceso de enrutamiento es la selección de la mejor ruta hasta un determinado destino. La utilización de enrutamiento dinámico en la red hace que, normalmente, las tablas de enrutamiento dispongan de todas las rutas posibles hacia una red determinada, incluyendo una métrica que indica el número de saltos necesarios para llegar a esa red. La mayoría de las veces, la eficiencia de una ruta en particular se mide por el valor de esa métrica, ya que cada salto implica el procesamiento en un ruteador, lo que introduce un pequeño retraso en la transmisión. Cuando un ruteador tiene que reenviar un paquete a una red representada con varias entradas en la tabla de enrutamiento, selecciona la que posee la menor métrica.

Descarte de paquetes

El objetivo de un ruteador es la transmisión de paquetes a su destino, utilizando la ruta con el menor número de saltos. Los ruteadores también realizan un seguimiento del número de saltos que sufren los paquetes en su viaje hacia su destino por otro motivo. Cuando se presenta un mal funcionamiento o un problema de configuración en uno o varios ruteadores, es posible que los paquetes se vean atrapados en un bucle de ruteadores y que pasen de uno a otro de forma indefinida.

Para evitar esto, la cabecera IP contiene un campo llamado *Tiempo de vida* (*TTL, Time-to-Live*) al que el sistema origen da un valor numérico determinado cuando crea el paquete. En los sistemas Windows, el valor predeterminado es 128. A medida que el paquete viaja por la red, cada ruteador que lo procesa disminuye en una unidad el valor de ese campo. Si, por cualquier motivo, el paquete pasa por ruteadores el suficiente número de veces para que el

valor de ese campo llegue a 0, el último ruteador lo elimina de la red y lo descarta. El ruteador, a continuación, devuelve un mensaje de ICMP Tiempo de vida excedido en tránsito al sistema origen para informarle del problema.

Fragmentación de paquetes

Los ruteadores pueden conectar redes de muy diferentes tipos, y el proceso de transferencia de datagramas entre protocolos del nivel de enlace de datos puede requerir algo más que eliminar una cabecera y aplicar una nueva. El problema más importante que puede aparecer durante este proceso de traducción es que un protocolo admita tramas más grandes que el otro.

Si, por ejemplo, un ruteador conecta una red Token Ring con una Ethernet, tendrá que aceptar datagramas de 4,500 bytes de una de ellas y transmitirlo por la otra, que sólo admite datagramas de 1,500 bytes. Los ruteadores determinan la Unidad máxima de transferencia (*MTU, Maximum Transfer Unit*) de una red en particular consultando la interfaz de esa red. Para que eso sea posible, el ruteador tiene que dividir el datagrama en fragmentos del tamaño adecuado y, a continuación, encapsular cada fragmento en una trama correcta del protocolo del nivel de enlace de datos. Ese proceso de fragmentación puede ocurrir varias veces durante el recorrido de un paquete entre el origen y el destino, en función del número y tipo de redes involucradas.

Por ejemplo, un paquete originado en una red Token Ring se dividirá en fragmentos de 1,500 bytes para utilizar una ruta a través de una red Ethernet y, posteriormente, cada uno de esos fragmentos se dividirá en nuevos fragmentos de 576 bytes para su transmisión por Internet. Hay que tener en cuenta, sin embargo, que aunque los ruteadores fragmentan los paquetes, nunca los reensamblan. Incluso aunque los datagramas de 576 bytes pasen por redes Ethernet según se aproximan a su destino, el ruteador no los reensambla de nuevo en datagramas de 1,500 bytes. Todo el reensamblado se realiza en el nivel de red del sistema destino final.

Enrutamiento e ICMP

El protocolo de mensajes de control de Internet (*ICMP, Internet Control Message Protocol*) proporciona varias funciones importantes para los ruteadores y los sistemas que los utilizan. La más importante de todas ellas es la posibilidad que tienen los ruteadores de utilizar los mensajes ICMP para proporcionar información de enrutamiento a los demás ruteadores. Los ruteadores envían mensajes de Redirección de ICMP a los sistemas origen cuando conocen una mejor ruta que la que está utilizando actualmente el sistema. Si, por ejemplo, una estación de trabajo en Red A envía un paquete al Ruteador A destinado a una computadora de Red B y el Ruteador A determina que el siguiente salto debería ser Ruteador B, que se encuentra en la misma red que la estación de trabajo transmisora, Ruteador A utilizará un mensaje ICMP para indicarle a la estación de trabajo que debería utilizar Ruteador B para tener acceso a Red B (Ver Fig. 4.8). Entonces la estación de trabajo modifica la entrada de su tabla de enrutamiento.

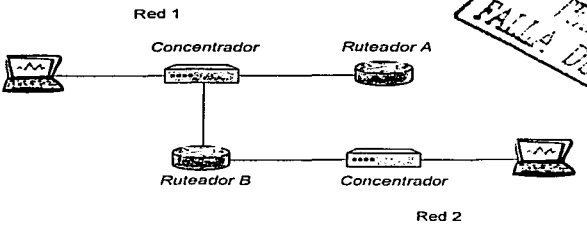


Figura 4.8. Los mensajes Redirección de ICMP proporcionan información de enrutamiento sencilla a los sistemas transmisores.

Los ruteadores también generan mensajes de ICMP Destino no alcanzable de varios tipos cuando no son capaces de reenviar los paquetes. Si un ruteador recibe un paquete destinado a una estación de trabajo en una red conectada de forma local y no puede entregar el paquete porque la estación de trabajo está apagada, el ruteador genera un mensaje *Host* no alcanzable y lo transmite al sistema que originó el paquete. Si el ruteador no es capaz de reenviar el paquete a otro ruteador que proporciona acceso al destino genera un mensaje Red no alcanzable. Los protocolos de nivel de red proporcionan comunicación extremo a extremo, lo que significa que suelen ser los sistemas finales los implicados en el diálogo. ICMP es, por tanto, un mecanismo que permite a los sistemas intermedios (los ruteadores) comunicarse con un sistema final origen (el transmisor) en el caso de que los paquetes no puedan alcanzar el sistema destino final.

Otros paquetes de ICMP, denominados mensajes de Petición de ruteador y Anuncio de ruteador, permiten a las estaciones de trabajo descubrir los ruteadores de la red local. Un *host* genera un mensaje de Petición de ruteador y lo transmite como difusión o como multidifusión a la dirección Todos los ruteadores de esta subred (224.0.0.2). Los ruteadores que reciben el mensaje responden con mensajes Anuncio de ruteador que utiliza el *host* para actualizar su tabla de enrutamiento. A continuación, los ruteadores generan actualizaciones periódicas para informar al *host* de que continúan en un estado operativo.

Protocolos de enrutamiento

Los ruteadores que admiten enrutamiento dinámico utilizan protocolos especializados para intercambiar información acerca de ellos mismos con los otros ruteadores de la red. El enrutamiento dinámico no altera el proceso real de enrutamiento; se trata sólo de un método diferente de creación de entradas en las tablas de enrutamiento. Existen dos tipos de protocolos de enrutamiento: protocolo de pasarela interior y protocolo de pasarela exterior. Las internetworks privadas suelen utilizar protocolos de pasarela interior, ya que disponen de un número relativamente pequeño de ruteadores y resulta práctico para que puedan intercambiar mensajes entre ellos.

En Internet, la situación es diferente. Sería imposible que todos los miles de ruteadores de Internet intercambiaran mensajes con todos los demás. La cantidad de tráfico implicado sería enorme y los ruteadores tendrían muy poco tiempo para otras tareas. En lugar de eso, como suele ser habitual en Internet, se diseñó un sistema de dos niveles que divide la gigantesca red en unidades discretas denominadas *sistemas autónomos*, a veces también *dominios administrativos* o, simplemente, *dominios*.

Un sistema autónomo (*AS, Autonomous System*) suele ser una internetwork privada administrada por una única autoridad, como las que se encuentran en las empresas, instituciones educativas y agencias gubernamentales. Los ruteadores de un sistema autónomo utilizan un protocolo de pasarela interior, como el protocolo de información de enrutamiento (*RIP, Routing Information Protocol*) o el protocolo de abrir el camino más corto (*OSPF, Open Shortest Path First*), para intercambiar la información de enrutamiento entre ellos. En los extremos de un sistema autónomo existen ruteadores que se comunican con los demás sistemas autónomos de Internet, utilizando un protocolo de pasarela exterior (ver Fig. 4.9), siendo los más habituales de Internet el protocolo de pasarela de borde (*BGP, Border Gateway Protocol*) y el protocolo de pasarela exterior (*EGP, Exterior Gateway Protocol*).

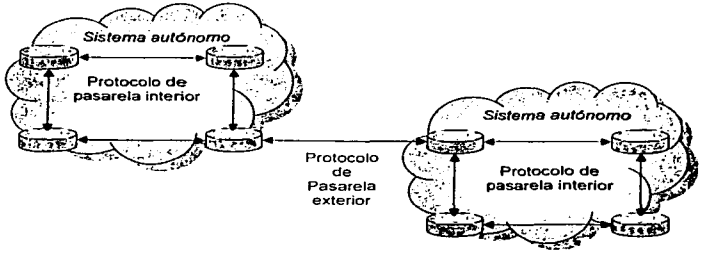


Figura 4.9. Los sistemas autónomos intercambian información de enrutamiento utilizando un protocolo de pasarela exterior.

Al dividir las tareas de enrutamiento en una jerarquía de dos niveles, los paquetes que viajen por Internet pasan a través de ruteadores que sólo contienen la información necesaria para legar al sistema autónomo adecuado (dominio adecuado).

Una vez que los paquetes llegan al extremo del AS en que se encuentra el sistema, los ruteadores que ahí se encuentran contienen información más específica acerca de las redes internas del AS. El concepto es muy similar a la forma en que se asignan las direcciones de IP y los nombres de dominio de Internet. Las entidades externas sólo realizan un seguimiento de las diferentes direcciones de red o dominios. Los administradores

individuales de cada red son responsables de mantener las direcciones y los nombres de *host* dentro la red o dominio.

Protocolo de información de enrutamiento (RIP)

El protocolo de información de enrutamiento (*RIP, Routing Information Protocol*) es el protocolo de pasarela interior utilizado con más frecuencia, debido principalmente a que está soportado por muchos sistemas operativos y resulta sencillo de configurar y utilizar. De hecho, RIP casi nunca necesita configurarse. Concebido originalmente par los servicios de red de Xerox (*XNS, Xerox Network Services*) e incluido en el Unix de Berkeley (BSD 4.2 y versiones posteriores), RIP toma la forma de un *demonio* denominado *routed* en la mayoría de los sistemas Unix. En 1988, el *Internet Engineering Task Force (IETF)* normalizó RIP como la RFC 1058. Desde entonces, el protocolo se ha implementado de forma universal en los productos *hardware* de enrutamiento, así como en los sistemas operativos de servidor de Windows y Novell NetWare.

NOTA: Un *demonio* es el nombre que utilizan los sistemas Unix para referirse a los programas que se ejecutan en segundo plano de forma continua e independiente de otras actividades del sistema. Este tipo de programas tiene diferentes nombres en los diversos sistemas operativos. En Windows es un *servicio*; en NetWare es un *módulo cargable NetWare (NLM)*; y como ya se comentó en Unix es un *demonio*.

Los ruteadores que usan RIP intercambian mensajes de petición y de respuesta utilizando el protocolo de datagramas de usuario (*UDP, User Datagram Protocol*) y el puerto 520, como se especifica en la RFC "*Assigned Numbers*". Cuando un ruteador arranca, envía un mensaje de petición de RIP a los demás ruteadores de la red, utilizando una transmisión de difusión o de multidifusión, en función de las versiones de RIP. Los demás ruteadores responden enviando sus tablas de enrutamiento en mensajes de respuesta de RIP y repiten el anuncio cada 30 segundos. Los ruteadores también pueden utilizar RIP para solicitar información acerca de una red específica.

RIP siempre utiliza un contador de saltos como la métrica de una entrada en la tabla de enrutamiento e impone un número máximo de 15 saltos. Las redes o *host* a más de 15 saltos de distancia se consideran no alcanzables. Esto demuestra que el protocolo se diseñó para utilizarlo en redes privadas y no en Internet, ya que las rutas de Internet suelen necesitar más de 15 saltos. Esta limitación en el número de saltos es independiente del campo Tiempo de vida de la cabecera IP, aunque los ruteadores de RIP generan los mismos mensajes de ICMP Destino no alcanzable cuando se excede el número máximo de saltos.
Las entradas de la tabla de enrutamiento de RIP también poseen un valor de tiempo de vida de tres minutos. Si una entrada no se actualiza por medio de un mensaje de RIP en tres minutos, el ruteador aumenta su métrica a 16, lo que, para RIP, es infinito. Un minuto más tarde se elimina por completo la entrada de la tabla.

El formato de mensaje de RIP

Los mensajes de IP se componen de una cabecera de 4 bytes y de una o más rutas de 20 bytes. Un mismo mensaje puede contener hasta 25 rutas, para un tamaño total de datagrama

UDP de 512 bytes, incluyendo la cabecera UDP de 8 bytes. Si en una tabla de enrutamiento existen más de 25 entradas, el ruteador genera mensajes adicionales hasta que transmite toda la tabla.

La Fig. 4.10 muestra el formato del mensaje RIP. Las funciones de los campos de la cabecera a parecen a continuación:

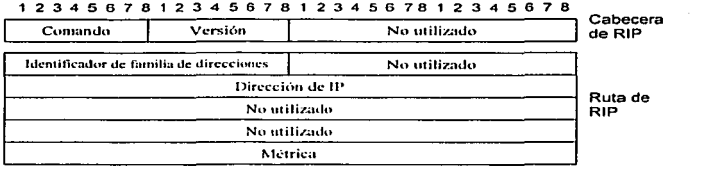


Figura 4.10. Formato de cabecera y ruta de RIP.

Campo	Longitud [byte]	Descripción
Comando	1	Indica la función del mensaje, utilizando los siguientes valores: 1 – *Request* (Petición) Solicita la transmisión de toda la tabla de enrutamiento o de una ruta específica de todos los ruteadores de la red local. 2 – *Reply* (Respuesta) transmite las entradas de la tabla de enrutamiento.
Versión	1	Indica la versión de RIP que se ejecuta en el sistema que genera el paquete. Los valores posibles son 1 y 2.
No utilizado	2	
Identificador de familia de direcciones	2	Identifica el protocolo del nivel de red para el que el mensaje transporta información de enrutamiento. El valor para IP es 2.
No utilizado	2	
Dirección de IP	4	Indica la dirección de una red o *host* que está accesible a través del ruteador que genera el mensaje.
No utilizado	4	
No utilizado	4	

Métrica	4	Indica el número de saltos entre le sistema que genera el mensaje y la red o *host* identifica por el valor del campo de dirección de IP.

Problemas de RIP

RIP es lo que se conoce como un protocolo de enrutamiento de *vector de distancia*. Esto significa que todo ruteador de la red anuncia su tabla de enrutamiento a los ruteadores vecinos. A continuación, cada uno de los ruteadores analiza la información proporcionada por los demás, selecciona la mejor ruta a cada rede destino y la agrega a su propia tabla de enrutamiento. El proceso de actualización de las tablas de enrutamiento de todos los ruteadores de la red en respuesta a un cambio en dicha red, como el fallo o adición de un ruteador, se denomina *convergencia*. El ruteador de vector de distancia es relativamente sencillo y razonablemente eficiente en términos de búsqueda de la mejor ruta hacia una red determinada. Sin embargo, plantea algunos problemas fundamentales.

Los protocolos de vector de distancia como RIP poseen una velocidad de convergencia bastante lenta debido a que las actualizaciones se realizan en cada ruteador de forma asíncrona, esto es, sin sincronización ni confirmación. Son, por tanto, propensas a sufrir una condición conocida como *problema de cuanta hasta el infinito*. El problema de cuenta hasta el infinito se presenta cuando un ruteador detecta un fallo en la red, modifica la entrada correspondiente de su tabla de enrutamiento y, a continuación, actualiza esa misma entrada como consecuencia de un anuncio de otro ruteador antes de difundirla como un anuncio propio. Entonces, los ruteadores empiezan a modificar sus tablas una y otra vez, aumentando cada vez la métrica para la misma entrada hasta que llega al infinito (16). El proceso, al final, se corrige a sí mismo, pero el retardo introducido cada vez que se produce una modificación en la red ralentiza todo el proceso de enrutamiento.

A RIP también se le critica por la cantidad de tráfico de difusión que genera. Todo ruteador de RIP difunde toda su tabla de enrutamiento cada 30 segundos.

En función del tamaño de la red, esto puede implicar muchos mensajes de RIP por servidor. Sin embargo, una ventaja de la utilización de difusiones es que permite a los sistemas procesar los mensajes de anuncio sin anunciar su propia tabla de enrutamiento. Esto se conoce como *RIP silencioso*, y es más probable encontrarlo implementado en los *host* que no son ruteadores.

RIP tampoco incluye una máscara de subred con cada una de las rutas de un mensaje de anuncio. El protocolo está diseñado para su uso con direcciones de red que se ajusten a las clases de direcciones de IP estándar, las cuales se pueden identificar por medio de los 3 primeros bits de la dirección. Si la dirección de red de una entrada de la tabla de enrutamiento se justa a las clases de direcciones, el protocolo utiliza la máscara de subred asociada con esa clase. Cuando no es el caso, el protocolo utiliza la máscara de subred de la interfaz de red por donde se ha recibido el mensaje RIP. Si esa máscara no es la adecuada, el protocolo asume que la entrada de la tabla contiene una ruta de *host* y utiliza máscara de subred 255.255.255.255. Estas suposiciones pueden provocar que el tráfico se reenvíe de

forma incorrecta en algunos tipos de redes, como las que utilizan subredes de longitud variable o disjuntas.

RIP tampoco permite ninguna forma de autenticación para los ruteadores participantes. Un ruteador de RIP acepta y procesa mensajes que provienen de cualquier origen, por lo que es posible corromper las tablas de enrutamiento de toda la red con información incorrecta suministrada, de forma accidental o deliberada, por un ruteador malicioso.
RIP v2

Como consecuencia de las limitaciones del estándar original RIP se desarrollaron otros protocolos de pasarela interior, como OSPF, pero también se mejoró el propio protocolo RIP. La versión 2 de RIP se publicó inicialmente como la RFC 1388, propuesta como borrador de estándar en la RFC 1723 y ratificada finalmente como estándar del IETF y publicada en noviembre de 1998 como la RFC 2453. La versión original de Windows NT Server 4.0 admite RIP v1, pero la actualización Servidor de enrutamiento y acceso remoto (*RRAS, Routing and Remote Access Server*) agrega el soporte para RIP v2, tal como se define en la RFC 1723. Los productos de servidor Windows XP y 2000 también admiten RIP v2, al igual que la mayoría de los servidores actualmente en el mercado.
RIP v2 soluciona muchos de los problemas inherentes a la versión 1, incluyendo los siguientes:

Tráfico de difusión RIP v2 permite la actualización de transmisiones de multidifusión para los anuncios de los ruteadores, así como difusiones. La RFC "*Assigned Numbers*" asigna a los ruteadores de RIP v2 la dirección de multidifusión 224.0.0.9. Las transmisiones que se envían a dicha dirección sólo las procesan los ruteadores y no afectan a los demás sistemas. La utilización de multidifusión es opcional en todos los ruteadores con RIP v2; también siguen soportando difusiones. El único posible inconveniente de la utilización de multidifusiones se produce cuando la red contiene sistemas que utilizan RIP silencioso, los cuales no pueden supervisar la dirección de multidifusión del tráfico RIP. El RIP silencioso se produce cuando un dispositivo de red se configura para procesar las difusiones de RIP generadas por otros sistemas, pero no genera sus propias difusiones de RIP.

Máscaras de subred Al contrario de RIP v1, RIP v2 incluye una máscara de subred para cada ruta que anuncia. Esto hace que el protocolo pueda soportar redes que utilizan subredes de longitud variable o disjuntas.

Autenticación RIP v2 permite la utilización de autenticación para garantizar que los mensajes de RIOP tengan su origen en ruteadores autorizados. El RRAS de Windows NT y Windows 2000 sólo permite el empleo de contraseñas sencillas, pero algunos ruteadores *hardware* pueden utilizar para este propósito mecanismos de autenticación más avanzados, como *Message Digest 5* (MD5).

Formato de mensaje de RIP v2 El formato de mensaje de RIP v2 es el mismo que el de RIP v1, excepto que el campo versión posee el valor 2 y los campos no utilizados en ele formato original transportan ahora información adicional. El formato de mensaje de RIP v2 se muestra el la Fig. 4.11. Las funciones de los campos de las cabeceras aparecen a continuación:

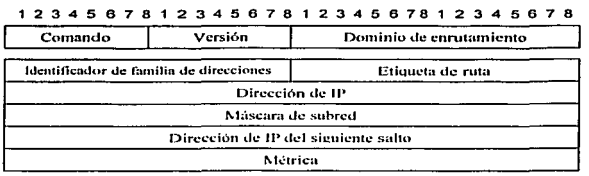


Figura 4.11. Formato de cabecera y ruta de RIP versión 2.

Campo	Longitud [bytes]	Descripción
Comando	1	Indica la función del mensaje, utilizando los siguientes valores: 1 – *Request* (Petición) Solicita la transmisión de toda la tabla de enrutamiento o de una ruta específica de todos los ruteadores de la red local. 2 – *Reply* (Respuesta) transmite las entradas de la tabla de enrutamiento.
Versión	1	Indica la versión de RIP que se ejecuta en el sistema que genera el paquete. Los valores posibles son 1 y 2.
Dominio de enrutamiento	2	Indica el proceso de enrutamiento para el que se ha generado el mensaje. Utilizando diferentes valores en este campo, los administradores pueden crear dominios de enrutamiento independientes y separa la información de enrutamiento de cada uno de ellos. El valor predeterminado es 0.
Identificador de familia de direcciones	2	Identifica el protocolo del nivel de red para el que el mensaje transporta información de enrutamiento. El valor para IP es 2.
Etiqueta de ruta	2	Contiene un valor que permite distinguir las rutas originadas dentro del sistema autónomo actual de aquellas suministradas por un protocolo de pasarela exterior o un sistema autónomo diferente. Normalmente, el valor es un número que identifica de forma única al sistema autónomo.
Dirección de IP	4	Indica la dirección de una red o *host* que está accesible a través del ruteador que genera el mensaje.

Máscara de subred	4	Contiene una máscara utilizada para diferenciar los bits del identificador de red de los del identificador del *host* en el valor del campo de dirección de IP.
Dirección de IP del siguiente salto	4	Identifica la pasarela que debería utilizar el ruteador para enviar tráfico a la red o *host* especificado en el campo de dirección de IP. En la mayoría de los casos, el ruteador debería utilizar la pasarela de la que ha recibido la ruta, pero este campo resulta adecuado para evitar la propagación de información de enrutamiento que no sea óptima. Una ruta de *host*, por ejemplo, debería indicar a los sistemas de la misma red el *host* al cual enviar directamente el tráfico, no un ruteador, y ese campo se puede utilizar para proporcionar esa información de *host*. En otro ejemplo, cuando un ruteador utiliza OSPF y RIP, puede hacer uso de RIP para propagar información de enrutamiento obtenida de OSPF, en cuyo caso el campo de dirección de IP del siguiente salto puede contener la dirección del ruteador de OSPF origen de la información.
Métrica	4	Indica el número de saltos entre le sistema que genera el mensaje y la red o *host* identifica por el valor del campo de dirección de IP.

Para proporcionar información de autenticación, RIP v2 utiliza la primera ruta de 20 bytes de un mensaje, con el formato que se muestra en la Fig. 4.12. Las funciones de los campos de esta sección del paquete de RIP v2 se muestran a continuación:

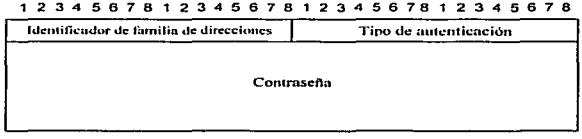


Figura 4.12. Sección de autenticación de RIP v2.

Campo	Longitud [bytes]	Descripción
Identificador de familia de direcciones	2	Contiene el valor hexadecimal FF FF, que indica que la ruta contiene datos de autenticación. Los ruteadores de RIP v1 no reconocen este valor y, por tanto, ignoran la ruta.

Tipo de autenticación	2	Indica el tipo de autenticación que utiliza el ruteador. La autenticación sencilla por contraseña utiliza el valor 2.
Contraseña	16	Contiene la contraseña de autenticación en un formato especificado por el valor del campo de tipo de autenticación.

Protocolo abierto de primero el camino más corto (OSPF)

El enrutamiento de vector de distancia posee un defecto fundamental, basa sus métricas de enrutamiento solamente en el número de saltos entre dos redes. Cuando una internetwork se compone de varias LAN en la misma ubicación, todas ellas conectadas utilizando el mismo protocolo del nivel de enlace de datos, el contador de saltos resulta ser un indicador válido. Sin embargo, cuando están implicados enlaces WAN, un salto puede hacer referencia a ruteadores de dos habitaciones contiguas o a un enlace trasatlántico, y existe una gran diferencia en el tiempo necesario para atravesar uno y otro.

La alternativa al enrutamiento de vector de distancia se conoce como *enrutamiento de estado del enlace*, utilizado sobretodo en el protocolo OSPF (*Open Shortest Path First*). OSPF es un protocolo de pasarela interior documentado por el IETF en 1989 y publicado como la RFC 1131. La especificación actual, ratificada como estándar del IETF, se publicó en abril de 1998 como la RFC 2328. La mayor parte de los ruteadores actuales soportan OSPF y RIP, incluyendo Windows XP y 2000, el RRAS de Windows NT y Novel NetWare.

Al contrario de RIP y gran parte de los demás protocolos de TCP/IP, OSPF no viaja dentro de un protocolo de transporte como UDP o TCP. Los mensajes de OSPF se encapsulan directamente en datagramas IP utilizando el número de protocolo 89.

El enrutamiento de estado del enlace, tal como se implementa en OSPF, utiliza una formula denominada algoritmo de Dijkstra para juzgar la eficiencia de una ruta, en función de varios criterios, entre los que se incluyen los siguientes:

Cuenta de saltos Aunque los protocolos de enrutamiento de estado del enlace siguen utilizando la cuenta de saltos para medir la eficiencia de una ruta, ésta sólo es una parte de la ecuación.

Velocidad de transmisión La velocidad a la que trabajan los distintos enlaces es una parte importante de su eficiencia. Obviamente, los enlaces más rápidos tienen prioridad sobre los más lentos.

Retardos por congestión Los protocolos de enrutamiento de estado del enlace consideran la congestión de red originada por el patrón actual de tráfico a la hora de evaluar una ruta y evitan los enlaces demasiados congestionados.

Costo de ruta El costo de ruta es una métrica asignada por el administrador de red para clasificar la funcionalidad relativa de las diferentes rutas. El costo puede hacer referencia literal al gasto financiero que supone el enlace o a cualquier otro factor pertinente.

El enrutamiento de estado del enlace es más complejo que RIP y requiere mayor procesamiento en el ruteador, pero juzga la eficiencia relativa de las rutas de forma más precisa y posee una tasa de convergencia mayor que RIP. OSPF también reduce la cantidad de ancho de banda utilizado por el protocolo de enrutamiento, ya que sólo transmite actualizaciones a otros ruteadores cuando se producen modificaciones en la configuración de red, al contrario que RIP, que transmite continuamente toda la tabla de enrutamiento.

Muchas de las ventajas de OSPF han servido, claramente, de inspiración para las mejoras introducidas en la versión 2 de la especificación de RIP. Por ejemplo, todas las rutas de OSPF incluyen una máscara de subred, y el ruteador receptor autentica todos los mensajes de OSPF antes de procesarlos. El protocolo también puede utilizar la información de enrutamiento obtenida de fuentes externas, como protocolos de pasarela exterior. Además, OSPF proporciona la posibilidad de crear, dentro de un sistema autónomo, áreas discretas que intercambian información de enrutamiento entre ellas. Sólo ciertos ruteadores, denominados *ruteadores de borde de área*, intercambian información con otras áreas. Esto reduce la cantidad de tráfico de red generado por el protocolo de enrutamiento.

Al contrario que RIP, OSPF puede mantener varias rutas con un destino específico. Cuando dos rutas a una misma dirección de red poseen la misma métrica, OSPF equilibra la carga de tráfico entre ellas.

La versión 2 de RIP, por tanto, es comparable con OSPF en sus características, y es, en definitiva, la alternativa preferida en una internetwork relativamente pequeña que no sufre problemas severos de tráfico. Sin embargo, en una internetwork con conexiones WAN o con muchos ruteadores provistos con grandes tablas de enrutamiento que provocarían mucho tráfico de red, OSPF es la alternativa aconsejable.

Capitulo 5 Conmutadores (Switch)

Descripción

La configuración tradicional de redes se compone de varias LAN conectadas por ruteadores para formar una red mayor de lo que sería posible con una sola LAN. Esto es necesario, ya que cada una de ellas se basa en un medio de red compartido por varias computadoras y existe límite en el número de sistemas que pueden compartir el medio sin que la red se sature de tráfico. Los ruteadores segregan el tráfico de las LAN individuales, reenviando sólo aquellos paquetes dirigidos a sistemas de otras LAN.

Los ruteadores han estado ahí durante décadas, pero un nuevo tipo de dispositivo, denominado *conmutador de LAN (Switch),* ha revolucionado el diseño de redes y ha hecho posible la creación de LAN de tamaño casi ilimitado. Un *conmutador (Switch)* es, en esencia, un puente multipuesto en el que cada uno de los puertos es un segmento de red independiente. Similar en apariencia a un concentrador, un conmutador recibe tráfico por sus puertos. Al contrario que un concentrador, el cual reenvía el tráfico a través de todos los demás puertos, un conmutador sólo reenvía el tráfico por el puerto necesario para alcanzar su destino (ver Fig. 5.1). Si, por ejemplo, existe una red de un pequeño grupo de trabajo con cada una de las computadoras conectada a un puerto del mismo concentrador conmutador, cada uno de los sistemas posee el equivalente a una conexión dedicada con cada uno de los sistemas restantes y con todo el ancho de banda.

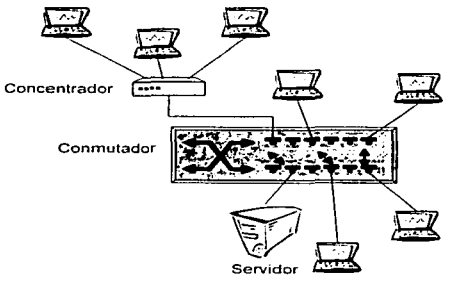


Figura 5.1. Los conmutadores transmiten el tráfico de entrada, pero sólo por el puerto específico al que va destinado.

No existe ningún medio de red compartido y, en consecuencia, tampoco existe congestión de tráfico ni colisiones. Como valor añadido, también se dispone de mayor seguridad, ya que, al no compartir un medio, una estación de trabajo no-autorizada no puede ver ni capturar el tráfico que no va dirigido a ella.

Los conmutadores operan en el nivel 2 del modelo de referencia OSI, el nivel de enlace de datos, por lo que se utilizan para crear una única red mayor, en lugar de una serie de redes pequeñas conectadas por ruteadores. Esto también significa que los conmutadores pueden admitir cualquier protocolo del nivel de red. Al igual que los puentes transparentes, los conmutadores pueden aprender la topología de una red y realizar funciones tales como filtrado y reenvío de paquetes. Algunos conmutadores también son capaces de realizar comunicaciones *full duplex* y ajustes automáticos de velocidad.

En la configuración tradicional de una gran internetwork, varias LAN se conectan a una red soporte con ruteadores. Sin embargo, la red soporte es una LAN de medio compartido con las demás y tiene que transportar, por tanto, todo el tráfico entre redes generado por las redes horizontales.

Ese es el motivo por el que, tradicionalmente, la red soporte utiliza un protocolo más veloz. En una red conmutada, las estaciones de trabajo se conectan a conmutadores de grupo individuales, las cuales, a su vez, se conectan a un único conmutador de altas prestaciones, permitiendo, por tanto, que cualquier sistema de red establezca una conexión dedicada con cualquier otro (ver Fig. 5.2). Esta configuración se puede expandir aún más para incluir también un nivel intermedio de conmutadores departamentales. Los servidores a loas que tienen acceso todos los usuarios se pueden conectar directamente a un conmutador departamental o a un conmutador de nivel superior, para obtener mayor rendimiento.

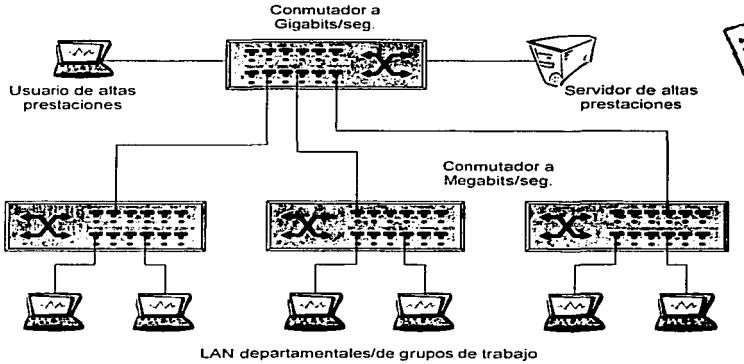


Figura 5.2. Una jerarquía de conmutadores puede sustituir a los ruteadores y concentradores.

La sustitución de concentradores por conmutadores es una forma excelente de mejorar el rendimiento de una red sin cambiar de protocolo o modificar las estaciones de trabajo individuales. Incluso una red Ethernet estándar experimenta una mejora considerable cuando a cada estación de trabajo se le proporciona un ancho de banda de 10 Mbps completos, en lugar de compartirlo con otros 20 o 30 sistemas. Los conmutadores *full duplex* pueden duplicar el ancho de banda efectivo para alcanzar 20 Mbps. Aunque la mayoría de los conmutadores de LAN del mercado están diseñados para redes Ethernet, incluyendo Fast y Gigabit Ethernet, también existen conmutadores para Token Ring y FDDI.

Aunque una red completamente conmutada proporciona un nivel de rendimiento ideal, los conmutadores son mucho más caros que los concentradores repetidores estándar y muchas redes combinan las dos tecnologías para lograr un término medio. Se puede, por ejemplo, conectar concentradores estándar a los puertos de un conmutador y compartir el ancho de banda de una conexión conmutada entre un puñado de máquinas, en lugar de varias docenas.

Tipos de conmutadores

Existen dos tipos básicos de conmutación: de envío inmediato y de almacenamiento y reenvío.

Conmutador de envío inmediato

Sólo lee la dirección MAC de un paquete de entrada, busca la dirección en su tabla de reenvío y comienza a transmitirlo de inmediato por el puerto que proporciona el acceso hacia su destino. El conmutador reenvía el paquete sin ningún procesamiento adicional, como comprobación de errores y antes, incluso, de recibir todo el paquete. Este tipo de conmutador es relativamente barato y se utiliza habitualmente a nivel departamental o de grupo de trabajo, donde la falta de comprobación de errores no afecta el rendimiento de toda la red. El reenvío inmediato de los paquetes entrantes reduce el retardo originado por la comprobación de errores y otros procesos. Sin embargo, si se está utilizando el puerto destino, el conmutador almacena en memoria los datos entrantes, originando un retardo de cualquier forma, sin el beneficio añadido de la comprobación de errores.

Conmutador de almacenamiento y reenvío

Como su nombre lo indica, almacena un paquete entrante completo en memoria antes de reenviarlo por el puerto destino. Mientras se encuentra en memoria, el conmutador comprueba el CRC (Comprobación de Redundancia Cíclica) del paquete en busca de errores y otras condiciones, como enanos (*runts*), gigantes (*giants*), y parloteo (*jabber*). El conmutador descarta de inmediato cualquier paquete con errores; los que no tienen errores se reenvían a través del puerto correspondiente. Ambos métodos de conmutación no son necesariamente excluyentes. Algunos conmutadores pueden trabajar en modo de envío inmediato hasta que se alcanza un umbral de error preestablecido, momento en el que pasan a operar en modo de almacenamiento y reenvío. Cuando los errores vuelven a caer por debajo de umbral, el conmutador vuelve a trabajar en modo de envío inmediato.

NOTA: Los enanos, gigantes y el parloteo son algunos de los errores que pueden producirse en una red Ethernet.

- Un enano es un paquete con una longitud menor de 64 bytes, originado por una NIC o un puerto de concentrador que funciona de forma incorrecta, o por un nodo que deja de transmitir en medio de un paquete debido a la detección de una colisión.
- Un gigante es un paquete mayor que el máximo de Ethernet de 1,518 bytes, causado por una NIC que está parloteando. Esta falla indica el incorrecto funcionamiento de un dispositivo *hardware* o un fallo de cable.
- El parloteo es la transmisión continua e incorrecta de tramas por parte de alguna interfaz de red que no espera a detectar la presencia de portadora o colisiones.

Los conmutadores de LAN implementan esas funciones utilizando tres posibles configuraciones *hardware*. La *conmutación de matriz*, llamada también *conmutación de barras cruzadas*, utiliza una rejilla de conexión de entrada y salida, como lo muestra la Fig. 5.3. Los datos que entran a través de cualquiera de las entradas de los puertos se pueden reenviar a la salida de cualquiera de ellos. Debido a que esta solución se basa en *hardware*, no se vincula en el proceso de conmutación a ninguna CPU o *software*. En caso de que los datos no se puedan reenviar de inmediato, el conmutador los almacena en *buffer* hasta que se desbloquea el puerto de salida.

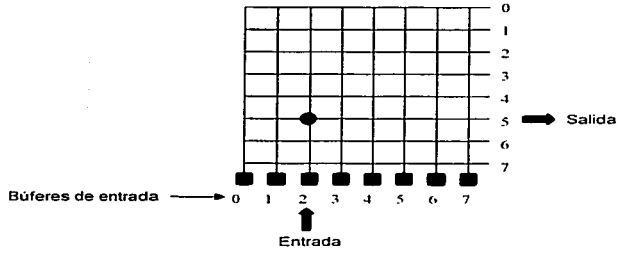


Figura 5.3. La conmutación en matriz utiliza una rejilla de circuitos de entrada y salida.

En un *conmutador de memoria compartida*, todos los datos de entrada se almacenan en un buffer de memoria compartido por todos los puertos del conmutador y, posteriormente, reenviado por un puerto de salida (ver Fig. 5.4). Una tecnología utilizada con más frecuencia, la cual se muestra en la Fig. 5.5, denominada *conmutación con arquitectura en bus*, reenvía todo el tráfico a través de un bus común utilizando multiplexado por división de tiempo, para garantizar que todos los puertos tengan acceso por igual al bus. En este modelo, cada uno de los puertos posee su buffer individual y se controla por medio de un

ASIC (*Application-Specific Integrated Circuit*, o circuito integrado específico de la aplicación).

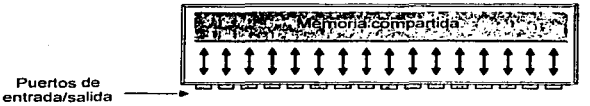


Figura 5.4. Conmutación de memoria compartida

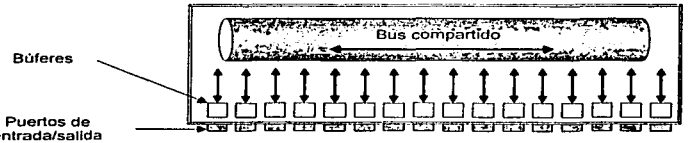


Figura 5.5. Conmutación con arquitectura en bus.

Al igual que en el caso de los concentradores, existen conmutadores para redes de cualquier tamaño, desde conmutadores baratos para grupos de trabajo, diseñados para redes de oficina pequeña, hasta unidades apilables y modulares de precio más elevado.

Enrutamiento frente a conmutación

La pregunta de si en una red es mejor enrutar que conmutar es difícil de responder. La conmutación es más rápida y barata que el enrutamiento, pero origina ciertos problemas en la mayoría de las configuraciones de red. Al utilizar conmutadores se eliminan las subredes y se crea un único segmento de red plano que alberga a todas las computadoras. Dos sistemas cualesquiera pueden comunicarse utilizando un enlace dedicado, que es, en esencia, una red temporal de dos nodos. El problema aparece cuando las estaciones de trabajo generan mensajes de difusión. Puesto que una red conmutada forma un único dominio de difusión, los mensajes de difusión se propagan por toda la red y todos los sistemas deben procesarlos, lo que puede consumir una gran cantidad de ancho de banda. Una de las ventajas de crear varias LAN y de conectarlas con ruteadores es que las difusiones se limitan a las redes individuales. Los ruteadores también proporcionan seguridad al limitar las transmisiones a una única subred. Para evitar el consumo de ancho de banda ocasionado por las difusiones, se ha hecho necesario implementar ciertos conceptos de enrutamiento en las redes conmutadas. Debido a ello han hecho su aparición gran número de tecnologías nuevas que integran el enrutamiento y la conmutación en diversos grados. Algunas de estas tecnologías se examinarán a continuación:

LAN virtuales

Una *LAN virtual*, o *VLAN*, es un grupo de sistemas de una red conmutada que funciona como una subred y se comunican con otras VLAN por medio de ruteadores. Sin embargo, la red física sigue siendo conmutada; Las VLAN existen como un revestimiento del armazón de conmutación, como lo muestra la Fig. 5.6.

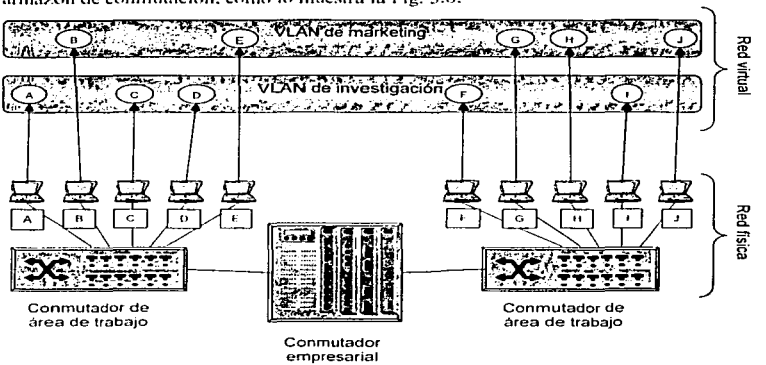


Figura 5.6. Las VLAN son seudo-redes de estaciones de trabajo conmutadas, conectadas por ruteadores.

Los administradores de red crean VLAN indicando las direcciones MAC, de puerto o de IP de los sistemas que van a formar parte de cada una de las subredes. Los mensajes de difusión de una VLAN se limitan a la subred, igual que en una red ruteada. Debido a que las VLAN son independientes de la red física, los sistemas de una red en particular pueden estar ubicados en cualquier parte, y un mismo sistema puede formar parte, incluso, de más de una VLAN.

A pesar del hecho de que todas las computadoras están conectadas por conmutadores, los ruteadores aún son necesarios para la comunicación entre sistemas de VLAN diferentes. Las VLAN que se basan exclusivamente en tecnología del nivel 2, como las que utilizan la configuración de puerto o las direcciones MAC para definir los sistemas miembros, necesitan disponer de un puerto dedicado a una conexión de ruteador. En este tipo de VLAN, el administrador de red selecciona ciertos puertos de conmutación para designar los miembros de una VLAN o crea una lista con las direcciones MAC de las estaciones de trabajo.

Debido a ese procesamiento adicional, el enrutamiento es más lento que la conmutación. Esta configuración en particular se conoce a veces como *conmuta cuando puedas, enruta cuando no te quede otro remedio*, ya que el enrutamiento sólo se utiliza para la comunicación entre las VLAN; todas las comunicaciones dentro de una VLAN son conmutadas. Se trata de una configuración eficiente, en la medida en que la mayor parte del tráfico de red, del 70 al 80 por ciento, es entre sistemas de la misma VLAN.
Se maximiza la velocidad de comunicación dentro de una VLAN a expensas de la comunicación entre las VLAN. Cuando existe mucho tráfico entre sistemas de subredes diferentes, el enrutamiento retarda demasiado el proceso y la velocidad de los conmutadores se desaprovecha en gran medida.

Conmutación de nivel 3

La conmutación de nivel 3 también utiliza VLAN, pero mezcla las funciones de enrutamiento y conmutación para que las comunicaciones entre las VLAN sean más eficientes. Esta tecnología se conoce por diversos nombres, en función del fabricante del equipo, como *conmutación IP*, *enrutamiento multinivel*, *enrutamiento inmediato* e *IP rápido*. La esencia del concepto se puede definir como *enruta primero, conmuta después*. Sigue siendo necesario un ruteador para establecer las conexiones entre los sistemas de VLAN diferentes, pero una vez establecida la conexión, el tráfico posterior viaja sobre la conmutación del nivel 2, que es mucho más rápida.

La mayoría de los dispositivos *hardware* denominados conmutadores de nivel 3 fabricados por los principales suministradores combinan las funciones de un conmutador y un ruteador en una misma unidad. El dispositivo es capaz de realizar todas las funciones estándar de un ruteador, pero también es capaz de transmitir datos utilizando conmutadores de alta velocidad, todo ello con un costo sustancialmente menor que el de un ruteador estándar. Los conmutadores de nivel 3 están optimizados para conexiones de LAN y de MAN (*Metropolitan Area Network*) pero no para WAN.

La conmutación de nivel 3 aún no ha madurado hasta el punto en que los fabricantes dispongan de soluciones completamente compatibles, pero esta tecnología podría representar potencialmente el camino ideal de mejora de las internetworks que ahora se basan en ruteadores y concentradores repetidores. Al sustituir los ruteadores que conectan redes departamentales o de grupos de trabajo a la red de soporte por conmutadores de nivel 3., se mantiene toda la funcionalidad de enrutamiento a la vez que se aumenta la velocidad global de reenvío de datos. Al final, al trasladar las conexiones de las estaciones de trabajo de los concentradores repetidores a conmutadores de nivel 2 es posible migrar a una red sin un medio compartido, excepto los enlaces de área extensa, que continuaran conectados a los ruteadores tradicionales.

Capitulo 6 Pasarelas (Gateway)

Descripción

La pasarela (Gateway) es el más complejo de todos los dispositivos de red. Potencialmente, puede operar en las siete capas del modelo OSI. Una pasarela es un convertidor de protocolos. Un ruteador por si mismo, acepta y transmite paquetes sólo a través de redes que utilizan protocolos similares. Una pasarela, en cambio, puede aceptar un paquete formateado con un protocolo (por ejemplo, *Apple Talk*) y convertirlo a un paquete formateado para otro protocolo (por ejemplo, TCP/IP) antes de reenviarlo hacia delante.

Las pasarelas conocen y entienden los protocolos usados por cada red ligada a un ruteador y es por lo tanto capaz de traducirlo de uno a otro. En algunos casos, la única modificación necesaria son los encabezados y colas del paquete. En otros, la pasarela debe ajustar la velocidad de transmisión, tamaño y formato también (ver Fig. 6.1).

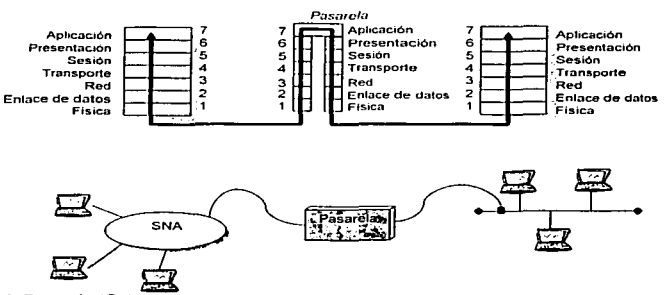


Figura 6.1. Pasarela (Gateway).

Por ejemplo, una pasarela puede recibir un paquete de una red de área local y traducirlo en un protocolo específico para poder tener acceso a una computadora central (*mainframe*) o a una red de paquetes. Por lo general, la mayoría de las pasarelas convierten cualquiera de los paquetes de Ethernet o Token Ring a un protocolo serial de bits, como es el caso de la arquitectura de red de sistemas (SNA/SDLC) de IBM. Al realizar esta conversión, una pasarela puede también realizar aquellas funciones como conversión de carácter-código, conversión de atributos de pantalla, etc.

Antecedentes

Las internetworks son entidades inherentemente heterogéneas. Los equipos que se utilizan para interconectar las redes han sido desarrollados por diferentes organizaciones, que ofrecen servicios diferentes, que imponen diferentes restricciones para acceder a dichos

servicios, y que utilizan diferentes protocolos para distribuir la información de enrutamiento y la transferencia interna de paquetes. Esto implica que, el enrutamiento en las internetworks necesite que las redes dispares que la constituyen, cooperen intensamente unas con otras.

Evolución de Internet

El sistema que hoy conocemos como Internet tuvo su origen en la ARPANET. La ARPANET se formó a finales de los 1970s. En aquel entonces, estaba dedicada a satisfacer las necesidades de comunicación de datos de una selecta comunidad, compuesta principalmente por investigadores dedicados al estudio de aspectos relacionados con redes de computadoras.

Hasta 1983 ARPANET era la única red que interconectaba varios sitios a nivel mundial. Los sitios ligados a ARPANET no tenían una conexión directa unos con otros. De modo que la topología de Internet estaba restringida a una jerarquía estricta de dos niveles, con la ARPANET en el nivel superior.

En 1983 una parte de ARPANET se dividió para crear una red separada, la MILNET. El objetivo de la MILNET era proporcionar servicio operacional a instalaciones militares. A consecuencia de esta separación la red única fue reemplazada por dos redes directamente conectadas entre sí, ARPANET y MILNET.

En 1984 la Fundación Nacional de Ciencias de los Estados Unidos (*NSF, National Science Foundation*) implementó una red de soporte (*backbone*) llamada NSFNET, cuyo propósito era proveer conectividad entre distintos institutos de investigación de aquel país, y conformar una red de investigación académica a nivel nacional. Los campus y otros sitios individuales, fueron enlazados al *backbone* a través de una o varias Redes Regionales, como es el caso de la red de investigación y educación del estado de Nueva York (NYSERNET); el *backbone* se conectó directamente a la ARPANET en varios puntos. De forma tal que, todas las redes, ARPANET, MILNET y NSFNET, estaban directamente interconectadas. La estructura jerárquica inicial de la ARPANET dio entonces paso a una topología menos restrictiva, donde algunas de las Redes Regionales tenían múltiples puntos de conexión al *backbone* NSFNET. Conexiones directas entre redes regionales fueron usadas para complementar la conectividad provista por el *backbone*, y los sitios individuales fueron conectados a una o varias Redes Regionales, y en algunos casos también a la ARPANET o a la MILNET o a ambas.

A finales de los 1980's la Internet tuvo cambios significativos. Una rápida expansión geográfica dio como resultado que la red centralizada de EUA evolucionara a una infraestructura de comunicaciones a nivel mundial. A finales de 1993 la Internet proveyó conectividad a más de 2 millones de computadoras en más de 100 países de América, Europa, Asia, África y Australia. A pesar de que la topología original de Internet fue substituida por otra mucho menos restrictiva, la estructura total aún preserva su naturaleza jerárquica. De igual forma, el enfoque de Internet se desplazó de ser primordialmente una red de investigación a una infraestructura que provee servicios de comunicación de datos a una enorme y diversa población de usuarios, como es el caso de escuelas, industria privada,

universidades, librerías, etc. La Internet evolucionó de un ambiente homogéneo a una infraestructura conformada por una colección de multi-proveedores de diversas tecnologías de red conectadas unas con otras, cuya operación esta controlada por múltiples organizaciones con metas y objetivos heterogéneos.

Proveedores de servicio y usuarios del servicio

Los recursos que conforman hoy día la infraestructura de Internet (conmutadores, subredes, etc.) pertenecen, como ya se comentó, a varias organizaciones (por ejemplo, MERIT controla los conmutadores y las subredes que integran el *backbone* NSFNET, pero no controla ni los conmutadores ni las subredes de Red Regional alguna, como pudiera ser el caso de NYSERNET). A consecuencia de esto, el proveer conexión generalizada dentro de Internet implica el compartir recursos con las organizaciones. Para cubrir los costos asociados con la adquisición y el mantenimiento de los recursos, así como tener algún beneficio económico, las organizaciones necesitan ser capaces de ejercer control sobre los recursos compartidos.

Para facilitar discusiones posteriores introduciremos dos conceptos, proveedores de servicio y usuarios del servicio. Las organizaciones que comparten sus recursos con otras organizaciones son llamadas proveedores de servicio (o simplemente proveedores). Las organizaciones que usan los recursos de otras organizaciones son llamadas usuarios del servicio (o simplemente usuarios). Usando la notación de proveedores de servicio y usuarios de servicio, podemos modelar la Internet como una colección de proveedores y usuarios de servicio interconectados.

El servicio básico suministrado por un proveedor de la capa de red consiste en un grupo de destinos (*hosts*) que pueden ser alcanzados a través de dicho proveedor. Una vez que el usuario establece conexión directa con el proveedor, puede alcanzar todos los destinos alcanzables a través del proveedor. Debido a que el valor del servicio ofrecido por el proveedor se incrementa en función del número de destinos alcanzables a través de él, los proveedores han fomentado la interconexión de unos con otros. Así, las organizaciones juegan un doble rol, como proveedor y como usuario. Por ejemplo, una Red Regional como NYSERNET actúa como proveedor de la red del campus, por ejemplo, la Universidad de Columbia, y como usuarios del *backbone* NSFNET.

Aplicaciones de pasarelas

Como ya se comentó, las pasarelas permiten interconectar redes con arquitecturas dispares. Esto significa que el diseño de las pasarelas es realizado para satisfacer los requerimientos de interconexión de dos redes en particular. Esta interconexión puede darse entre redes de conmutación de paquetes con arquitecturas distintas, o incluso entre una red de conmutación de circuitos con otra de conmutación de paquetes.

A efectos de conocer en que consisten y como operan los diferentes diseños de pasarelas, vamos a revisar 3 diferentes aplicaciones de estas:

- Pasarela entre una LAN Token Ring y un *mainframe* IBM.
- Pasarela de medios para redes móviles.

- Pasarela de medios entre redes de conmutación de circuitos y redes IP.

Pasarelas Token Ring

Las pasarelas Token Ring proveen conexión entre redes LAN Token Ring y una computadora central (*mainframe*). IBM y otros vendedores comercializan una serie de productos que ofrecen una variedad de métodos para obtener conectividad de pasarela desde una red Token Ring a un *mainframe*.

Las pasarelas IBM son computadoras personales que pueden ser conectadas a un *mainframe* a través de cualquiera de los tres tipos de tarjetas de adaptación de comunicación, IBM 3278/9, IBM SDLC, o una tarjeta adaptadora de red IBM para Token Ring.

Conectividad con un adaptador SDLC

El uso de un adaptador SDLC permite que una PC pasarela sea conectada directamente a un controlador de comunicaciones IBM, como los dispositivos 3720, 3725 o 3745. Ya que el adaptador SDLC es utilizado para obtener conectividad directa, el enlace entre la pasarela y el controlador de comunicaciones se obtiene ya sea con el uso de un par de módems o con unidades de servicio digital (*DSU, Digital Service Unit*). La Fig. 6.2 ilustra el uso de un adaptador SDLC en una PC pasarela.

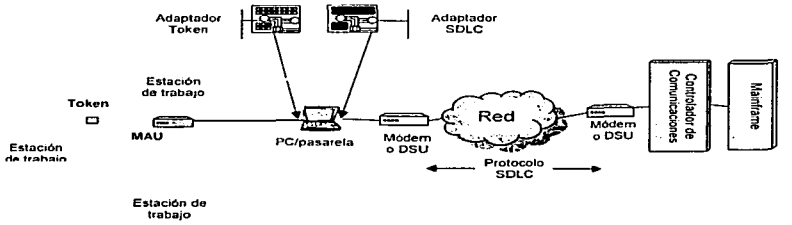


Figura 6.2. Pasarela entre Token Ring y *mainframe* IBM, utilizando un adaptador SDLC.

Cuando una pasarela utiliza un adaptador SDLC, la tasa de transmisión de datos es limitada a un máximo de 19.2Kbps cuando se comunica con el *host*. La pasarela PC se comunica con otras estaciones de trabajo de la red a través de la interfaz NETBIOS de IBM y una tarjeta de adaptación Token Ring a 4 o 16 Mbps. Una limitación clave en este método de conectividad es la tasa de transmisión de datos entre la pasarela y el *mainframe*, la cual puede convertirse en un cuello de botella con respecto al tiempo de respuesta de otras estaciones de trabajo de la red accediendo a aplicaciones del *mainframe*.

Cuando una PC es utilizada como una pasarela por medio de un adaptador SDLC, sólo la pasarela PC es reconocida como una unidad física SNA. Cada una de las estaciones de

trabajo de la red es designada como una unidad lógica (*LU, Logical Unit*). El hecho de que sólo un máximo de 32 LUs pueden ser asociadas con una unidad física (*PU, Physical Unit*) cuando se utiliza el programa de emulación de estaciones de trabajo, representa una segunda limitación relacionada con este método de conectividad. Sin embargo, el uso del programa de comunicación personal de IBM extiende el número de LUs soportadas a 254.

Conectividad con el adaptador 3278/9

El uso de la tarjeta de adaptación 3278/9 requiere que una PC pasarela sea cableada a la unidad de control 3X74 por medio de cable coaxial. La unidad de control puede estar enlazada localmente a la computadora *host* o de forma remota por medio del uso de módems o unidades de servicio digital (*DSU, Digital Service Unit*). La Fig. 6.3 ilustra la conectividad de pasarela obtenida vía un adaptador IBM 3278/9.

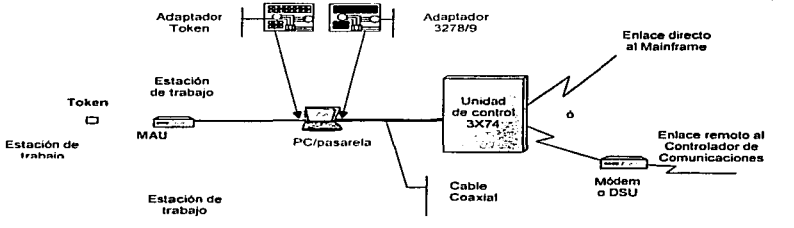


Figura 6.3. Conectividad entre una red Token Ring y un *mainframe* utilizando un adaptador 3278/9.

Una pasarela utilizando un adaptador IBM 3278/9 sólo puede soportar hasta 5 comunicaciones de estaciones de trabajo de red concurrentes hacia el *mainframe*. Esto es debido a que el puerto de la unidad de control debe ser configurado como un puerto terminal de función distribuida (*DFT, Distributed Function Terminal*), el cual está limitado a soportar 5 sesiones concurrentes. Siete pasarelas utilizando tarjetas de adaptación 3278/9 podrían ser requeridas para proveer un nivel equivalente de sesiones concurrentes obtenidas a través del uso de una tarjeta de adaptación SDLC.

Al igual que con el uso de un adaptador SDLC, la utilización de un adaptador 3278/9 presenta un cuello de botella. Este cuello de botella reside en la unidad de control 3X74 del enlace controlador de comunicaciones. A menos que se realicen modificaciones de *hardware* especiales a la unidad de control y al controlador de comunicaciones, su máxima tasa de transferencia de datos está limitada a 19.2 Kbps. Con las modificaciones de *hardware*, la tasa de transferencia de datos se incrementa a 56Kbps.

Hardware de conectividad para Token Ring

La conectividad de un *mainframe* por medio del uso del *hardware* de la red Token Ring puede realizarse por dos métodos similares. Ambos métodos eliminan el uso de una PC especial a modo de pasarela, convirtiendo a cada estación de trabajo de la LAN en una estación de trabajo combinada con pasarela.

El primer método por medio del cual el *hardware* de Token Ring puede ser utilizado para proveer conectividad a un *mainframe* se realiza con el uso de la unidad de control 3174 equipada con un adaptador de Token Ring. Este *hardware* permite que la unidad de control se convierta en un participante activo de la LAN operando a 4 o a 16 Mbps. El segundo método involucra la instalación de una tarjeta interfaz Token Ring (*TIC, Token-ring Interface Card*) en un controlador de comunicaciones IBM, el cual también habilita al controlador a convertirse en un participante activo de la LAN.

Cuando un adaptador Token Ring es usado sobre una unidad de control 3174, el cuello de botella de la tasa de transferencia de datos se da entre la unidad de control y el controlador de comunicaciones. Como ya se mencionó, este enlace está limitado a 19.2 o 56 Kbps; por lo tanto, puede soportar hasta 256 estaciones de trabajo. Cuando una TIC es utilizada, la tasa de transferencia de datos de la LAN es la tasa del flujo de datos del controlador de comunicaciones, eliminando cualquier cuello de botella en la tasa de transmisión de datos que pudiera afectar el tiempo de respuesta cuando un significante número de usuarios de estaciones de trabajo acceden a aplicaciones del *mainframe*. A diferencia de la unidad de control TRA (*Token-Ring Adapter*), el controlador de comunicaciones TIC soporta hasta 9999 estaciones de trabajo por LAN.

Pasarelas de medios (Media Gateway)

Al igual que otros elementos críticos de las redes modulares, las pasarelas de medios proveen una funcionalidad única, permiten que el tráfico de voz y datos circule a través de redes dispares de forma transparente. Una pasarela de medios puede conectar una red telefónica conmutada pública (*PSTN, Public Switched Telephone Network*) a una red con protocolo de modo de transferencia asíncrona (*ATM, Asynchronous Transfer Mode*), ATM a Internet (IP), la PSTN a IP, o incluso IP a IP cuando se utilizan diferentes protocolos o codificadores.

Pasarela de medios para redes móviles

Las empresas de telecomunicaciones están migrando a una nueva arquitectura de redes basada en capas horizontales. El control de llamadas y la conectividad, que en las redes de telecomunicaciones tradicionalmente han estado unidos, se están separando en distintas capas. La capa de conectividad se basa principalmente en la transmisión por el modo asíncrono (*ATM, Asynchronous Transfer Mode*) y el protocolo de Internet (IP). Las redes de acceso y el núcleo de la red son partes de la capa de conectividad, que ofrece interfaces a redes heredadas, tales como la red telefónica pública (*PSTN, Public Switched Telephone Network*). La arquitectura de capas se está implantando en redes móviles de la tercera generación, es decir, en el sistema de telecomunicaciones móviles universal (*UMTS, Universal Mobile Telecommunications System*). La Fig. 6.4 muestra de forma esquemática la nueva arquitectura de redes.

Se han introducido pasarelas de medios (*MGW, Media Gateway*) para que actúen como puente entre distintas tecnologías de transmisión y para añadir servicios de conexiones a usuarios finales. Una migración suave, paso a paso, hacia la nueva arquitectura de red se logra separando, en una pasarela de medios y servidores, el centro de conmutación de servicios móviles (*MSC, Mobile Services Switching Center*) y el nodo de soporte de GPRS (*SGSN, Serving GPRS Support Node*) que presta el servicio.

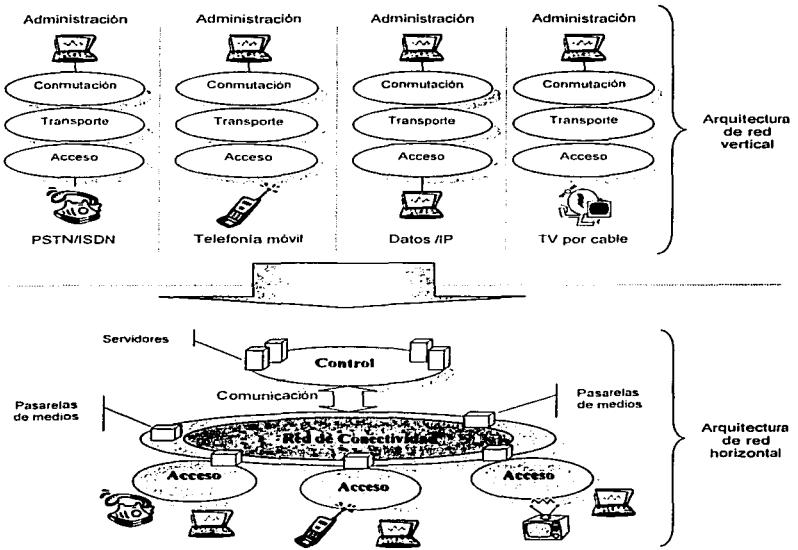


Figura 6.4. Convergencia de redes. Las redes actuales con arquitectura vertical están evolucionando a redes con arquitectura horizontal.

Introducción

A medida que las comunicaciones móviles vayan evolucionando, se ofrecerá a los usuarios finales funciones multimedia de banda ancha. Estas corrientes multimedia precisan unas

redes mucho más flexibles que las actuales, que están basadas en multiplexación por división en el tiempo (*TDM, Time-division Multiplexing*), en cuanto a proporcionar anchura de banda bajo demanda. Por tanto, la infraestructura debe evolucionar hacia tecnologías basadas en celdas y paquetes. A medida que la tecnología del transporte avanza, también cambia el paradigma de red. Las redes verticales, con una red separada dedicada a cada aplicación individual, serán reemplazadas por una arquitectura de red en capas horizontales. Las pasarelas de medios desempeñarán un papel fundamental en la evolución hacia la nueva arquitectura, mediando en el cruce entre las tecnologías existentes y de nueva transmisión, y los tipos de red. En el sistema de telecomunicaciones móvil universal (UMTS), la arquitectura en capas horizontales divide la red en:

- Una capa de aplicación.
- Una capa de control de red.
- Una capa de conectividad común.

En la capa de control de red (ver Fig. 6.5), el servidor de MSC supervisa los servicios en modo circuito, y el nodo de soporte de GPRS (*General Packet Radio Service*) en servicio (*SGSN, Serving GPRS Support Node*) supervisa las funciones en modo paquete.

En la capa de conectividad, la pasarela de medios usa interfaces abiertas para conectar diferentes tipos de nodo en el núcleo de la red y redes externas. La interfaz de control de pasarela de medios (H.248) facilita una separación de las capas de control de red y conectividad. La interfaz con la red de radio acceso terrestre de UMTS (UTRAN) se denomina *Iu*. En la figura 6.5, una llamada de voz entre la UTRAN y la PSTN se interconecta mediante dos pasarelas de medios. La pasarela A conmuta ATM o encamina el

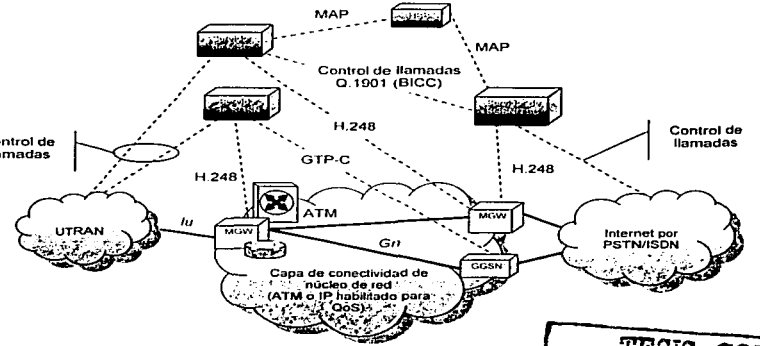


Figura 6.5. Arquitectura de red en capas, interfaces abiertas.

tráfico de IP. Asimismo, proporciona funciones de interoperabilidad entre ATM e IP. El servidor de MSC y el servidor de MSC de pasarela/centro de conmutación de tránsito (*TSC, Transit Switching Center*) controlan la pasarela de medios B mediante trayectos de control de H.248. La pasarela de medios B procesa la corriente de medios y proporciona interfaces a la PSTN. En este enfoque, el codificador de voz sólo se inserta en el borde del núcleo de la red cuando es necesario. Esto brinda una mayor calidad de voz y facilita un uso más eficiente de la anchura de banda en el núcleo de la red.

En la capa de conectividad, el interfaz *Gn* gestiona el tráfico en modo paquete entre la pasarela de medios y el nodo de soporte de GPRS (*General Packet Radio Service*) de la pasarela (*GGSN, Gateway GPRS Support Node*). El Servidor de SGSN (*Serving GPRS Support Node*) controla la pasarela de medios mediante H.248.

La calidad de servicio (*QoS, Quality of Service*) juega un papel central en las nuevas redes: constituye una manera de ofrecer un servicio cómodo a los usuarios finales y es esencial para la gestión de la red.

La pasarela de medios ofrece calidad de servicio sustentando ingeniería de tráfico de ATM e IP a través de una combinación de:

- Gestión de tráfico de ATM; para ATM, y
- Conmutación de etiqueta multiprotocolo (MPLS) y servicios diferenciados (DiffSer); para IP.

NOTAS:
Protocolo H.248.
El H.248 es un nuevo protocolo, cuyo cometido es controlar las pasarelas de medios desde los servidores. Lo ha desarrollado la Unión de Telecomunicaciones Internacional (ITU) y la *Internet Engineering Task Force* (IETF). El H.248 define un modelo de conexión que constituye un planteamiento central para describir las entidades lógicas dentro de la pasarela de medios que puede ser controlada por el servidor. Gracias a este modelo, pueden coexistir diferentes medios de transmisión, y en la conexión pueden procesarse corrientes de medios. El H.248 permite que un servidor autenticado establezca, desplace, modifique, retire y obtenga eventos que se hayan notificado en una conexión o grupo de conexiones. Un servidor puede verificar la pasarela de medios para determinar la extensión de sus posibilidades. El H.248 es un protocolo marco; es decir, pueden añadírsele nuevas funciones mediante paquetes y perfiles.

Componentes de corrientes de medios.
Ejemplos de componentes de corriente de medios:

- Codificador de voz; el codec de voz multirégimen adaptivo (AMR) es el algoritmo de codificación/descodificación de voz por defecto para UMTS. Se soportan todas las modalidades del codec de voz de AMR. Esto permite a los operadores elegir el subgrupo de codecs de voz que deseen usar en sus redes.
- Cancelador de eco; los canceladores de eco:
  - Atenúan el eco generado en la conversión entre transmisión de cuatro hilos y de dos hilos en la PSTN; y
  - Reducen la diafonía móvil.
- Datos en modo circuito; la aplicación de datos en modo circuito proporciona funcionalidad de módem a la PSTN y RDSI.

- Llamada multipartita; soporte para conversaciones entre más de dos partes.
- Emisor/receptor de tono; el emisor/receptor de tono proporciona tonos para enviar a usuarios finales y recibirlos de ellos.
- Emisor/receptor de DTMF; el emisor/receptor de DTMF envía tonos de DTMF al extremo alejado de la conexión, cuando lo solicita una estación móvil. También recibe tonos de DTMF; por ejemplo, tonos que vayan a usarse con la aplicación de mensajería interactiva.
- Mensajería interactiva; la aplicación de mensajería interactiva proporciona a los abonados mensajes informativos sobre condiciones especiales en la red o condiciones que pertenezcan al servicio en uso.
- Tasación; la función de tasación soporta la generación de información basada en el volumen, para servicios de GPRS.

Componentes de alineación de tramas de medios
La principal tarea de los componentes de alineación de tramas de medios es convertir protocolos entre distintas redes de transmisión y adaptarlos a los componentes de corriente de medios.
Los componentes de alineación de tramas de medios también soportan la funcionalidad de SGSN (*Serving GPRS Support Node*), gestionando el tráfico de datos de usuario entre el controlador de red de radio (*RNC, Radio Network Controller*) y el GGSN (*Gateway GPRS Support Node*) en la red de GPRS (*General Packet Radio Service*), interconectando dos componentes de alineación de trama de medios de protocolo de tunelización de medios (*GTP, Gateway Tunneling Protocol*). Por tanto, los túneles de GTP están adaptados en la pasarela de medios entre los interfaces *Iu* y *Gn*. Usando este mismo mecanismo, es fácil procesar las corrientes insertando un componente de corriente de medios. Por ejemplo, con la arquitectura perfilada, la red de GPRS puede expandirse fácilmente con corrientes de medios de tiempo real.

Migración hacia la nueva red

Los sistemas usuales de telefonía, descritos en términos de la nueva arquitectura de red, tradicionalmente han abarcado en el mismo nodo tanto el control de la red como las capas de conectividad. Para migrar hacia la nueva arquitectura, el MSC de la central telefónica móvil primero se divide internamente, creando un servidor de MSC y una pasarela de medios. Entonces el nodo puede dividirse físicamente (ver Fig. 6.6): el servidor de MSC se basa en central telefónica móvil, y la pasarela de medios en una plataforma de paquetes.

Una migración similar tiene lugar en la red de GPRS. El SGSN actual se divide en un servidor interno y una pasarela de medios. Estos luego pueden separarse físicamente; todas las funciones de la red de conectividad se llevan a la pasarela de medios, que, por tanto, es común para los núcleos de la red en modo circuito y en modo paquete. La citada pasarela también se introducirá en los núcleos de las redes de GSM.

Pasarela de medios

La pasarela de medios comprende diversas entidades funcionales. El nodo físico se divide en varias pasarelas de medios virtuales. Un servidor específico controla cada pasarela de este tipo, que comparte componentes de recursos visibles desde la base de datos de dichos componentes. Sin embargo, los componentes de recursos también pueden preconfigurarse, por identidad y tipo, para cualquier pasarela de medios virtual.

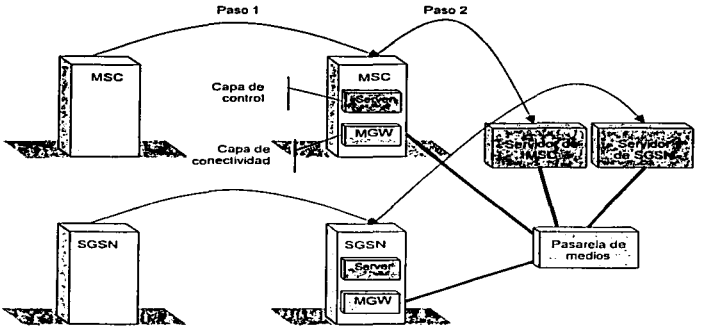


Figura 6.6. Trayecto de migración dividido de servidor-pasarela de Ericsson.

Se ha dedicado un gran cuidado para proporcionar interfaces limpias y robustas entre la pasarela de medios virtual, la base de datos de componentes de recursos y los componentes de recursos.

Dicho enfoque modular facilita una actualización suave en distintas partes (ver Fig. 6.7). Cuando llega un mensaje de H.248 del servidor, se analiza y suministra a la pasarela de medios virtual a la que pertenezca. El gestor de conexión establece la lógica de estado de la conexión y adjudica componentes de recursos disponibles de acuerdo con la base de datos de componentes de recursos. Estos componentes se interconectan para procesar una corriente y llevarla a través de la pasarela de medios de una red a otra.

Los componentes de recursos constan de componentes de alineación de tramas de medios, y componentes de corriente de medios. Los primeros efectúan la terminación de diferentes capas de protocolos, por ejemplo, IP, protocolo de datagrama de usuario (UDP) y protocolo de transporte de tiempo real (RTP). Los componentes de corriente de medios procesan las llamadas de voz y datos. Los componentes de recursos pueden considerarse como bloques versátiles para construir la arquitectura funcional.

También extraen datos relevantes sobre las prestaciones y gestión de fallos, de acuerdo con los requisitos en H.248 y los correspondientes objetos gestionados en el modelo objeto. Los componentes de recursos se interconectan con la plataforma de paquetes mediante interfaces de programas de aplicación (API).

La pasarela de medios está diseñada como una aplicación en la plataforma de paquetes, la cual es una plataforma de telecomunicaciones plenamente redundante que puede usarse

para varios productos diferentes. Su robusto sistema de control, de tiempo real, y el eficiente sistema de transporte por las celdas garantiza aplicaciones rentables que soportan la multiplexación por división en el tiempo, ATM e IP. La plataforma de ejecución de la plataforma de paquetes ofrece un grupo escalable de procesadores de intercomunicación, un sistema operativo de tiempo real distribuido, una base de datos de tiempo real distribuida, y soporte de O&M (Operación y Mantenimiento). Internamente, esta plataforma de paquetes abarca posibilidades de conmutación de ATM (incluyendo la capa de adaptación de ATM 2, AAL2).

Una estructura de conmutación de celdas permite distribuir la funcionalidad a través de placas y repisas.

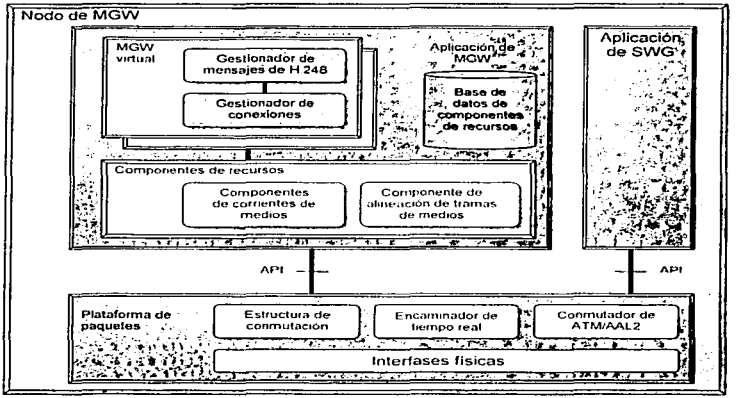


Figura 6.7. Arquitectura funcional de la pasarela de medios.

Un ruteador (router) de tiempo real integrado en la pasarela de medios, proporciona desvío distribuido a velocidades de cable a todos las interfaces. El ruteador de tiempo real:

- Gestiona IPv4, IPv6, compresión de cabecera, protocolo de seguridad de IP (IPsec), y servicios diferenciados (DiffServ).
- Proporciona funcionalidad de borde de MPLS, incluyendo ingeniería de tráfico y protección.
- Proporciona una avanzada clasificación y filtrado cortafuego.
- Soporta redes privadas virtuales (VPN).

La Fig. 6.8 muestra una visión simplificada del modelo de conexión. El gestor de conexión, que mantiene una vista lógica de las cadenas de conexión, interconecta componentes de recursos mediante la estructura de conmutación. Por tanto, los citados componentes pueden tener cualquier ubicación física en el nodo. La figura 6.8 muestra una cadena de conexión.

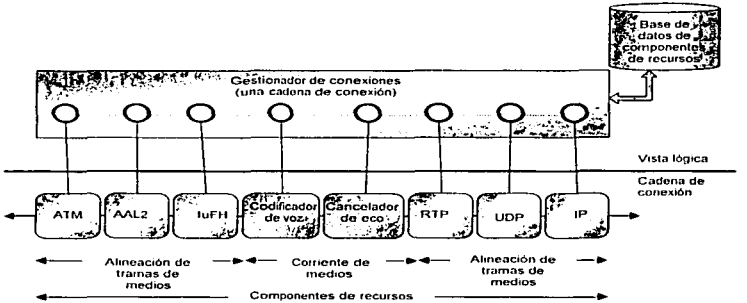


Figura 6.8. Modelo de conexión.

con voz comprimida por ATM/AAL2, convertida a voz sin comprimir por IP (VoIP). En este ejemplo, la codificación de voz y cancelación de eco se realizan en la corriente de voz.

Insertando distintos tipos de alineación de tramas de medios, y componentes de corriente de medios, es posible establecer bajo demanda el procesamiento de virtualmente cualquier corriente de medios. Sólo se necesita un pequeño juego de tipos de componentes, y en una cadena de conexión no es necesario preparar por adelantado todas las combinaciones venideras de funcionalidad.

La pasarela de medios comprende varios interfaces físicos con regímenes de 1,5 a 155 Mbit/s. Las versiones futuras incluirán interfaces de 622 Mbit/s y 2,5 Gbit/s, y Ethernet Gigabit.

La interfaz hacia la estructura de conmutador no depende de la velocidad de transmisión o la tecnología. Los operadores pueden actualizar la estructura de conmutación, interfaces o placas de procesador sin perturbar el tráfico.

Pasarela de señalización

En muchas configuraciones de red, la señalización y corriente de medios comparten las mismas líneas físicas que la pasarela de medios. Se precisa una función de pasarela de señalización para trasladar los mensajes de señalización a través de diferentes dominios de

transporte. Por ejemplo, los mensajes de control de llamada deben cambiarse por una llamada que abarque un núcleo de red basado en IP y la PSTN. Estos mensajes se preparan entre los servidores pero la llamada se transmite a través del nodo de pasarela de medios. Para reducir la superficie sobre el suelo, la aplicación de pasarela de señalización, que proporciona interoperabilidad de señalización entre las redes de IP, ATM y TDM, también se ha ubicado junto con el nodo de pasarela de medios. La aplicación de pasarela de señalización contiene asimismo funcionalidad de punto de transferencia (STP) a fin de retransmitir mensajes del sistema de señalización núm. 7 (SS7) por la parte de transferencia de mensajes (MTP3 y MTP3b) en redes TDM y ATM, así como por el protocolo de transporte de control de corriente (SCTP) en redes de IP.

Pasarela de medios entre redes de conmutación de circuitos e IP

En la industria de las telecomunicaciones, los cambios drásticos son raros. Por ejemplo, durante los últimos treinta años hemos atestiguado cambios dramáticos sólo en dos ocasiones: la evolución de la tecnología analógica a la digital y la introducción de la tecnología móvil celular. Con la entrada al siglo XXI, otro cambio significativo está tomando forma: el mundo se está adaptando a la tecnología IP.

Este cambio se dio a raíz de los rápidos avances en el ámbito regulatorio promovido por la privatización de los monopolios en telecomunicaciones de todo el mundo. Esto generó, un nuevo entorno en las Telecomunicaciones, un entorno de competencia en donde los usuarios impersonales de los servicios se convirtieron en clientes valiosos. Los servicios existentes se ofrecen a precios menores para enfrentar a la competencia, y nuevos servicios están siendo demandados para mejorar la eficiencia en los negocios y explotar las redes de telecomunicaciones como una herramienta estratégica de negocios globales altamente competitivos. Los avances en la tecnología, el rápido crecimiento de Internet, y la nueva generación de poderosas computadoras están devorando la capacidad de ancho de banda disponible, la cual tiene un impacto considerable en las redes de área amplia existentes (WAN). Este creciente apetito de ancho de banda cambia las reglas de la topología y el diseño de las redes tradicionales. La capacidad es la clave de la nueva generación de redes que hoy día están siendo diseñadas e implementadas.

El protocolo de Internet provee los ingredientes esenciales que requiere la receta de todas las redes futuras que cambiaran la forma en la que trabajamos y jugamos. El utilizar IP como un agente de convergencia para enlazar voz, datos y video en un sólo flujo de comunicación representa beneficios económicos obvios tanto para operadores como para usuarios en general.

Esta es la carrera de la cual formaremos parte en este nuevo milenio. Los jugadores en este juego son muchos, incluyendo:

- Proveedores que diseñaron y construyeron redes de comunicaciones durante los últimos cien años.
- Los carriers que mantuvieron y evolucionaron estas redes.

- La nueva raza de vendedores que ofrecen soluciones radicales para este nuevo entorno.
- Y el nuevo grupo de carriers que se han incorporado a esta industria con una muy alta sensibilidad empresarial y una urgencia por tener éxito.

Características de las pasarelas de medios

Como lo ilustra la Fig. 6.9, las pasarelas de medios proveen conectividad entre redes de conmutación de circuitos y redes IP. La flexible arquitectura de las pasarelas de medios permite que las llamadas de conmutación de circuitos tradicionales, como la voz, datos y fax, entren o salgan del mundo de IP. Las pasarelas de medios que hoy día se encuentran en el mercado, cumplen con tres características básicas:

- Multiservicio.
- Multi-entrega.
- Integración.

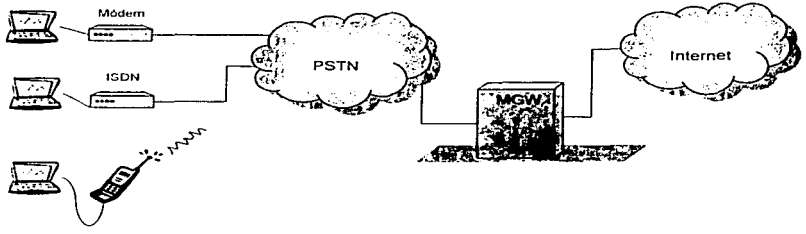


Figura 6.9. La pasarela de medios es un "puente" de comunicación entre la red telefónica pública (PSTN) y el mundo de conmutación de paquetes de IP.

Multiservicio

Por multiservicio debemos entender la habilidad de ofrecer diferentes aplicaciones sobre una sola plataforma. En un mundo que está convergiendo rápidamente, esto significa la habilidad de soportar voz, datos y video sobre IP. El resultado es la capacidad de ofrecer cualquier tipo de servicios sobre IP, incluyendo voz, fax, datos de alta velocidad, datos de módem, datos de celular, y video. Para conseguir esto, las pasarelas de medios son lo suficientemente flexibles para reaccionar en función de las demandas del usuario. Por ejemplo, en un instante dado, una llamada sobre un puerto puede requerir que tráfico módem sea convertido al protocolo Internet, y momentos más tarde ese mismo puerto puede ser requerido para convertir una llamada de voz de conmutación de circuitos a IP. De igual forma, la pasarela debe ser capaz de determinar cuando se debe o no establecer una conexión (servicio de autenticación y confirmación de que dicha capacidad está disponible para el tipo de servicio solicitado), para lo cual se basa en el número marcado, el indicador de la llamada, el indicador de transporte, o el nombre del dominio del que llama.

Por ejemplo, si un usuario solicita puertos adicionales para una aplicación de acceso remoto, el operador de red puede incrementar inmediatamente la asignación de puertos, o puede reasignar automáticamente puertos a diferentes aplicaciones con base en la hora y fecha.

Multi-entrega

Por multi-entrega debemos entender la habilidad de ofrecer diferentes interfaces de red para igualar los modelos de red en uso por los proveedores de servicio. La clásica tarea de concentración ha sido para soportar exclusivamente tráfico conmutado, usualmente a través de T1 (1.5Mbps) o E1 (2 Mbps) o accesos primarios (*PRI, Primary Rate Interface*) conectados a centrales públicas u oficinas centrales utilizando señalización de red digital de servicios integrados (*ISDN, Integrated Services Digital Network*) o algún tipo de canal común. Sin embargo, existen pasarelas en el mercado que además de esto ofrecen capacidad para manejar líneas rentadas desde 56 Kbps hasta una señal digital nivel 3 (DS3, 44.736 Mbps). *Frame Relay*, X.25, Servicios de datos multimegabit conmutados (*SMDS, Switched multi-megabit data service*), ATM (*Asynchronous Transfer Mode*), y xDSL (incluyendo ADSL y SDSL).

Desde la perspectiva de los proveedores de servicio los beneficios del multi-entrega son obvios: una sola plataforma para soportar múltiples servicios de acceso.

Integración

El término POP en una caja (*POP in a Box*), que es ampliamente utilizado en Norte América, se refiere a los productos que proporcionan, en una sola plataforma, acceso, enrutamiento y conectividad WAN. Arquitecturas de este tipo no sólo atraen a pequeños proveedores quienes están preocupados por el costo del capital sino también a grandes proveedores quienes están preocupados por el desempeño, el espacio, y aspectos operacionales.

En este contexto, integración significa que las pasarelas son capaces de manejar diferentes tecnologías de acceso, como módem, ISDN, celular, datos, voz sobre IP y fax. Además, integración significa soportar una variedad de protocolos de enrutamiento, incluyendo el Protocolo de información de enrutamiento (*RIP, Routing Information Protocol*), el Protocolo abierto de primero el camino más corto (*OSPF, Open Shortest Path First*), y protocolos de pasarela de frontera (*BGP-4, border gateway protocol*), el cual permite una conexión directa hacia Internet. Integración también implica mínimo retardo en la forma en la que el tráfico pasa del mundo de conmutación de circuitos al de conmutación de paquetes.

Pasarela en el mundo de banda angosta

Una de las aplicaciones más comunes de las pasarelas de medios es la de pasarela de banda angosta dentro del ancho de banda de una red IP. Como tal, su principal función es convertir señales de módem, fax, ISDN, datos o voz en paquetes IP. En la configuración más simple, una pasarela puede estar conectada con circuitos T1s o E1s desde la central telefónica pública o la oficina central y convertir el tráfico entrante en paquetes y señales IP (ver Fig. 6.10).

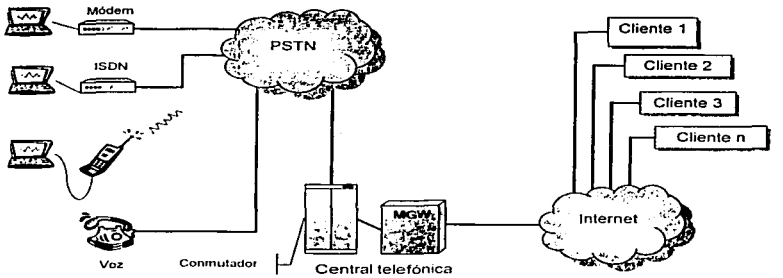


Figura 6.10. Pasarelas en el mundo de banda angosta.

Esta aplicación común provee mecanismos, basados en estándares, para conectar cualquier tipo de equipo de una central pública. Sin embargo, aunque esto ofrece un mecanismo de conexión sencillo para el proveedor de servicio, tiene una debilidad inherente. La debilidad más importante es la carga de tráfico inusual que es generada en las centrales públicas cuyo modelo de llamadas están enfocado para manejar altas tasas de llamadas con cortos tiempos de duración. Por su parte, el mundo de IP se caracteriza por una tasa de llamadas baja y largos tiempos de duración.

Desafortunadamente, este nuevo fenómeno de tráfico está generalmente fuera del control del proveedor de servicio, ya que en muchos casos, el servicio de IP es suministrado por ISP (*Internet Service Provider*) independientes y no por el proveedor de servicio que opera la red telefónica pública. Las consecuencias de esta relación varían a lo largo del mundo, dependiendo de la regulación local, y de las políticas acerca del manejo de tráfico, pero en general ocasiona congestión en la red y un incremento en el crecimiento de la red con una pequeña o nula utilidad extra. Otras áreas de preocupación en este modelo son:

- El costo de los circuitos T1/E1 o ISDN.
- El impacto de estos circuitos en el control lógico de la central pública.
- El impacto de pasarelas con sistema de señalización no. 7 (SS7) no probadas con la red CCITT no. 7.
- Aspectos de mantenimiento y operación del nuevo equipo.

Pasarelas en un mundo de banda ancha

Las pasarelas de medios son elementos naturales de las redes de banda ancha. Debido a que muchas de ellas están equipadas con capacidades ATM, pueden ser conectadas directamente a redes ATM basadas en paquetes. Existen en esencia dos formas de hacer esto:

- Utilizando el estándar de conmutación de etiquetas multiprotocolo (*MPLS, Multiprotocol Label Switching*). En este caso, la pasarela de medios interconecta internamente el equivalente a un conmutador ATM MPLS. En esta operación, el conmutador ATM funciona como un ruteador dentro de la red, de la misma forma como si un nuevo ruteador hubiera sido conectado a la pasarela de medios.
- Utilizando el estándar multiprotocolo sobre ATM (*MPOA, MultiProtocol Over ATM*). En esta modalidad, la pasarela de medios provee una conexión virtual en un conmutador ATM basado en MPOA. Un servidor de enrutamiento centralizado provee comandos de enrutamiento a la pasarela de medios.

Pasarela en un mundo 100% IP

Esta última aplicación ofrece ventajas para los nuevos proveedores de servicio que están entrando al mercado, con una red de transmisión IP pura. Al igual que las redes enrutadas actuales, este sistema ofrece ciertos beneficios. Es, sin embargo, un rol de ruteador puro que transfiere paquetes sobre enlaces de alta velocidad con un alto desempeño.

En este contexto, una pasarela de medios funciona como un ruteador de acceso conectando máquinas de ruteo masivo.

Capitulo 7 Modems

Transmisión digital de datos

Una de las primeras preocupaciones que surgen cuando se desea transmitir datos de un dispositivo a otro, es el cableado. La transmisión de datos binarios puede realizarse en modo serial o en modo paralelo. Existe una sola forma de enviar datos en modo paralelo, y dos subclases para la transmisión en modo serie: síncrona y asíncrona.

Transmisión en paralelo

Los datos binarios (1's y 0's), pueden estar organizados en grupos de *n* bits. Al agrupar es posible enviar *n* bits en cada ocasión en lugar de uno por uno. Esto es llamado transmisión en paralelo.

El mecanismo para la transmisión en paralelo es conceptualmente sencillo: utiliza *n* alambres para enviar *n* bits a la vez. De esta forma, cada bit tiene su propio cable y los *n* bits de un grupo pueden ser transmitidos de un dispositivo a otro con cada pulso de reloj. La Fig. 7.1 muestra como trabaja la transmisión en paralelo para $n = 8$. Típicamente se utilizan grupos de 8 alambres por cable con un conector en cada extremo.

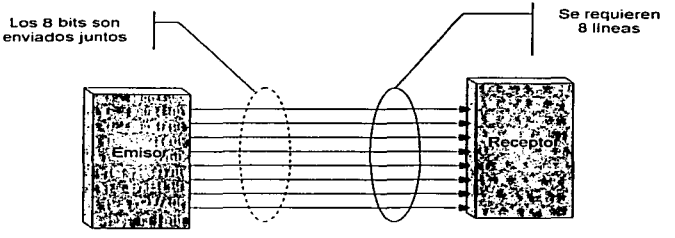


Figura 7.1. Transmisión en paralelo.

La ventaja de la transmisión en paralelo es la velocidad. Manteniendo todo lo demás constante, la transmisión en paralelo puede manejar velocidades de transferencia *n* veces mayores a la de la transmisión serial. Sin embargo, existe una desventaja significativa: el costo. La transmisión en paralelo requiere *n* líneas de comunicación para transmitir el flujo de datos. Debido a esto es una solución cara, por lo que usualmente está limitada a distancias cortas no mayores de 10 metros.

Transmisión en serie

En la transmisión serial un bit sigue al otro, de forma tal que sólo necesitamos un canal de comunicación en lugar de *n* para transmitir datos entre dos dispositivos. La Fig. 7.2 ilustra en que consiste la transmisión serial.

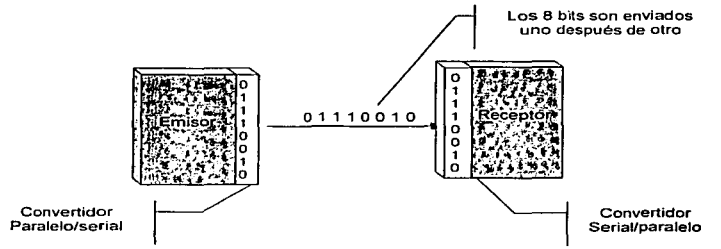


Figura 7.2. Transmisión en serie.

Las ventajas de la transmisión en serie es el costo, ya que al utilizar un sólo canal de comunicación para realizar la transmisión de datos, los costos se reducen con un factor de *n* respecto a la transmisión en paralelo.

En virtud de que los dispositivos se comunican de forma paralela, se requieren dispositivos de conversión entre el sistema emisor y la línea de transmisión (paralelo-serial) y entre la línea y el receptor (serial-paralelo).

La transmisión en serie se puede llevar a cabo en forma asíncrona o síncrona.

Transmisión asíncrona

La transmisión asíncrona es llamada así debido a que el ritmo de transmisión de la señal no es importante. La información es recibida y traducida con base en patrones o diseños previamente establecidos. Con sólo seguir dichos patrones, el dispositivo receptor puede recuperar la información sin depender del ritmo con que esta fue enviada. Los patrones están basados en el agrupamiento de cadenas de bits en bytes. Cada grupo, usualmente de 8 bits, es enviado a través del enlace como si se tratara de una unidad. El sistema emisor maneja cada grupo de forma independiente, retransmitiéndolo al enlace cada vez que este está listo, sin importar la temporización.

Sin un pulso de sincronización, el receptor no puede utilizar un temporizador para pronosticar cuando arribará el siguiente grupo de información. Con la intención de que el receptor se entere del arribo de un nuevo grupo de datos, un bit extra es añadido al principio de cada byte. Este bit, usualmente igual a 0, es llamado *bit de arranque*. Para permitir que

el dispositivo receptor sepa que el byte ha terminado, uno o más bits adicionales son añadidos al final del byte. Estos bits, usualmente 1s, son llamados *bits de parada*. Al utilizar este método, el tamaño de cada byte se incrementa hasta alcanzar, al menos, 10 bits, de los cuales 8 son información y 2 o más son señales para el sistema receptor. Además de esto, la transmisión de cada byte puede ser seguida por un *hueco sin información real* (*gap*) de duración variable. Este *gap* puede ser representado por un canal libre o por una cadena de bits de parada adicionales.

Los bits de arranque y parada y el gap alertan al receptor del inicio y fin de cada byte, permitiendo su sincronización con la cadena de datos. Este mecanismo es llamado asíncrono porque, a nivel de byte, el emisor y el receptor no tienen que estar sincronizados. Sin embargo, dentro de cada byte, el receptor debe estar sincronizado con la cadena de bits entrante. Esto significa que, de cualquier forma, alguna sincronización es requerida, aunque sólo sea por la duración de un solo byte. El dispositivo receptor se re-sincroniza al comienzo de cada nuevo byte. Cuando el receptor detecta un bit de arranque, fija un temporizador e inicia el conteo de los bits que se van recibiendo. Después de *n* bits el receptor busca el bit de parada. Tan pronto como detecta dicho bit, ignora cualquier otro pulso recibido hasta que vuelva a detectar el siguiente bit de arranque. La Fig. 7.3 ilustra esquemáticamente la transmisión asíncrona.

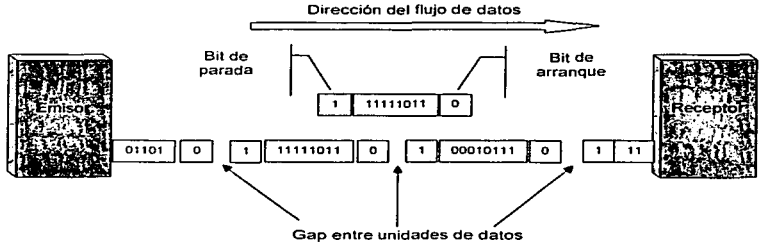


Figura 7.3. En este ejemplo, los bits de arranque son 0s, los bits de parada son 1s, y los intervalos están representados por espacios vacíos en lugar de bits de parada adicionales.

La adición de bits de arranque y parada así como la inserción de gaps, entre la cadena de bits, hace que la transmisión asíncrona sea más lenta que aquellas que operan sin la necesidad de añadir información de control. Pero, por otro lado, es barata y efectiva, dos ventajas que la hacen una opción atractiva para comunicaciones que no demanden altas velocidades. Por ejemplo, la conexión entre una terminal y una computadora es una aplicación natural para la transmisión asíncrona.

Transmisión síncrona

En la transmisión síncrona, la cadena de bits se integra en largas tramas, las cuales pueden contener múltiples bytes. Cada byte, sin embargo, es introducido en el enlace de transmisión sin añadir gaps entre ellos. Es responsabilidad del receptor separar la cadena de bits en bytes para fines de decodificación. En otras palabras, los datos son transmitidos como si se tratara de una cadena no-interrumpida de 1s y 0s, y el receptor separa los bits en bytes, o caracteres, para poder reconstruir la información. La Fig. 7.4 muestra de forma esquemática en que consiste la transmisión síncrona.

Como ya se mencionó, el sistema emisor pone los datos en la línea como si se tratara de una sola y larga cadena de información. Si el emisor desea enviar datos en ráfagas separadas, los gaps entre cada una de ellas deben ser llenados con una secuencia especial de 1s y 0s que significan libre. El receptor cuenta los bits y los agrupa en unidades de ocho bits.

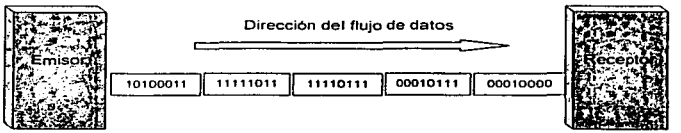


Figura 7.4. Transmisión síncrona.

Sin gaps ni bits de arranque y parada, no existe un mecanismo que ayude al dispositivo receptor a ajustar su sincronización de bits en cadenas. La temporización se convierte entonces en algo vital, debido a que la precisión de la información recibida es completamente dependiente de la habilidad que el dispositivo receptor tenga de mantener un conteo preciso de los bits que recibe.

La ventaja de la transmisión síncrona es la velocidad. Sin la necesidad de tener que incluir bits extras o gaps entre los bytes enviados, y en consecuencia, por tener que enviar un menor número de bits a través del enlace, la transmisión síncrona es más rápida que la asíncrona. Por esta razón, es mucho más frecuente su utilización en aplicaciones de alta velocidad como la transmisión de datos entre dos computadoras. La sincronización de bytes se realiza en la capa de enlace de datos.

Interfaz DTE-DCE

Usualmente existen 4 unidades funcionales involucradas en la comunicación de datos: un Equipo Terminal de Datos (*DTE, Data Terminal Equipment*) y un Equipo de terminación del circuito de datos (*DCE, Data Circuit-terminating Equipment*) en un extremo del enlace y un DCE y un DTE en el otro, como se muestra en la Fig. 7.5. El DTE genera los datos y los transfiere, junto con toda la información de control requerida, a su DCE. El DCE tiene

la responsabilidad de convertir la señal a un formato apropiado para el medio de transmisión e introducirlo en el enlace de red. Cuando la señal llega al receptor final, se realiza el proceso inverso.

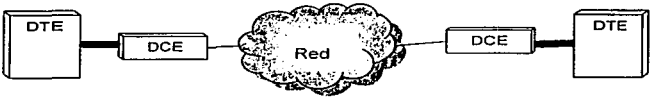


Figura 7.5. DTE y DCE

Equipo terminal de datos (DTE)

El equipo terminal de datos (DTE) incluye cualquier unidad que funcione como origen o como destino de datos digitales. En la capa física, pudiera ser una terminal, una computadora, una impresora, un fax, o cualquier otro dispositivo que genere o consuma datos digitales. Las DTE no suelen comunicarse directamente unas con otras, ellas generan y consumen información pero requieren de un intermediario para que puedan comunicarse.

Equipo de terminación de circuito de datos (DCE)

Un equipo de terminación de circuito de datos (DCE) incluye a cualquier unidad funcional que transmita o reciba datos a través de la red, en forma analógica o digital. En la capa física, una DCE toma los datos generados por la DTE, los convierte en una señal apropiada y la introduce al medio de comunicación. Usualmente los DCE utilizados en esta capa incluyen módems (modulador/de-modulador). En cualquier red, una DTE genera datos digitales y los pasa a una DCE. La DCE convierte los datos a un formato aceptable para el medio de transmisión y envía la señal convertida a otro DCE sobre la red. El segundo DCE toma señal de la línea, la convierte a un formato utilizable por su DTE, y la entrega. Para que esta comunicación sea posible, ambos, el DCE emisor y receptor deben utilizar el mismo método de codificación (FSK, PSK, etc.). No es necesario que los DTE estén coordinados uno con otro, pero cada uno de ellos debe estar coordinado con su propio DCE y los DCE, a su vez, deben estar coordinados entre ellos para que la transferencia de información pueda llevarse a cabo sin perder su integridad.

Interfaz EIA-232

Uno de los estándares de interfaz más importante desarrollado por la EIA (*Electronic Industries Association*) es la EIA-232, el cual define las características mecánicas eléctricas y funcionales de la interfaz entre un DTE y un DCE. Editada inicialmente en 1962 como el estándar RS-232, la EIA la ha revisado y robustecido en varias ocasiones. La versión más reciente, la EIA-232-D, no sólo define los tipos de conectores a ser usados sino que también define los cables y enchufes (*plugs*) así como la funcionalidad de cada pin.

Especificación mecánica

La especificación mecánica del estándar EIA-232 define la interfaz como un cable con 25 alambres en cuyos extremos se fijan conectores DB25 macho y hembra. La longitud del cable no debe exceder los 15 metros.

Un conector DB-25 es un enchufe *(plug)* con 25 pines o receptáculos, cada uno de los cuales está unido a un solo alambre con una función en particular. Con este diseño, es posible manejar 25 interacciones diferentes entre un DCE y un DTE.

La EIA-232 especifica que el cable de 25 alambres debe contar con un conector macho en un extremo y con uno hembra en el otro. En el conector DB25, los pines y tubos están ordenados en 2 renglones, el superior con 13 de pines y el inferior con 12.

Especificación Eléctrica

La especificación eléctrica del estándar define los niveles de voltaje y el tipo de señal que será transmitida en cada dirección entre la DTE y la DCE. EIA-232 establece que todos los datos deben ser transmitidos en forma de 1s y 0s utilizando una codificación digital-digital de no retorno a cero (NRZ-L), donde 0 define al voltaje positivo y 1 al negativo.

Envío de datos. En lugar de definir un simple rango con amplitudes máximas y mínimas. La EIA-232 define dos rangos distintos, uno para voltajes positivos y otro para negativos. El receptor reconoce y acepta como una señal real cualquier señal que caiga dentro de estos rangos, y no así a aquellos voltajes por afuera de los rangos. Para ser reconocido como un dato, la amplitud de la señal debe caer entre 3 y 15 voltios o -3 y -15 voltios.

Control y temporización

Sólo 4 de los 25 cables de la interfaz EIA-232 son utilizados para funciones relacionadas con los datos. Los 21 restantes están reservados para funciones como control, temporización, aterrizaje y prueba. La especificación eléctrica para estos otros alambres es similar a la de aquellos que gobiernan la transmisión de datos, pero más sencilla. Cualquiera de las funciones se considera ON si el voltaje transmitido es al menos +3 voltios; y OFF si el voltaje transmitido es menor de -3 voltios.

Es importante resaltar que el valor de OFF se consigue mediante la transmisión de un voltaje específico. La ausencia de voltaje en cualquiera de estos alambres mientras que el sistema esta operando significa que algo no está trabajando adecuadamente, y no que la línea está puesta en OFF.

Una función muy importante de la especificación eléctrica es la definición de la tasa de transferencia de bits (*bit rate*). EIA-232 permite un *bit rate* máximo de 20 Kbps, a pesar de que en la práctica esto es excedido frecuentemente.

Especificación funcional

La EIA-232 define las funciones asignadas a cada uno de los 25 pines del conector DB-25. La Fig. 7.6 muestra el orden y la funcionalidad de cada pin para un conector macho.

Es importante recordar que para un conector hembra las funciones de cada receptáculo serán una imagen espejo del conector macho, de forma tal que el pin 1 del enchufe coincida con el tubo 1 del receptáculo, y así con todos los pines. Cada función de comunicación tiene un espejo o función de respuesta para tráfico en dirección opuesta, con la intención de permitir la operación *full duplex*. Por ejemplo, el pin 2 es para transmisión de datos, mientras que el pin 3 es par recepción de datos. En este sentido ambas partes pueden transmitir datos al mismo tiempo. Como se puede observar en la Fig. 7.6, no todos los pines están asignados a una función en particular. Los pines 9 y 10 están reservados para usos futuros y el pin 11 aún no ha sido asignado.

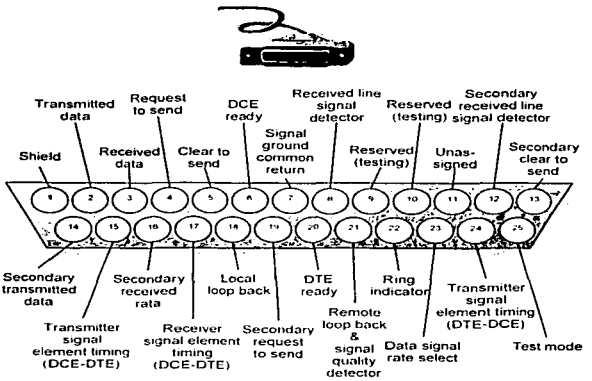


Figura 7.6. Funciones de los pines según la EIA-232.

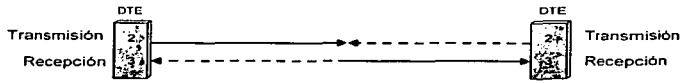
Null modem

Supongamos que ahora deseamos conectar 2 DTE en el mismo edificio, por ejemplo, dos estaciones de trabajo o una terminal a una estación de trabajo. En este caso, los módems no serían necesarios, ya que la transmisión no atraviesa líneas analógicas, y por lo tanto no requiere ser modulada. Lo que necesitamos es una interfaz que maneje el intercambio de datos, de la misma forma en que lo hace un cable EIA-232.

La solución, provista por el estándar de la EIA, es llamada *null modem*. Un *null modem* provee la interfaz DTE-DCE / DCE-DTE sin DCE. El esquema *a* de la Fig. 7.7, muestra una conexión a través de la red telefónica. Los dos DTE están intercambiando información a través de los DCE. El cable EIA-232 conecta el pin 2 del DTE con el pin 2 del DCE (transmisión) y el pin 3 del DCE con el pin 3 del DTE (recepción). El tráfico que circula por el pin 2 es siempre saliente de los DTE. Mientras que el tráfico de los pines 3 es siempre entrante a los DTE. Un DCE reorganiza la dirección de la señal y la pasa a través del circuito correcto.

El esquema *b* de la figura, muestra lo que ocurre cuando utilizamos las mismas conexiones entre dos DTE. Sin DCE que conmuten la señal desde o hacia los pines adecuados, ambos DTE están intentando transmitir sobre el mismo alambre conectado al pin 2, y de recibir sobre el mismo alambre conectado al pin 3. Las DTE están transmitiendo hacia el pin de transmisión del otro, en lugar de hacerlo hacia el de recepción.

a). DTEs conectados a través de DCEs.



b). DTEs conectados directamente.

Figura 7.7. Utilización de una conexión de pines de datos regular con y sin DCE.

Crossing connections. Para que la transmisión ocurra, los cables deben estar cruzados de forma tal que el pin 2 del primer DTE se conecte al pin 3 del segundo DTE; y el pin 2 del segundo DTE al pin 3 del primer DTE. Estos dos pines son los más importantes. Sin embargo, muchos otros pines tienen problemas similares y sus cables también tienen que ser reconectados.

Un *null modem* es una interfaz EIA-232 que completa los circuitos necesarios para engañar a los DTE y que crean que tienen un DCE y una red entre ellos. La Fig. 7.8 muestra la configuración de un cable *null modem*.

Es importante resaltar que un cable interfaz DTE-DCE cuenta con un conector macho en un extremo y hembra en el otro, mientras que un cable *null modem* tiene conectores hembra en ambos extremos para poderse conectar al puerto de la DTE el cual es macho.

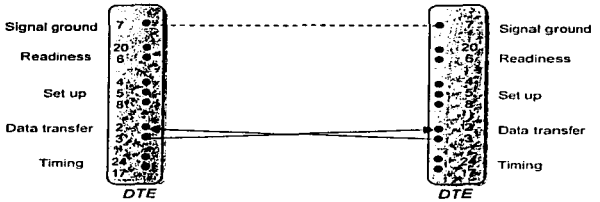


Figura 7.8. Conexión de pines de un cable *null modem*.

Módem

El más común de los DCE es el módem. El módem interno o externo asociado a una computadora personal es el responsable de convertir la señal digital, generada por la PC, a una señal analógica para ser transportada por una línea telefónica convencional. Es también el dispositivo que convierte las señales analógicas, recibidas sobre la línea telefónica, en señales digitales que son utilizadas por la computadora remota.

El término módem es una palabra compuesta que se refiere a las dos entidades funcionales que lo conforman: un modulador de señal y un demulador de señal. La relación de estos dos elementos se muestra en la Fig. 7.9.

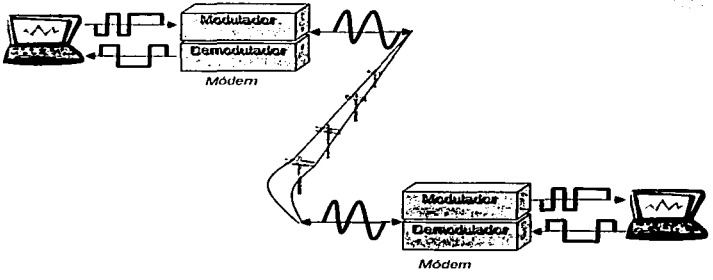


Figura 7.9. Concepto módem.

Un modulador convierte una señal digital en una analógica y un demulador hace exactamente lo contrario. A pesar de que el demulador se asemeja a un codificador analógico-digital, de ningún modo son lo mismo. El demulador no realiza muestreos de una señal para crear un tren de información digital, sino que simplemente reinvierte el proceso de la modulación.

Tanto el modulador como el demulador, sin embargo, hacen uso de la misma técnica utilizada por un codificador analógico-digital: los moduladores para codificar la señal y los demuladores para decodificarla. Un modulador maneja las señales digitales como una serie de 1s y 0s, de forma tal, que puede convertirla por completo en una señal analógica utilizando alguno de los mecanismos de conversión digital-analógica (ASK, FSK, PSK y QAM).

(*Para conocer como operan los diferentes tipos de codificación y sus mecanismos, referirse al Apéndice D*).

Velocidad de transmisión

En términos generales, la velocidad de transmisión no es otra cosa que la cantidad de bits por segundo que un dispositivo puede transmitir o recibir. Pero antes de referirnos a las diferencias entre módems comerciales y sus velocidades de transmisión, debemos examinar las limitaciones, que a nivel de velocidad de transmisión, presentan los medios.

Bit rate y Baud rate

Frecuentemente los términos *bit rate* y *baud rate* se utilizan indistintamente, lo cual es incorrecto. *Bit rate* es el número de bits transmitidos durante un segundo. Mientras que *Baud rate* es el número de unidades de señal transmitidas por segundo, cuya función es representar los bits. La razón de esta confusión, es que los primeros módems transmitían un bit por *baud*, es decir, un módem de 1,200 *bauds* transmitía 1,200 bps. Sin embargo con el tiempo, fue necesario transmitir a una tasa mayor de bits, por lo que se diseñaron técnicas para "empaquetar", tantos bits como fuera posible, en un *baud*. La relación entre bits y bauds se muestra en la siguiente formula:

Bit rate = *Baud rate* * el número de bits por *baud*

Ancho de banda

La tasa de datos que un enlace puede transferir depende del tipo de codificación utilizada, de la duración de la señal, del tamaño de los voltajes utilizados, y de las propiedades físicas del medio de transmisión, siendo este último el que impone las mayores limitaciones. Una forma de incrementar la velocidad de transmisión de datos es incrementar la velocidad (frecuencia) de la señal portadora. Teóricamente, la frecuencia de una señal es directamente proporcional a la tasa de datos. Pero el incrementar la frecuencia de la señal significa incrementar el número de cambios por segundo (*baud*), y cada línea tiene imitaciones inherentes al número de cambios que puede soportar (de hecho el *baud rate* determina el ancho de banda requerido para enviar una señal). En otras palabras, cada línea, basada en sus características eléctricas, puede aceptar sólo un cierto rango de cambios de señal por segundo. Si la señal es muy lenta, no podrá vencer la capacitancia de la línea, y si por el

contrario, es muy rápida, puede ser frenada por la inductancia de la línea. Esto significa que cada línea tiene un límite inferior y uno superior respecto a la frecuencia de las señales que puede transportar. Este rango delimitador es llamado ancho de banda.

Las líneas telefónicas tradicionales pueden transportar señales con frecuencias entre 300 Hz y 3,300 Hz., ofreciendo un ancho de banda de 3,000 Hz. Todo este rango es utilizado para transmitir voz, donde se pueden dar un gran número de interferencias y distorsiones sin dejar de ser comprensible. En cambio, las señales de datos requieren un mayor grado de precisión para asegurar la integridad de la información. Por lo tanto, las fronteras de estos rangos no se utilizan para la comunicación de datos. En general, podemos decir que el ancho de banda de la señal debe ser menor que el ancho de banda del cable. El ancho de banda efectivo de una línea telefónica utilizada para la transmisión de datos es de 2,400 Hz. cubriendo el rango que va desde 600 Hz. a 3,000 Hz. Es importante resaltar que, hoy en día, algunas líneas telefónicas son capaces de manejar un ancho de banda mayor que el de las líneas tradicionales. Sin embargo, el diseño de los módems aún se basa en la capacidad tradicional.

Velocidad del módem.

Todos los mecanismos de codificación digital-analógica manipulan la señal en diferente forma: ASK manipula la amplitud; FSK manipula la frecuencia; PSK manipula la fase; y QAM manipula fase y amplitud.

El ancho de banda requerido por la transmisión ASK es igual a la tasa de *bauds* de la señal. Asumiendo que el enlace entero es utilizado por una señal, como pudiera ser el caso de una transmisión *simplex* o *half-duplex*, la máxima tasa de *baud* para una codificación ASK es igual a todo el ancho de banda del medio de transmisión. Debido a que el ancho de banda efectivo de una línea telefónica es de 2,400 Hz., la máxima tasa de *baud* es también 2,400. Y, ya que la tasa de transmisión de *baud* y bits es la misma en la codificación ASK, la máxima tasa de transmisión de bits es también de 2,400.

En la transmisión en modo *full-duplex*, sólo la mitad del total del ancho de banda puede ser utilizado en cualquiera de las dos direcciones. Por lo tanto, la máxima velocidad para una transmisión ASK en modo *full-duplex* es 1,200 bps. Aunque ASK es el más popular de los tipos de codificación, los problemas de ruido hacen impráctico que se utilice en módems.

Por su parte, el ancho de banda requerido por la transmisión FSK es igual a la tasa de transferencia de *baud* de la señal más el desplazamiento de la frecuencia. Asumiendo que todo un enlace está siendo utilizado por una señal, como pudiera ser el caso de la transmisión *simplex* o *half-duplex*, la máxima velocidad de *baud* para una codificación FSK es igual a todo el ancho de banda del medio de transmisión menos el desplazamiento de la frecuencia. Debido a que el ancho de banda efectivo de una línea telefónica es de 2,400 Hz, la máxima velocidad de *baud* es por lo tanto 2,400 menos el desplazamiento de la frecuencia. Y ya que, la velocidad de *baud* y bits es la misma en la codificación FSK, la máxima velocidad de bits es también 2400 menos el desplazamiento de la frecuencia.

Para la transmisión *full-duplex*, sólo la mitad del total del ancho de banda del enlace puede ser utilizado en cualquiera de las dos direcciones. Por lo tanto, la velocidad teórica máxima para FSK en modo *full-duplex* es la mitad del total del ancho de banda menos la mitad del desplazamiento de la frecuencia.

Finalmente, el mínimo ancho de banda requerido por la transmisión PSK o QAM es el mismo que el requerido por la transmisión ASK pero la velocidad de transmisión de bits puede ser mayor en función del número de bits que pueden ser representados por cada pulso.

La tabla 7.1 resume la tasa máxima de transmisión de bits sobre líneas telefónicas convencionales para cada uno de los mecanismos de codificación citados arriba. Si se utilizaran 4 hilos de cobre en lugar de 2, la tasa de datos para la transmisión en modo *full-duplex* podría duplicarse. En dado caso, 2 alambres se utilizarían para la transmisión y 2 para la recepción de datos, duplicando el ancho de banda disponible. Es importante aclarar que, estas cantidades son teóricas y no siempre se pueden alcanzar con la tecnología actual.

Tabla 7.1. Velocidad de transmisión de bits teórica para módems

Codificación	Bits/baud	Bit rate	
		Half-duplex	Full-duplex
ASK, FSK, 2-PSK	1	2400	1200
4-PSK, 4-QAM	2	4800	2400
8-PSK, 8-QAM	3	7200	3600
16-QAM	4	9600	4800
32-QAM	5	12000	6000
64-QAM	6	14400	7200
128-QAM	7	16800	8400
256-QAM	8	19200	9600

Dirección downstream y upstream

Desde el punto de vista del usuario de cualquier red de datos, la transferencia de información entre su computadora, conectada a la red, y la misma red es bidireccional. La transferencia de datos que se lleva a cabo desde la red, por ejemplo Internet, hacia la computadora del usuario es llamada *downstream*. Mientras que la que se realiza desde la computadora del usuario (conectado a la red) hacia la propia red es llamada *upstream*.

Estándares de módem

Los principales estándares de módems son: los desarrollados por Bell y los de ITU-T.

Módems Bell

El primer módem comercial fue producido por la compañía telefónica Bell a principio de los 1970s. Como el primer, y por mucho tiempo, único fabricante en el mercado, Bell desarrolló la tecnología y proveyó un estándar de facto que subsecuentes fabricantes han utilizado para sus propios diseños. Hoy día existen docenas de compañías produciendo cientos de diferentes tipos de módems por todo el mundo. La Tabla 7.2 muestra las características de las principales series de módems desarrolladas por Bell.

Tabla 7.2. Principales módems desarrollados por Bell.

103/113	FDX	1 par de cobre	Asíncrona	FSK	300	300	V.21
202	HDX	1 par de cobre	Asíncrona	FSK	1200	1200	V.23
212	FDX	1 par de cobre	Asíncrona	FSK	300	300	V.22
			Asíncrona/Síncrona	4-PSK	600	1200	
201	HDX	1 par de cobre	Síncrona	4-PSK	1200	2400	V.26
	FDX	2 pares de cobre					
208	FDX	2 pares de cobre	Síncrona	8-PSK	1600	4800	V.27
209	FDX	2 pares de cobre	Síncrona	16-QAM	2400	9600	V.29

Nomenclatura:
FDX Full-duplex
HDX Half-duplex

Módems ITU-T

Hoy día, la mayoría de los módems disponibles en el mercado se basan en estándares de la ITU-T. La ITU-T, además de contar con estándares compatibles con las series de módems Bell (ver tabla 7.2), también ha desarrollado otros estándares, cuyas características se muestran en la Tabla 7.3.

Tabla 7.3. Principales estándares desarrollados por ITU-T.

Estándar	Modo	Medio	Codificación	Velocidad		Comentarios
V.22bis	FDX	1 par de cobre	4-PSK 16-QAM	600	1200 2400	El término *bis* indica que este módem es la segunda generación de la serie.
V.32	FDX	1 par de cobre	32-QAM	2400	9600	5 bits/baud. 4 bits de datos y uno redundante.
V.32bis	FDX	2 pares de cobre	64-QAM	2400	14,400	Primer estándar de módem con una velocidad de 14,400 bps.
V.32terbo	FDX	2 pares de cobre	256-QAM	2400	19,200	El término *terbo* indica que este modem es la tercera generación de la serie.
V.33	FDX	2 pares de cobre	128-QAM	2400	14,400	7 bits/baud. 6 bits de datos y uno redundante.
V.34	FDX	2 pares de cobre	4096-QAM	2400	28,800	12 bits/baud. Velocidad estándar 28,800 bps, pero con compresión de datos puede alcanzar velocidades tres veces mayores.
V.34bis	FDX	2 pares de cobre	16,384-QAM	2400	33,600	14 bits/baud.
V.42	FDX	2 pares de cobre	4096-QAM	2400	28,800	12 bits/baud. A pesar de que maneja la misma velocidad que V.34, es más confiable en virtud de que cuenta con funciones para corrección de errores.

Módems inteligentes

El propósito de un módem es modular y demodular una señal. Sin embargo, muchos de los módems actuales hacen mucho más. En particular una clase de módems llamados módems inteligentes que contienen *software* para soportar un gran número de funciones adicionales, como marcación y contestación automática.

Hayes Microcomputers Products, Inc., fue el primero en introducir al mercado este tipo de módems. Las instrucciones en los módems *Hayes* y compatibles-*Hayes* son conocidas como comandos AT. El formato de los comandos AT es:

Comando AT [parámetro] comando [parámetro]...

Cada comando empieza con las letras AT seguido por uno o más comandos, cada uno de los cuales puede requerir uno o varios parámetros.

Módems 56Kbps (V.90, V.92)

Los estándares tradicionales asumen que en ambos extremos de una sesión entre módems, la conexión hacia la red telefónica pública es analógica. Esto implica que en cada uno de dichos extremos, se lleva a cabo la codificación de señales digitales a analógicas y viceversa, limitando la velocidad de transmisión a 33.6Kbps, como ocurre con los módems V.34.

La tecnología V.90, en cambio, parte de un supuesto diferente: asume que, en virtud de que uno de los extremos de una sesión entre módems contará con una conexión digital pura hacia la red telefónica, es posible tomar ventaja de la velocidad ofrecida por la porción digital del trayecto (el supuesto de un sólo segmento analógico es valido en la mayoría de los casos, ya que más del 80% de los ISP's y de las Empresas Corporativas están conectados a la red en forma digital).

Es este sentido, podemos considerar que el trayecto entre dos módems está compuesto por una porción digital que corre a 64Kbps y otra analógica, que va desde las premisas del usuario hasta su central telefónica local, en donde el flujo de datos es "estrangulado" a 33.6Kbps. La Fig. 7.10 ilustra esta situación.

Con base en lo anterior, V.90 también conocido como V.PCM (*Pulse Coded Modulation*), utiliza un método de transferencia de datos asimétrico, a fin de aprovechar las ventajas que ofrece la porción digital del trayecto en dirección downstream.

En la transferencia con dirección downstream, la información es codificada en forma digital, en lugar de modulada como lo hacen los módems analógicos, y enviada a través de la porción digital del trayecto hasta alcanzar la central local a la cual está conectado el módem. En este punto, la central telefónica convierte, por medio de un codificador D-A (*PCM, Pulse Coded Modulation*), la información digital en una señal analógica, enviándola a su destino a través del par trenzado. Este proceso acelera la transferencia de datos y permite alcanzar una velocidad de 56Kbps*.

La transmisión en dirección *upstream*, por su parte, se lleva a cabo mediante la codificación de la información digital a analógica conforme al estándar V.34, alcanzando velocidades de hasta 33.6Kbps.

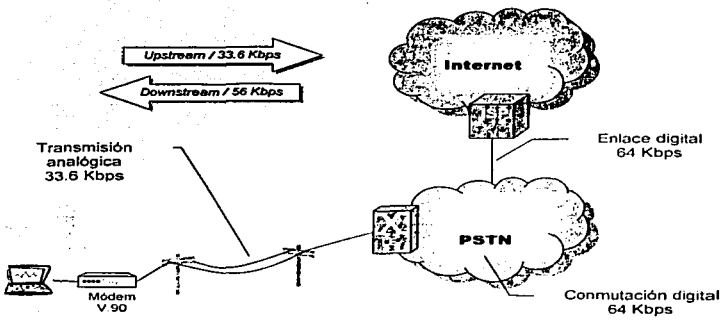


Figura 7.10. Configuración de red en la cual se basó la ITU-T para desarrollar el estándar V.90.

La tecnología V.90 es ideal para usuarios de Internet, ya que generalmente se requiere una mayor velocidad (56Kbps*) en *downstream* para acceder a páginas Web con sonido, video y otros archivos grandes, y otra mucho menor (fácilmente satisfecha con 33.6Kbps) en dirección upstream, para la transmisión de escritura vía teclado o comandos del *mouse*.

Además de V.90, existe otro estándar llamado V.92, que hace uso del esquema PCM en ambas direcciones, consiguiendo soportar velocidades de 48Kbps en dirección upstream y 56Kbps* en downstream.

NOTA: Los módems pueden recibir datos a velocidades mayores de 56Kbps sin embargo debido a especificaciones de la FCC (Comisión Federal de Comunicaciones), enfocadas a minimizar el efecto de interferencia telefónica entre líneas adyacentes, el nivel de potencia de transmisión máximo permitido en downstream es de 54Kbps. Además, las velocidades de recepción también varían en función de las condiciones de la línea.

Conclusiones

Una *internetwork* consiste en un grupo de redes interconectadas que actúan como un todo coordinado. La mayor ventaja de una internetwork es que proporciona interconexión universal y permite que grupos individuales utilicen cualquier hardware de red que satisfaga sus necesidades.

Los dispositivos que participan en la interconexión de redes, tienen una responsabilidad específica en función de las entidades que interconectan y del servicio que dichas entidades esperan de ellos. A excepción de los repetidores que por su limitada función prácticamente no son utilizados, los otros dispositivos de red que se revisaron en este documento, forman parte de las redes de datos actuales, cumpliendo, cada uno de ellos, con una función única y complementaria al resto.

Es importante resaltar que todos y cada uno de dichos dispositivos surgieron en respuesta de alguna necesidad ocurrida durante el proceso de evolución de las redes, proceso que evidentemente no ha terminado ni terminará y que en la medida en que las aplicaciones y los servicios, que demandan los usuarios, continúen evolucionando, las características de aquellos también evolucionarán. Esto provoca que los límites de las funciones y capacidades de que cada uno de los dispositivos no sean claras ni estáticas, apareciendo dispositivos "híbridos" como los *brouters* (*bridge-router*), que realizan funciones de puente y de ruteador.

Los dispositivos más comúnmente utilizados para la transmisión en las redes de datos son:

- Módems.
- Repetidores y Concentradores.
- Puentes.
- Ruteadores.
- Conmutadores.
- Pasarelas.

Los módems son los dispositivos responsables de convertir señales digitales a analógicas y viceversa. El término módem es una palabra compuesta que hace mención a las dos entidades funcionales que lo conforman: un modulador y un demulador de señal. Los mecanismos de codificación digital-analógica que se utilizan para manipular la señal son ASK, FSK, PSK y QAM, siendo este último el más popular y poderoso, ya que manipula tanto la fase como la amplitud de la señal. Además de esto, y con base en el aprovechamiento de las ventajas que ofrecen los tramos digitales de gran parte de las trayectorias de comunicación, surgió la tecnología V.90, la cual permite manejar una velocidad de 56Kbps en dirección *downstream* y 33.6Kbps en *upstream*.

Los repetidores no son más que dispositivos eléctricos que extienden la distancia máxima que puede alcanzar un cable de LAN, amplificando las señales que pasan por ellos. Los concentradores por su parte son una especie de repetidores multipuerto, aunque con muchas otras características que les permiten tener vigencia en las redes actuales. Tal es el caso de

los MAU, Unidades de Acceso Multipuerto utilizados en las redes Token Ring o de los concentradores inteligentes que permiten ser supervisados y gestionados de forma elemental. Usar un repetidor o un concentrador para expandir un segmento de red no la divide en dos LAN ni crea una interconexión de redes.

Los puentes proporcionan, además de la función de amplificación de un repetidor o un concentrador, la posibilidad de filtrar selectivamente paquetes basándose en su dirección. Los paquetes que se originan a un lado del puente, se propagan al otro lado solamente si están dirigidos a un sistema de ese otro lado. Como los puentes no impiden que los mensajes de multidifusión se propaguen a lo largo de los segmentos del cable conectados al puente, tampoco crean múltiples LAN ni transforman una red en una interconexión de redes.

Los ruteadores son dispositivos que conectan dos LAN para formar una interconexión de redes. Al igual que un puente, un ruteador solamente transmite el tráfico al segmento al que está destinado, pero, a diferencia de los concentradores y los puentes, los ruteadores no transmiten mensajes de multidifusión. Los ruteadores también pueden conectar diferentes tipos de redes entre sí, como Ethernet y Token Ring, mientras que los puentes y los concentradores solamente pueden conectar segmentos del mismo tipo.

Los conmutadores son dispositivos revolucionarios que, en muchos casos, eliminan completamente el medio de transmisión compartido. Un conmutador es esencialmente un repetidor multipuerto, o concentrador, excepto que en lugar de funcionar en el nivel puramente eléctrico, el conmutador lee la dirección de destino de cada paquete entrante y la transmite exclusivamente al puerto al que está conectado el sistema destino.

Las pasarelas son los más complejos y poderosos de todos los dispositivos utilizados para la transmisión e interconexión de redes. Ofrecen la posibilidad de interconectar redes diametralmente opuestas, tanto a nivel protocolo y arquitectura como a nivel eléctrico y físico. Tal es el caso de la interconexión de redes de conmutación de circuitos con redes de conmutación de paquetes o celdas.

Entre las principales ventajas y desventajas ofrecidas por las redes conmutadas y las enrutadas, encontramos que la conmutación es más rápida y barata que el enrutamiento, pero origina ciertos problemas en la mayoría de las configuraciones de red. Una red conmutada permite que dos sistemas cualesquiera puedan comunicarse utilizando un enlace dedicado. El problema aparece cuando las estaciones de trabajo generan mensajes de difusión. En virtud de que una red conmutada forma un único dominio de difusión, los mensajes de difusión se propagan por toda la red y todos los sistemas deben procesarlos, lo que puede consumir una gran cantidad de ancho de banda. Por su parte, los ruteadores permiten crear varias LAN consiguiendo que las difusiones se limiten a las redes individuales. Sin embargo, han surgido nuevas tecnologías que integran el enrutamiento y la conmutación en diversos grados, para evitar el consumo de ancho de banda ocasionado por las difusiones. La conmutación de nivel 3 mezcla las funciones de enrutamiento y conmutación para que las comunicaciones entre redes LAN virtuales sean más eficientes. La esencia del concepto se puede definir como *enruta primero, conmuta después*. Sigue siendo necesario un ruteador para establecer las conexiones entre los sistemas de LAN

virtuales diferentes, pero una vez establecida la conexión, el tráfico posterior viaja sobre la conmutación del nivel 2, que es mucho más rápida.

Además de las diferencias en precio y en tecnología citadas, existen otras ventajas intangibles, pero igualmente importantes, que pueden influir en el criterio de compra de los Clientes al decidirse por alguna de estas soluciones. Se trata de la fuerza de la marca y la estrategia de comercialización, que en este caso se traduce en bajos costos de mantenimiento y baja o nula dependencia de personal altamente especializado. A que me refiero, Cisco, inventor/creador de los ruteadores, ha establecido un "estándar" en el mercado. Ha puesto al alcance de todo el mundo la información técnica necesaria para diseñar y configurar las redes con su equipo; por el otro lado tenemos a las empresas que mantienen bajo siete llaves gran parte de su información técnica por considerarla "confidencial". Esta estrategia de comercialización, ha colocado a Cisco en una posición muy ventajosa, no sólo frente al resto de los fabricantes de ruteadores, que dicho sea de paso, basan sus diseños en especificaciones Cisco, sino que también sobre los fabricantes de productos sustitutos como es el caso de los conmutadores. Tal vez exagere, pero en muy poco tiempo, sino es que ya, cualquier persona interesada en el tema podrá instalar, configurar y operar un ruteador Cisco sin mayor problema, y en caso de no saberlo bastará con comprar un libro en *Sanborns* para aprender como se hace.

Esto no es un asunto solamente de tecnología, es fundamentalmente un asunto de dinero, de negocios, de estrategia. Como hacer para que el mercado adquiera mis soluciones a pesar de ser más costosas que algunos productos sustitutos? La respuesta está en el tiempo. Si el día de hoy adquiero un ruteador, me representará una mayor inversión que si se tratara de un conmutador, pero a mediano y largo plazo las cuentas podrían nivelarse o incluso invertirse. Pensemos, por ejemplo, en los costos de operación y mantenimiento. En el caso de los conmutadores es muy probable que tengamos que depender del proveedor o de personal propio altamente especializado. En el caso de los ruteadores, como ya se comentó, la información está al alcance de todo aquel interesado en el tema, situación que se ha traducido en la generación de un gran número de técnicos calificados que se traduce en un abaratamiento de la mano de obra. Lo mismo pasaría en el caso del diseño o ampliación de una red, por un lado tendríamos un grupo de costosos especialistas conocedores de una tecnología propietaria y por el otro un grupo de especialistas conocedores de una tecnología "estándar" en el mercado.

Finalmente, refiriéndonos a la convergencia de las redes, es innegable que las pasarelas juegan un papel preponderante, y en un sentido más amplio, el concepto de plataformas abiertas es la característica por excelencia que deberán tener todos los nuevos desarrollos tecnológicos. En la medida en que las especificaciones de los protocolos de comunicación y control de los dispositivos se homologuen, en esa medida se facilitará y acelerará la integración de redes con diferentes arquitecturas, protocolos, etc.

Términos y acrónimos

ADSL	Asymmetrical digital subscriber line
AIEE	American institute of electrical engineers
AMR	Adaptive multi rate
API	Application program interface
ARB	All rings broadcast
ARP	Address resolution protocol
AS	Autonomous system
ASCII	American standard code for information interchange
ASIC	Application-specific integrated circuit
ASK	Amplitude shift keying
ATM	Asynchronous transfer mode
AUI	Attachment unit interface
Backbone	Red de soporte
Backplane	Bus interno de comunicación
Baud	unidad de señal (pulso)
BGP	Border gateway protocol
BGP-4	Border gateway protocol, version 4 (RFC 1771)
BIA	Burned-in address
BICC	Bearer-independent call control
BIS	Boundary intermediate system
Bit rate	Número de bits transmitidos por segundo
BITS	Building integrated timing system
BPDU	Bridge protocol data units
CCITT	Committee consultative for international telephone and telegraph (currently the ITU).
CDMA	Code-division multiple access
CORBA	Common object request broker architecture
CRC	Cyclic redundancy check
CSMA/CD	Carrier sense multiple access with collision detection
DCE	Data circuit-terminating equipment
DFT	Distributed function terminal
DHCP	Dynamic host configuration protocol
DNS	Domain name system
Downstream	Transferencia de datos desde la red hacia la computadora del usuario
DS3	Digital signal, level 3 (44.736 Mbit/s)
DSP	Digital signal processor
DSU	Digital service unit
DTE	Data terminal equipment
DTMF	Dual-tone multifrequency
E1	2 Mbit/s digital link
EGP	Exterior gateway protocol
EIA	Electronic industries association
ES	End system
ET	Exchange terminal
ETR	Early token release
ETSI	European telecommunication standards institute
FCC	Comisión federal de comunicaciones
FCS	Frame check sequence
FDDI	Fiber distributed data interface
Firewall	Producto de seguridad (*software*) para evitar que los intrusos tengan acceso a las redes desde el exterior
FSK	Frequency shift keying
FTP	File transfer protocol

Full duplex	Modo de operación en el cual los datos pueden viajar en ambas direcciones en un momento determinado
Gap	Hueco sin información real
GGSN	Gateway GPRS support node
GIF	Graphics interchange format
GPB	General-purpose board
GPRS	General packet radio service
GSM	Global system for mobile communication
GTP	Gateway tunneling protocol
GTP-C	GTP control
GTP-U	GTP user plane
GUI	Graphical user interface
H.323	ITU-T recommendation on visual telephone systems and equipment for local area networks that provide a non-guaranteed quality of service
Half-duplex	Modo de operación en el cual los datos solo pueden viajar en una dirección en un momento determinado
Header	Encabezado
Hop	Salto
Host	Sistema de computo interfaz de una red
HSS	Home subscriber server
HTML	Hypertext markup language
HTTP	Hypertext transfer protocol
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
ICS	Internet connection sharing
IEEE	Institute of electrical and electronic engineers
IESG	Internet engineering steering group
IETF	Internet engineering task force
IIOP	Internet inter-object request broker protocol
IN	Intelligent network
IP	Internet protocol
IPv4	IP version 4
IPv6	IP version 6
IPX	Internetwork packet exchange
IRE	Institute of radio engineers
IRP	Integrated reference point
IS	Intermediate system
ISDN	Integrated services digital network
ISO	International organization for standardization
ISP	Internet service provider
ITU	International telecommunication union
Jam pattern	Patrón de interferencia
JPEG	Joint photographic experts group
L2TP	Layer 2 tunneling protocol
LAN	Local area network
LAPM	Link access procedure for modems
LER	Label edge router
LLC	Logical link control
LU	Logical unit
MAC	Media access control
Mainframe	Computadora central
MAN	Metropolitan area network
MAU	Multistation access unit
MGCP	Media gateway control protocol
MGW	Media gateway
MIB	Management information base

MNP5	Microcom networking protocol, version 5
MPC	Multiparty call
MPEG	Motion picture experts group
MPLS	Multiprotocol label switching
MPOA	Multiprotocol over ATM
MSAU	Multistation access unit
MSB	Media stream board
MSC	Mobile switching center
MSC	Mobile services switching center
MSF	Multiservice switching forum
MTP	Message transfer part
MTU	Maximum transfer unit
Multihomed	Multi-hospedado
NAS	Network access server
NEBS	Network equipment building system
NFS	Network files system
NIC	Network interface card
NSF	National science foundation
OC3	Optical carrier, 155 Mbit/s link
OSI	Open systems interconnection
OSPF	Open shortest path first
OUI	Organizationally unique identifier
Overhead	Encabezado
PAM	Pulse amplitude modulation
Payload	Carga útil dentro de una celda
PCM	Pulse code modulation
PDP	Packet data protocol
PDU	Protocol data unit
Plug	Enchufe
PPP	Point to point protocol
PRI	Primary rate interface
PSK	Phase shift keying
PSTN	Public switched telephone network
PU	Physical unit
QAM	Quadrature amplitude modulation
QoS	Quality of service
Quad	Número de 8 bits
RARP	Reverse address resolution protocol
Rate	Velocidad de transmisión
RD	Receive data
RD	Route designator
RD	Routing domain
RDSI	Red digital de servicios integrados
RFC	Request for comments
RIF	Routing information field
RII	Route information indicator
RIP	Routing information protocol
RISC	Reduced instruction set computer
RNC	Radio network controller
ROM	Read-only memory
RPC	Remote process calls
RRAS	Routing and remote access server
RTP	Real-time transport protocol
SAP	Service access point
SAP	Service advertising protocol
SCCP	Signaling connection control part

SCP	Session control protocol
SCTP	Stream control transport protocol
SDH	Synchronous digital hierarchy
SDSL	Symmetrical digital subscriber line
SDU	Service data units
SGSN	Serving GPRS support node
Simplex	Equivalente a half-duplex
SIP	Single in-line package
SLIP	Serial line internet protocol
SMDS	Switched multimegabit data service
SMTP	Simple mail transfer protocol
SNMP	Simple network management protocol
SPA	Spanning tree algorithm
SPB	Special-purpose board
SQE	Signal quality error
SRT	Source route transparent
SS7	Signaling system no. 7
STM-1	Synchronous transfer module-1, 155 Mbit/s digital links
STP	Signal transfer point
T1	1.5 Mbit/s digital link
TCP	Transmission control protocol
TD	Transport data
TDM	Time-division multiplexing
Telnet	Servicio de Internet que permite establecer una conexión con otro sistema a través de la red y proporciona acceso a su interfaz de comandos (shell)
TFTP	Transfer files trivial protocol
TIC	Token-ring interface card
TIFF	Tagged Image File Format
Token	Testigo
Trailer	Cola
Troubleshooting	Solución de problemas técnicos
TSC	Transit switching center
TTC	Telecommunication technology committee
TTL	Time-to-live
UDP	User datagram protocol
UMTS	Universal mobile telecommunications system
Uplink	Enlace de subida (puerto)
UPS	Uninterruptible power supply
Upstream	Transferencia de datos desde la computadora del usuario hacia la red
V.100	ITU-T recommendation: Interconnection between public data networks (PDN) and the public switched telephone networks (PSTN)
V.21	ITU-T recommendation: 300 bit/s per duplex modem standardized for use in the general switched telephone network
V.34	ITU-T recommendation: A modem operating at data signaling rates of up to 33,600 bit/s for use on the general switched telephone network and on leased, point-to-point, two-wire telephone-type circuits
V.42bis	ITU-T recommendation: Data compression procedures for data circuit terminating equipment (DCE) using error correction procedures
VoIP	Voice over IP
VPN	Virtual private network
VPSM	Virtual port service manager
WAN	Wide area network
WAN	Wide area network
X.25	ITU-T recommendation: Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and

	connected to public data networks by dedicated circuit xDSL Collective term for several copper circuits-based modem technologies.
XNS	Xerox network services
ZIP	Zone information protocol

Apéndices

Apéndice A

Mecanismos de control de acceso al medio.

Mecanismo MAC de Ethernet

Ethernet es el protocolo del nivel de enlace de datos utilizado por la mayor parte de las redes de área local que operan en al actualidad. El protocolo Ethernet proporciona una interfaz unificada a medio de red que permite a un sistema operativo transmitir y recibir varios protocolos del nivel de red de forma simultánea. Al igual que la mayor parte de los protocolos del nivel de encale de datos que reutilizan en LAN, Ethernet es, en términos técnicos, no orientado a conexión y no fiable. Ethernet realiza todo lo posible para transmitir datos al destino especificado, pero no existe ningún mecanismo que garantice una entrega correcta. En lugar de eso, ciertos servicios, como la entrega garantizada, son responsabilidad de los protocolos que operan en niveles superiores del modelo OSI, si los datos así lo requieren.

Tal como se define el estándar de Ethernet, el protocolo consta de tres componentes esenciales:

- Una serie de directivas del nivel físico que especifican los tipos de cable, limitaciones de cableado y métodos de señalización para las redes Ethernet.
- Un formato de trama que define el orden y las funciones de los bits transmitidos en un paquete Ethernet.
- Un mecanismo de control de acceso al medio (*MAC, Media Access Control*) denominado acceso múltiple con detección de portadora y detección de colisiones (*CSMA-CD, Carrier Sense Multiple Access and Collision Detection*), que permite que todas las computadoras de la LAN dispongan de un acceso similar al medio de red.

CSMA/CD

La propiedad más categórica de una red Ethernet es su mecanismo de control de acceso al medio, denominado *Acceso múltiple con detección de portadora y detección de colisiones (CSMA, Carrier Sense Multiple Access and collision Detection)*. Al igual que cualquier método de MAC, CSMA/CD permite a las computadoras de la red compartir un único medio de banda base sin pérdida de datos. En una red Ethernet no existe prioridades, en lo que se refiere al acceso al medio; el protocolo está diseñado de forma que todos los nodos disponen de los mismos derechos de acceso al medio de red. El proceso por el que CSMA/CD arbitra el acceso al medio de red en una red Ethernet se muestra en la Fig. A.1.

Cuando un nodo de una red Ethernet desea transmitir datos, lo primero que hace es comprobar el medio de red para ver si se está utilizando en ese momento. Ésa es la fase del

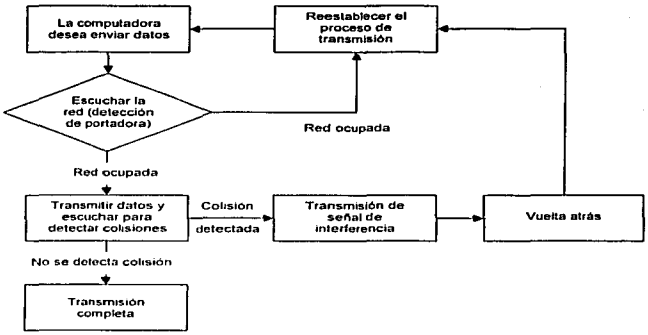


Figura A.1. Mecanismo de control de acceso al medio CSMA/CD.

Proceso de *detección de portadora*. Si el nodo detecta tráfico en la red, espera un momento y vuelve a escuchar la red. Una vez que la red está despejada, cualquiera de los nodos puede utilizarla para transmitir sus datos. Ésa es la fase de *acceso múltiple*. Este mecanismo arbitra por sí mismo el acceso al medio, pero no carece de defectos.

Resulta completamente posible que dos o más sistemas detecten una red despejada y comiencen a transmitir sus datos casi en el mismo momento. Eso ocasiona lo que el estándar 802.3 denomina un *error de calidad de la señal* (*SQE, Signal Quality Error*) o, como suele conocerse habitualmente dicha condición, una *colisión de paquetes*. Las colisiones se presentan cuando un sistema comienza a transmitir sus datos y otro sistema realiza la detección de portadora durante el breve intervalo de tiempo anterior a la llegada del primer bit del paquete transmitido (ver Fig. A.2). Dicho periodo de tiempo se conoce con el nombre de *intervalo de contienda* (*contention time o spot time*), ya que todos los sistemas implicados creen que han comenzado a transmitir en primer lugar. Por tanto, cada uno de los nodos de la red se encuentra siempre en uno de tres estados posibles: transmisión, contienda o inactivo.

Figura A.2. El nodo A ha comenzado a transmitir sus datos, pero puesto que el principio del paquete aún no ha llegado al nodo B, el nodo B tiene la sensación de que la red está desocupada. Si el nodo B comienza a transmitir en ese momento, se producirá una colisión.

Cuando los paquetes de dos nodos diferentes colisionan se crea una condición anómala en el cable que se propaga hacia ambos sistemas. En una red coaxial, el nivel de voltaje aumenta hasta un punto en que es igual o mayor que los niveles combinados de los dos transmisores (+/- 0.85v). En una red de pares trenzados o fibra óptica, la anomalía toma la forma de actividad de señal en los circuitos de transmisión y recepción al mismo tiempo.

Cuando uno de los sistemas transmisores detecta la anomalía, reconoce que se ha producido una colisión, deja de enviar datos inmediatamente y comienza a realizar las acciones necesarias para corregir el problema. Ésta es la fase de *detección de colisiones* del proceso. Puesto que los paquetes que colisionan se consideran inservibles, ambos sistemas transmiten un *patrón de interferencia (jam pattern)* que extiende el voltaje por todo el cable, informando de la colisión al resto de los sistemas de la red y evitando que inicien sus propias transmisiones.

El patrón de interferencia es una secuencia de 32 bits que puede tener cualquier valor, siempre que no sea igual al valor del cálculo de la comprobación de redundancia cíclica (*CRC, Cyclical Redundancy Check*) del campo de comprobación de secuencia de trama (*FCS, Frame Check Sequence*) del paquete dañado. Un sistema que recibe un paquete Ethernet utiliza el campo FCS para determinar si los datos del paquete se han recibido sin errores. Puesto que el patrón de interferencia es diferente al valor de CRC correcto, todos los nodos receptores descartarán el paquete.

Después de transmitir el patrón de interferencia, los nodos implicados en la colisión vuelven a programar sus transmisiones, utilizando un tiempo de espera aleatorio que calculan con un algoritmo que utiliza su dirección MAC como único factor. Este proceso se denomina *vuelta atrás (backing off)*. Puesto que ambos nodos realizan sus cálculos de vuelta atrás de forma independiente, la probabilidad de que vuelvan a transmitir a la vez disminuye de forma sustancial. Sin embargo, existe la posibilidad de que lo hagan, y si se produce otra colisión entre los mismos nodos, ambos aumentan la longitud posible de los intervalos de espera y vuelven a empezar de nuevo. A medida que aumenta el número de valores posibles para el intervalo de vuelta atrás, la probabilidad de que los sistemas vuelvan a seleccionar el mismo intervalo disminuye. Un sistema Ethernet tratará de transmitir un paquete hasta 16 veces, y si siempre se produce una colisión, descartará el paquete.

La mayor parte de las colisiones que se producen en una red Ethernet típica se resuelven en microsegundos. Lo más importante que hay que entender en lo que se refiere al arbitraje de medios Ethernet es que las colisiones de paquetes son comportamientos naturales y esperados en este tipo de redes, y esto no significa, necesariamente, que exista un problema. Si se utiliza un analizador de protocolos o cualquier otra herramienta de supervisión de red para analizar el tráfico en una red Ethernet, se puede ver que siempre se produce un cierto número de colisiones.

Mecanismo MAC de Token Ring

Token Ring es la alternativa tradicional al protocolo Ethernet en el nivel de enlace de datos. IBM fue el desarrollador original de este protocolo y, posteriormente, se normalizó en el documento 802.5 del IEEE.

La mayor diferencia entre Token Ring y Ethernet radica en el mecanismo de control de acceso al medio. Para transmitir sus datos, una estación de trabajo debe ser portadora del *testigo* (*token*), un paquete especial que circula, por turnos, entre todos los nodos de la red. Solamente el sistema que posee el testigo puede transmitir, después de lo cual pasa el testigo al siguiente sistema. Esto elimina toda posibilidad de que se produzcan colisiones en una red que funcione correctamente, así como la necesidad de un mecanismo de detección de colisiones.

Definición de Token Ring

Como su nombre lo indica, los nodos de una red Token Ring se conectan en una topología de anillo. Esto es, en esencia, un bus con los dos extremos conectados entre sí, de forma que los sistemas pueden pasar datos al siguiente nodo de la red hasta que vuelven de nuevo al origen. Así es, exactamente, como funciona el protocolo: el sistema que transmite un paquete también es responsable de eliminarlo de la red una vez que recorre el anillo.

Sin embargo, este anillo es lógico, no físico. Esto es, la red tiene la apariencia de una topología en estrella, con las estaciones de trabajo conectadas a un concentrador central denominado *unidad de acceso multi-estación (MAU* o, a veces, *MSAU, Multistation Access Unit)*. El anillo lógico es, en realidad, responsabilidad del MAU, el cual acepta los paquetes transmitidos por un sistema y los dirige, por turno, a cada puerto sucesivo, esperando que vuelvan por el mismo cable antes de proseguir con el siguiente puerto (ver Fig. A.3).

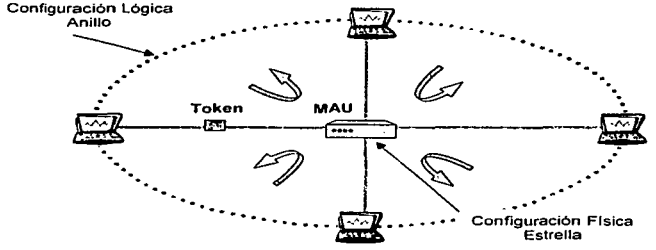


Figura A.3. Las redes Token Ring utilizan una topología lógica en anillo que opera sobre una topología física en estrella.

En esta disposición, por tanto, el circuito transmisor y receptor de cada una de las estaciones de trabajo son, en realidad, puertos diferentes que utilizan el mismo cable, ya que los sistemas siempre transmiten datos al siguiente sistema de la cadena y reciben datos del anterior.

Paso de testigo

El acceso al medio de red de una red Token Ring se arbitra utilizando un paquete de 3 bytes denominado *testigo (token)*. Cuando la red está inactiva, se dice que las estaciones de trabajo se encuentran en *modo de repetición de bit*, esperando una transmisión entrante. El testigo circula de forma continua por el anillo, de nodo a nodo, hasta que llega a una estación de trabajo que desea transmitir datos. Para transmitir datos, la estación de trabajo modifica un único *bit monitor* en el testigo para indicar que la red está ocupada y lo envía a la siguiente estación de trabajo, seguido inmediatamente de su paquete de datos.

El paquete también circula por el anillo. Cuando uno de los nodos lee la dirección destino de la cabecera de trama del paquete y o bien copia el paquete en sus búferes de memoria para procesarlo antes de transmitirlo al nodo siguiente, o bien sólo lo transmite sin procesarlo. De esta forma, los paquetes pasan por todos los nodos de la red hasta que llegan de nuevo a al estación de trabajo que los envió originalmente.

Al recibir el paquete una vez que ha recorrido el anillo, el nodo emisor compara los datos que llegan con los transmitidos originalmente para comprobar si se ha producido algún error durante la transmisión. Si se ha producido algún error, la computadora retransmite el paquete. Si no se ha producido ningún error, la computadora elimina el paquete de la red y lo descarta, modifica el bit monitor del testigo para que refleje de nuevo el estado libre y lo transmite. Así se repite el proceso de forma que todos los sistemas tienen la misma posibilidad de transmitir.

Aunque no formaba parte del estándar original, la mayor parte de los sistemas Token Ring de 16 Mbps actuales incluyen una característica denominada *liberación rápida del testigo (ETR, Early Token Release)*, que permite al sistema emisor enviar al testigo "libre" inmediatamente después del paquete de datos, en lugar del testigo "ocupado" antes del paquete de datos, sin tener que esperar a que los datos recorran la red. De esta forma, el siguiente nodo de la red puede recibir el paquete de datos, captura el testigo libre y transmite su propio paquete de datos, seguido por otro testigo libre. Esto permite que existan varios paquetes de datos en la red de forma simultánea, pero sólo un testigo. La liberación rápida del testigo elimina algunos de los retardos por latencia que se producen en la red mientras los sistemas esperan a que llegue un testigo libre.

Puesto que sólo la computadora que tiene el testigo en su poder puede transmitir datos, las redes Token Ring no sufren colisiones a menos que se produzca un mal funcionamiento grave. Esto significa que la red puede trabajar en plena capacidad sin degradación del rendimiento, al contrario de las redes Ethernet. El sistema de paso de testigo también es determinista, lo que significa que se puede calcular el intervalo máximo de tiempo que transcurre antes de que un nodo determinado pueda transmitir.

Token Ring no es el único protocolo del nivel de enlace de datos que utiliza el paso de testigo como método de control de acceso al medio. FDDI *(Fiber Distributed Data Interface)* también utiliza el paso de testigo. La característica opcional de liberación rápida del testigo en una red Token Ring, es estándar en una red FDDI. Además, los sistemas FDDI también pueden transmitir varios paquetes antes de entregar el testigo a la siguiente estación. Cuando un paquete ha recorrido todo el anillo y ha vuelto al sistema que lo creó originalmente, dicho sistema retira el testigo del anillo para evitar que circule indefinidamente.

Apéndice B

Redes de soporte.

Una red de soporte o troncal no es más que una red encargada de conectar entre sí otras redes, formando lo que se denomina una interconexión de redes. Los segmentos pueden ser redes que den servicio a grupos de trabajo, departamentos, plantas de un edificio, o incluso edificios enteros. Cada uno de los segmentos estará conectado a una red troncal mediante un ruteador o un conmutador, o incluso con un concentrador, como se muestra en la Fig. B.1. Esto permite que la estación de trabajo de una de las redes puedan comunicarse con cualquiera otra estación de trabajo.

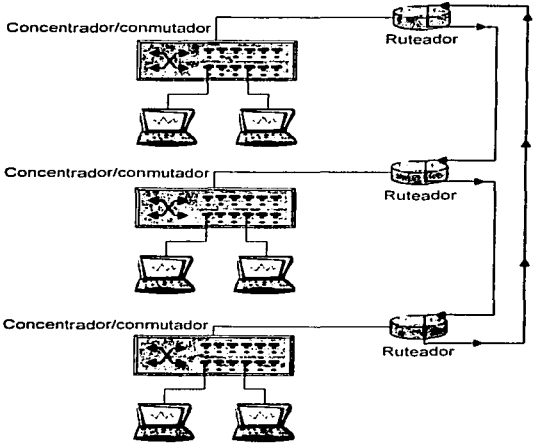


Figura B.1. Una red empresarial consiste de múltiples redes LAN interconectas mediante una red troncal.

Una de las configuraciones más comunes para la interconexión de redes que englobe un edificio entero de varias plantas consiste en tener una LAN independiente encargada de conectar todos los equipos que existen en cada planta (éste es el origen del término "red

horizontal") y una red troncal vertical que conecte entre sí todas y cada una de las LAN de cada planta. Evidentemente, la configuración utilizada dependerá del edificio en el cual se instale la interconexión de redes. Si una gran compañía se aloja en un enorme edificio de sólo dos plantas, probablemente será necesario instalar varias LAN en cada planta y unirlas todas a través de una red troncal que abarque todo el edificio.

Cuando dos equipos de la misma LAN se comunican entre sí, el tráfico generado permanece en la red de área local. Sin embargo, cuando los equipos que se comunican pertenecen a LAN diferentes, el tráfico generado pasa a través del ruteador conectando el equipo de origen con la red troncal, y ésta a su vez con la LAN en la cual se encuentra el equipo de destino. Es también una práctica común conectar todos los recursos de red utilizados por los usuarios directamente a la red troncal, en lugar de hacerlo a redes horizontales. Por ejemplo, si se dispone de un único servidor de correo electrónico para toda la compañía, conectarlo a una de las redes horizontales obligará a que todo el tráfico generado por los clientes del servicio de correo electrónico de toda la compañía viaje hacia ese segmento, posiblemente sobrecargándolo.

Como la red troncal es compartida por todos los segmentos horizontales, cursa todo el tráfico de red que genera cada uno de los equipos de cada LAN. Ello supone una gran carga de tráfico, razón por la que la red troncal funciona a velocidades superiores a las de las redes horizontales. La red troncal puede tener que cubrir mayores distancias que las de las redes horizontales, por lo que usualmente se utiliza fibra óptica para su construcción.

Tipos de redes troncales

Generalmente se utilizan dos tipos de redes troncales: la red troncal distribuida y la red troncal colapsada. En una red troncal distribuida, la red troncal tiene la forma de un segmento de cable que recorre toda la empresa y que se conecta a cada una de las redes horizontales mediante un ruteador o un conmutador. En una red troncal colapsada, el concentrador de cada una de las redes horizontales se conecta a un ruteador modular centralizado o un conmutador (ver Fig. B.2). Este ruteador o este conmutador funciona como una red troncal para el conjunto de la interconexión de redes, permitiendo el paso del tráfico generado por las redes horizontales. Este tipo de red troncal no utiliza segmentos de cables adicionales, ya que el ruteador/conmutador central tiene módulos individuales para cada una de las redes conectados internamente en una tarjeta posterior. La tarjeta posterior (*backplane*) es un bus interno de comunicación que sustituye el segmento de cable troncal en una red troncal distribuida.

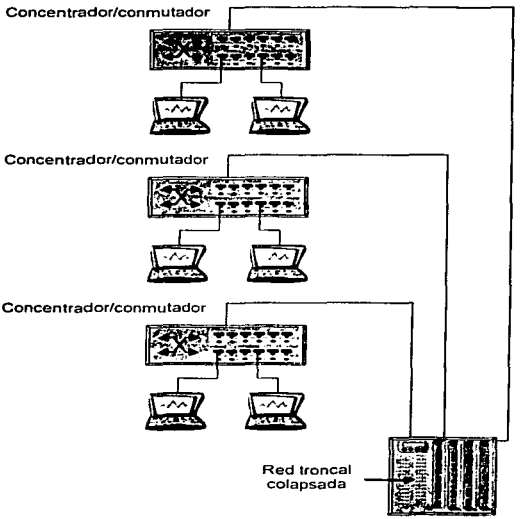


Figura B.2. Una red troncal colapsada conecta todas las LAN a un único ruteador o conmutador.

La ventaja de una red troncal colapsada está en que el tráfico de la internetwork sólo tiene que atravesar un ruteador de camino a su destino, a diferencia de una red troncal distribuida, en la que existen diferentes ruteadores conectando cada red a al red troncal. El inconveniente de una red troncal colapsada es que el concentrador de cada red debe conectarse al ruteador central con un segmento de cable. Dependiendo de la disposición del lugar y de la localización del ruteador, esta distancia puede ser demasiado larga para utilizar cable de cobre.

Una red troncal colapsada no necesita protocolo propio, ya que no utiliza un segmento de cable distinto para interconectar las redes horizontales. La tecnología Fast Ethernet actual ha convertido a la red troncal colapsada en una solución práctica. Sin embargo, existen miles de redes que todavía funcionan a 10 Mbps Ethernet u otros protocolos relativamente lentos en redes horizontales, y que no pueden adaptarse fácilmente al concepto de red troncal colapsada. En esos casos, es necesario utilizar una red troncal distribuida.

Tolerancia a fallos

La red troncal es una parte vital del diseño de una red, ya que es el soporte de todas las comunicaciones entre redes horizontales. Una red horizontal que no pueda acceder a la red troncal estará aislada. Los equipos de esa LAN podrán comunicarse entre sí, pero no con los equipos de otra LAN, lo que puede privarles de servicios vitales de red. Para asegurar el acceso permanente a la red troncal, algunos diseños de interconexión de redes duplican elementos dentro de un plan de actuación frente a fallos. Se puede, por ejemplo, utilizar dos ruteadores en cada LAN, ambos conectados al concentrador de la red troncal, de forma que si un ruteador falla, el otro continuará ofreciendo acceso al resto de la red.

Algunos diseños van más allá, incluyendo dos redes troncales distribuidas distintas. Esta planificación incluye dos ruteadores en cada red horizontal, aunque en este caso cada ruteador está conectado a una red troncal distribuida distinta, como se muestra en la Fig. B.3. De esta forma, la interconexión de redes continuará funcionando a pesar del fallo de un ruteador, un concentrador de la red troncal, o cualquier segmento de cable de la misma.

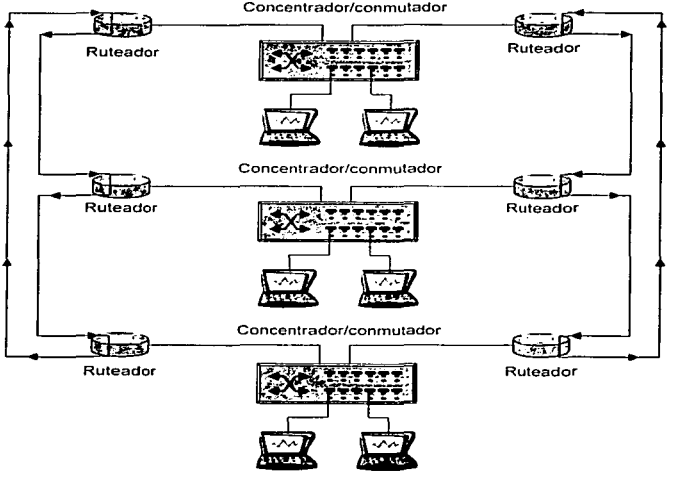


Figura B.3. Las redes troncales redundantes pueden proporcionar tolerancia a fallos.

Selección de un protocolo para la red troncal

El protocolo utilizado por la red troncal que conecta las redes horizontales entre sí, deberá depender del tráfico que tenga que cursar y de la distancia a cubrir. En algunas organizaciones, la mayor parte de la comunicación de red está limitada a redes LAN horizontales. Si, por ejemplo, una compañía está organizada en varios departamentos con gran autonomía, cada uno de ellos disponiendo de sus propios servidores en una red horizontal independiente, todo el tráfico generado permanece en la red horizontal y nunca alcanza la red troncal. En un caso como el mencionado, es posible utilizar la misma tecnología, como por ejemplo Fast Ethernet, tanto en la red troncal como en la red horizontal. Si, por el contrario, dicha compañía esta organizada en varios departamentos que comparten los mismos recursos, tales como bases de datos centralizadas, cuyos servidores de bases de datos se encuentran conectados directamente a la red troncal, implicará que, la red troncal deberá ser capaz cursar todo el tráfico generado por todas las redes horizontales. Si las redes horizontales trabajan con Fast Ethernet, la red troncal deberá utilizar tecnología de mayor velocidad, como por ejemplo Gigabit Ethernet, para admitir todo el tráfico.

La distancia que hay de cubrir la red troncal, así como el entorno en donde ésta se utilice, afectará a la elección de protocolo. Si la zona que se ha de cubrir es lo suficientemente amplia, de forma que el cable de red troncal pueda exceder del límite de los 100 metros para cable UTP, se deberá contemplar la posibilidad de utilizar fibra óptica.

Apéndice C

Fundamentos básicos de TCP/IP.

Existen muchas razones por las que TCP/IP se ha convertido en el grupo de protocolos preferido en la mayoría de las redes de datos; una de las principales es que son los protocolos utilizados en Internet. TCP/IP se diseñó para dar soporte a la incipiente Internet, entonces denominada ARPANET, en una época anterior a la aparición de las PC, en que la interoperatividad de productos informáticos realizados por diferentes fabricantes era, cuando menos, algo sin precedentes. Internet estaba, y está, compuesta por muchos tipos diferentes de computadoras y lo que se necesitaba era un grupo de protocolos comunes a todas ellas.

El elemento principal que diferencia a TCP/IP de los otros grupos de protocolos que proporcionan servicios de los niveles de red y de transporte en su mecanismo de direccionamiento autocontenido. A todo dispositivo de una red TCP/IP se la asigna una dirección de IP(a veces más de una), que lo identifica de forma única frente a los otros sistemas. La mayor pare de las PC de las redes actuales utilizan adaptadores de interfaz de red Ethernet o Token Ring que disponen de identificadores únicos (direcciones MAC) grabados en su interior, lo que hace que la dirección de IP se redundante. Sin embargo, muchos otros tipos de computadoras disponen de identificadores asignados por los administradores de red, y no existe ningún mecanismo para garantizar que ningún otro sistema en una red interconectada a escala mundial como Internet utiliza el mismo identificador.

Puesto que las direcciones de IP las registra un cuerpo centralizado, se pude tener la certeza de que no existen dos máquinas en Internet, correctamente configuradas, que posean la misma dirección. Debido a este direccionamiento, los protocolos TCP/IP pueden administrar prácticamente cualquier tipo de plataforma *hardware* o *software* que se utilice en la actualidad.

Otro aspecto único de los protocolos TCP/IP es el método de diseño, refinamiento y ratificación de sus estándares. En lugar de confiar el trabajo a un cuerpo elaborador de estándares institucionalizado, como la IEEE (*Institute of Electrical and Electronic Engineers*), los protocolos TCP/IP son desarrollados de forma democrática por un grupo de voluntarios *ad hoc* que se comunican principalmente por medio de la propia Internet. Cualquiera lo suficientemente interesado en contribuir en el desarrollo de un protocolo es siempre bienvenido. Además, los propios estándares son publicados por un organismo denominado *Internet Engineering Task Force (IETF)* y se entregan al dominio público, por lo que están disponibles para todo el mundo. Es posible descargar de forma legal cualquiera de los estándares de TCP/IP, denominados Petición de comentarios (*RFC, Request For Comments*), del sitio Web del IETF, en http:/www.ietf.org/, o de otros muchos sitios de Internet.

El principal factor que limita el crecimiento de Internet es el tamaño de 32 bits del propio espacio de direcciones de IP, y ya existe una nueva versión del protocolo IP, denominada IPv6, que solventa esa carencia con un espacio de direcciones de 128 bits.

Arquitectura de TCP/IP

TCP/IP esta diseñado para admitir redes de, prácticamente, cualquier tamaño. Como resultado, TCP/IP debe ser capaz de proporcionar los servicios que necesitan las aplicaciones que lo utilizan sin derrochar demasiado ancho de banda de red u otros recursos. Para satisfacer las necesidades de aplicaciones y funciones específicas, TCP/IP utiliza una combinación de varios protocolos para proporcionar la calidad de servicio requerida para la tarea, y nada más.

Pila de protocolos TCP/IP

TCP/IP ha precedido al modelo de referencia OSI, pero sus protocolos se reparten entre cuatro niveles que se pueden equiparar, más o menos, a los siete de la pila OSI, como se muestra en la Fig. C.1

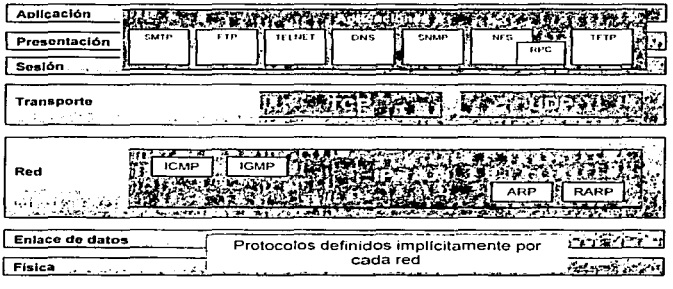


Figura C.1. La pila de protocolos de TCP/IP es, en términos generales, análoga al modelo de referencia OSI.

Para LAN, el protocolo TCP/IP no define la funcionalidad del nivel de enlace de datos, sino que lo hacen los protocolos estándar de ese nivel, como Ethernet o Token Ring. Para compaginar las direcciones MAC proporcionadas por un adaptador de interfaz de red con la dirección de IP utilizada en el nivel de red, los sistemas utilizan un protocolo TCP/IP denominado Protocolo de resolución de direcciones *(ARP, Address Resolution Protocol)*.

Sin embargo, los estándares de TCP/IP no definen los dos protocolos utilizados con más frecuencia para establecer comunicaciones de nivel de enlace mediante Modems y otras conexiones directas. Se trata del Protocolo punto a punto (*PPP, Point to Point Protocol*) y del Protocolo de Internet de línea serie (*SLIP, Serial Line Internet Protocol*).

En el nivel de internetwork se encuentran el Protocolo de Internet (*IP, Internet Protocol*), que es el portador principal para todos los protocolos que operan en niveles superiores y el Protocolo de mensajes de control de Internet (*ICMP, Internet Control Message Protocol*), que utilizan los sistemas TCP/IP para diagnóstico e informe de errores. IP, como protocolo portador de propósito general, es no orientado a conexión y no fiable, ya que servicios tales como corrección de errores y entrega garantizada se proporcionan, cuando se requieren, en el nivel de transporte.

En el nivel de transporte operan dos protocolos: el Protocolo de control de la transmisión (*TCP, Transmission Control Protocol*) y el Protocolo de datagramas de usuario (*UDP, User Datagram Protocol*). TCP es orientado a conexión y fiable, mientras que UDP es no orientado a conexión y no fiable. Una aplicación utilizará uno u otro en función de sus requisitos y de los servicios proporcionados por los demás niveles.

Se puede decir que, en términos generales, el nivel de transporte engloba los niveles de sesión y de transporte del modelo OSI, pero no en todos los casos. Ambos modelos son más bien herramientas pedagógicas y de diagnóstico que directrices para el desarrollo e implementación de protocolos, y no se pueden comparar de forma estricta con las funciones de los diferentes niveles de los protocolos reales.

El nivel de aplicación es el más difícil de definir, ya que los protocolos que operan en dicho nivel pueden ser aplicaciones totalmente completas, autocontenidas en sí mismas, como el Protocolo de transferencia de archivos (*FTP, File Transfer Protocol*), o mecanismos utilizados por otras aplicaciones para proporcionar un servicio, como el Sistema de nombres de dominio (*DNS, Domain Name System*) y el Protocolo sencillo de transferencia de correo (*SMTP, Simple Mail Transfer Protocol*).

Direccionamiento de IP

La dirección de IP es un identificador absoluto de la máquina individual y de la red en que reside. Todo paquete de datagramas IP transmitido por una red TCP/IP contiene la dirección IP del sistema origen que lo ha generado y del sistema destino al que va dirigido en su cabecera IP. Aunque los sistemas Ethernet y Token Ring disponen de una dirección *hardware* única codificada en la tarjeta de interfaz de red, no existe ningún método inherente para enrutar de forma efectiva, en una red grande, el tráfico hacia un sistema individual utilizando esta dirección.

La dirección *hardware* de una NIC se compone de un prefijo que identifica al fabricante de la tarjeta y una dirección de nodo que es única entre todas las tarjetas de ese fabricante. El prefijo del fabricante no tiene utilidad, en lo que se refiere al enrutamiento del tráfico, ya que cualquiera de las tarjetas del fabricante puede encontrarse de forma aleatoria en

cualquier parte de la red. Al identificar la red en la que se encuentra un equipo, las direcciones de IP se pueden enrutar hacia el lugar adecuado utilizando una lista relativamente manejable de direcciones de red.

Las direcciones de IP tienen una longitud de 32 bits y su notación consta de 4 números decimales de 8 bits separados por puntos, como 192.166.45.29. Esto se conoce como *notación decimal con puntos*; cada uno de los números de 8 bits se denomina *octeto* o *quad*. Puesto que cada *quad* es el equivalente decimal de un número binario de 8 bits, sus valores posibles están entre 0 y 255. Por tanto el intervalo completo de direcciones de IP posibles va de 0.0.0.0 a 255.255.255.255.

Las direcciones de IP en sí no representan computadoras; en lugar de eso representan interfaces de red. Una computadora con dos tarjetas de red o una NIC y una conexión vía módem a un servidor de TCP/IP dispone de dos direcciones de IP. Un sistema con dos o más interfaces se denomina *multi-hospedado* (*multihomed*). Si las interfaces conectan a la computadora a redes diferentes y el sistema está configurado para intercambiar tráfico entra las redes, se dice que el sistema funciona como ruteador.

Toda dirección de IP contiene bits que identifican una red y bits que identifican una interfaz, denominada *host*, de dicha red. Para hacer referencia a una red, los sistemas utilizan los bits de red, sustituyendo los bits de *host* por ceros. Los ruteadores utilizan los bits de red para dirigir paquetes a otro ruteador conectado en la red de destino, el cual transmite los datos al sistema *host* destino.

Máscaras de subred

Las direcciones de IP siempre dedican algunos bits al identificador de red, y otros al identificador de *host*, pero el número de bits utilizado para cada propósito no es siempre el mismo. Las direcciones más comunes utilizan 24 bits para la red y ocho para el *host*, pero la división entre los bits de red y de *host* puede encontrarse en cualquier parte de la dirección. Para identificar que bits se utilizan en cada caso, todo sistema TCP/IP dispone de una máscara de subred además de su dirección de IP. Una *máscara de subred* es un número binario de 32 bits cuyos bits corresponden a los de la dirección de IP. Un bit con un valor 1 en la máscara indica que el bit correspondiente de la dirección de IP forma parte del identificador de red, mientras que un bit a 0 indica que el bit de dirección correspondiente forma parte del identificador de *host*. Al igual que la dirección de IP, la máscara de subred se expresa en notación decimal con puntos, por lo que, aunque a veces pueda parecer una dirección de IP, la máscara posee una función completamente diferente.

Como ejemplo, considérese el sistema con la siguiente configuración TCP/IP:

Dirección de IP:	192.168.2.45
Máscara de subred:	255.255.255.0

En este caso, la parte 192.168.2 de la dirección de IP identifica la red, mientras que el 45 identifica al *host*. Cuando se expresa en forma decimal, esto puede parecer confuso. Por lo

que, con la intención de exhibir más claramente la división entre los bits de red y los bits de *host*, se muestra el equivalente en binario:

```
Dirección de IP:      11000000 10101000 00000010 00101101
Máscara de subred:    11111111 11111111 11111111 00000000
```

Como se puede ver en este ejemplo, la línea divisoria entre los bits de red y de *host* se encuentra entre el tercer y cuarto *quad*. Sin embargo, la línea divisoria no tiene porque encontrarse necesariamente entre dos *quad*. Una máscara de subred 255.255.240.0 asigna 12 bits a la dirección de *host*, ya que su equivalente binario es el siguiente:

```
11111111 11111111 11110000 00000000
```

La línea divisoria entre los bits de red y de *host* puede encontrarse en cualquier parte de los 32 bits de la máscara, pero nunca aparecen bits de red mezclados con bits de *host*. Una línea clara separa siempre los bits de red de la izquierda de los bits de *host* de la derecha.

Registro de direcciones de IP

Para que las direcciones de IP identifiquen de forma única los sistemas de la red, resulta esencial que no se asigne la misma dirección a dos interfaces. En una red privada, los administradores deben garantizar que cada dirección sea única. Pueden hacerlo controlando de forma manual las direcciones asignadas a sus redes y *host* o utilizando un servicio como DHCP (*Dynamic Host Configuration Protocol* o Protocolo de configuración dinámica de *host*) para asignar las direcciones de forma automática.

Sin embargo, en Internet este problema es considerablemente más complicado. Como administradores individuales controlando miles de redes diferentes, no sólo resulta poco práctico asumir que se pueden poner de acuerdo y garantizar que no se repite ninguna dirección, sino que además no existe ningún servicio a escala mundial que pueda asignar direcciones de forma automática. En lugar de eso, debe existir un agente neutro o registro para la asignación de direcciones de IP que asegure la no duplicidad de direcciones.

Sin embargo, incluso esta tarea es gigantesca, ya que se encuentran conectados a Internet millones de sistemas. De hecho, tal registro existe, pero en lugar de asignar direcciones de *host* individuales a cada sistema, asigna direcciones de red a organizaciones y empresas. La organización a cargo de registrar direcciones de red para Internet se denomina *Autoridad de asignación de números de Internet* (*IANA, Internet Assigned Numbers Authority*). Una vez que una organización obtiene una dirección de red, el administrador es responsable de asignar direcciones de *host* únicas a las máquinas de esa red.

Este sistema de administración en dos niveles constituye uno de los principios organizativos básicos de Internet. El registro de nombres de dominio funciona de la misma forma Una oficina de registro como *Network Solutions* registra nombres de dominio para organizaciones e individuos, y los administradores de esos dominios son responsables de asignar nombres a los *host* de esos dominios.

Clases de direcciones de IP

La IANA registra varias clases de direcciones de red, que se diferencian en las máscaras de subred, esto es, en el número de bits utilizados para representar la red y el *host*. Las clases de direcciones aparecen resumidas en la Tabla C.1.

Tabla C.1. Clases de direcciones de IP

	Clase A	Clase B	Clase C	Clase D	Clase E
Bits de dirección de red	8	16	24	N/D	N/D
Bits de dirección de *host*	24	16	8	N/D	N/D
Máscara de subred	255.0.0.0	255.255.0.0	255.255.255.0	N/D	N/D
Las direcciones comienzan por: (binario)	0	10	110	1110	1111
Valores del primer byte (decimal)	0-127	128-191	192-223	224-239	240-255
Número de redes	127	16,384	2,097,151	N/D	N/D
Número de *hosts*	16,777,214	65,534	254	N/D	N/D

La idea que se esconde detrás de las distintas clases es la de crear redes de varios tamaños, adecuadas para organizaciones y aplicaciones diferentes. Una empresa que dispone de una red relativamente pequeña puede registrar una dirección de Clase C, la cual, puesto que las direcciones sólo disponen de ocho bits de *host*, admite hasta 254 sistemas, mientras que organizaciones muy grandes pueden utilizar direcciones de Clase B o A con 16 o 24 bits de *host* y crear subredes a partir de ellas. Se crean subredes "tomando prestados" algunos de los bits de *host* y utilizándolos para crear identificadores de subred, en esencia redes dentro de una red. La forma más segura de identificar la clase de una dirección en particular consiste en mirar el valor del primer *quad*. El primer bit de las direcciones de Clase A siempre es un 0, lo que significa que los valores binarios del primer *quad* va de 00000000 01111111, lo que se traduce en los valores decimales 0 a 127. De la misma forma, las direcciones de Clase B siempre comienzan por 10, proporcionando valores para el primer *quad* desde 10000000 a 10111111, o 128 a 191. Las direcciones de Clase C comienzan con 110, por lo que el primer *quad* va de 11000000 a 11011111, o de 192 a 223.

En la práctica las empresas y organizaciones que poseen las redes individuales no registran las direcciones de red directamente con la IANA. En lugar de eso, existen ciertas compañías cuyo negocio consiste en proporcionar acceso a Internet, denominadas *Proveedores de servicio de Internet* (*ISP, Internet Service Provider*), que registran varias redes y proporcionan bloques de direcciones a clientes según las necesidades.

Las direcciones de Clase D no están diseñadas para la asignación en bloques como las otras clases. Esta parte del espacio de direcciones está destinada a direcciones de multidifusión. Las *direcciones de multidifusión* representan grupos de sistemas que poseen un atributo en común, pero que no se encuentran ubicadas, necesariamente, en el mismo lugar ni están administradas por al misma administración. Por ejemplo, los paquetes que se envían a la dirección de multidifusión 224.0.0.1 son procesados por todos los ruteadores de la subred local. El bloque de direcciones diseñadas como Clase E está reservado para su uso en el futuro.

Direcciones de IP no registradas

El registro de direcciones de IP está diseñado para redes conectadas a Internet con computadoras que deben estar accesibles desde otras redes. Cuando se registra una dirección de red nadie más puede utilizarla y los ruteadores de Internet disponen de la información necesaria para dirigir paquetes a esa red. Para una red privada, no conectada a Internet, no es necesario registrar direcciones de red. Además, la mayor parte de las redes comerciales conectadas a Internet utilizan algún tipo de producto de seguridad *(firewall)* para evitar que los intrusos tengan acceso a sus redes desde el exterior. En casi ningún caso existe la necesidad real de que todos los sistemas de la red estén accesibles directamente desde Internet, y existe un peligro genuino en hacerlo así. Muchos productos de seguridad, por tanto, aíslan los sistemas de la red, haciendo que no sea necesario registrar las direcciones de IP.

Para una red completamente aislada de Internet, los administradores pueden utilizar la dirección de IP que deseen, siempre que no esté duplicada en la misma red. Sin embargo, si alguna de las computadoras de la red se conecta a Internet, existe el potencial de un conflicto entre una dirección interna y el sistema de Internet con esa misma dirección registrada. Si, por ejemplo, se asigna a uno de los sistemas de la red la misma dirección que a un servidor de Web de la UNAM., el usuario de la red que trate de tener acceso al sitio de la UNAM puede llegar, en su lugar, a la máquina interna que tiene la misma dirección.

Para evitar esos conflictos, la RFC 1918, "*Address allocation for private Internets*", especifica tres intervalos de direcciones para redes no registradas, las cuales se muestran en la Tabla C.2. Dichas direcciones no se asignan a ninguna red registrada y, por tanto, las puede utilizar cualquier organización, pública o privada.

La utilización de direcciones IP no registradas no sólo simplifica el proceso de obtención y asignación de direcciones a los sistemas en red, sino que también conserva las direcciones de IP registradas para que las utilicen los sistemas que realmente las necesitan para comunicarse directamente con Internet.

Internet ha crecido tanto que casi todas las direcciones se obtienen de terceras partes y no directamente de la IANA. Además, la proliferación de otros dispositivos de comunicación que utilizan direcciones de IP, como computadoras de bolsillo (*palmtop*) y teléfonos móviles, podría originar una grave escasez de direcciones en un futuro próximo. El protocolo IPv6, actualmente en desarrollo, afronta esta escasez expandiendo el espacio de direcciones desde 32 bits a 128.

Tabla C.2. Direcciones de IP no registradas

Clase A	de 10.0.0.0 a 10.255.255.255
Clase B	de 172.16.0.0 a 172.31.255.255
Clase C	de 192.168.0.0 a 192.168.255.255

Direcciones de IP especiales

Además de los bloques de direcciones diseñados para redes no registradas, existen otras direcciones no asignadas a redes registradas porque poseen un cometido especial. Dichas direcciones se muestran en la Tabla C.3.

Tabla C.3. Direcciones de IP de propósito especial.

Dirección	Ejemplo	Función
Todos los bits a 0	0.0.0.0	Se refiere al *host* actual, como durante una transacción de DHCP antes de asignar una dirección de IP a una estación de trabajo.
Todos los bits a 1	255.255.255.255	Difusión limitada; se refiere a todos los *host* de la red local.
Todos los bits de *host* a 0	192.168.2.0	Identifica una red.
Todos los bits de *host* a 1	192.168.2.255	Difusión directa; se refiere a todos los *host* de otra red.
Todos los bits de red a 0	0.0.0.22	Se refiere a un *host* concreto de la red actual.
Primer *quad* a 127	127.0.0.1	Dirección interna de bucle de *host*.

Subredes

En teoría, las direcciones de IP que se asignan a los sistemas de una red no tienen que corresponder exactamente con los segmentos físicos de red, pero en la práctica es aconsejable. Obviamente, una organización que registra una dirección de Clase B no tiene 65,534 nodos en un mismo segmento de red; posee una internetwork compuesta por muchos segmentos, unidos por ruteadores, conmutadores u otros dispositivos. Para soportar una red de varios segmentos con una sola dirección de IP se crean subredes que corresponden a los segmentos físicos de red.

Una *subred* es, sencillamente, una subdivisión de la dirección de red, la cual se crea tomando algunos de los bits del identificador de *host* y utilizándolos como identificador de subred. Para hacerlo se modifica la máscara de subred en las máquinas para que los bits prestados aparezcan como parte del identificador de red, en lugar del identificador de *host*. Por ejemplo, se puede crear una subred a partir de una dirección de red de Clase B utilizando el tercer *quad*, cuyo propósito original era formar parte del identificador de *host*, para identificar la subred, Como se muestra en la Fig. C.2. Al modificar la máscara de subred de 255.255.0.0 a 255.255.255.0, se divide la dirección de Clase B en 254 subredes de 254 *host* cada una. Se asigna, a continuación, un valor diferente para el tercer *quad* a cada uno de los segmentos físicos de la red y se numeran los sistemas individuales utilizando solamente el cuarto *quad*. El resultado es que los ruteadores de la red pueden utilizar el valor del tercer *quad* para dirigir el tráfico a los segmentos apropiados.

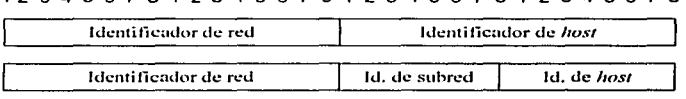


Figura C.2. Partiendo de una dirección estándar de Clase B (16 bits para red y 16 bits para *host*), se crean 254 subredes tomando prestados ocho bits de *host* para utilizarlos como identificador de subred.

El ejemplo anterior muestra el tipo más sencillo de subred, en el que los límites del identificador de subred se encuentran entre dos *quad*. Sin embargo, se puede utilizar cualquier cantidad de bits de *host* para el identificador de subred y ajustar la máscara de subred y la dirección de IP según corresponda. Esto se denomina *subredes de máscara variable*. Si, por ejemplo, se tiene una dirección de Clase B y se decide utilizar cuatro bits como identificador de subred, se tendría que utilizar una máscara de subred con el siguiente valor binario:

11111111 11111111 11110000 00000000

Los primeros cuatro bits del tercer *quad* pasan de 0 a 1 para indicar que ahora forman parte del identificador de red. El equivalente decimal de ese número es 255.255.240.0, que es el valor que se utiliza como máscara de subred en la configuración de TCP/IP del sistema. Al tomar prestados 4 bits de esta forma, se pueden crear hasta 14 subredes, cada una de las cuales compuesta por 4.094 *host*. La formula para determinar el número de subredes y *host* es la siguiente:

$$2^x - 2$$

donde x es igual al número de bits empleados para el identificador de subred. Se restan dos unidades para tener en cuenta los identificadores compuestos por todo 0 o todo 1, que no se

suelen asignar, ya que el valor 255 se utiliza para difusiones y el valor 0 para representar a la red. Para este ejemplo, por tanto, se realiza el siguiente cálculo:

$2^4 - 2 = 14$
$2^{12} - 2 = 4{,}094$

Para determinar que direcciones de IP se asignan a los sistemas particulares, se incrementan los cuatro bits del identificador de subred de forma independiente a los 12 bits del identificador de *host* y se convierte el resultado al formato decimal. Por lo tanto, asumiendo que se dispone de la dirección de red de Clase B 172.16.0.0 y la máscara de subred 255.255.240.0, la primera dirección de IP de la primera subred tendría la siguiente dirección binaria:

10101100 00010000 00010000 00000001

Los dos primeros *quad* son el equivalente binario de 172 y 16. El tercer *quad* está compuesto por los cuatro bits del identificador de subred, con el valor 0001, y los primeros cuatro bits del identificador de *host* de 12 bits. Puesto que es la primera dirección de esta subred, el valor del identificador de *host* es 000000000001.

Aunque esos 12 bits se incrementan como una sola unidad, cuando se convierten los valores binarios al formato decimal, se maneja cada *quad* por separado. Por tanto, el valor del tercer *quad* (00010000) en formato decimal es 16 y el valor del cuarto *quad* (00000001) en formato decimal es 1, resultando la dirección de IP 172.16.16.1.

La última dirección de esta subred tendría el siguiente valor binario:

10101100 00010000 00011111 11111110

que corresponde a la dirección de IP 172.16.31.254.

Para la siguiente subred, se incrementan los bits del identificador de subred a 0010 y se comienza de nuevo con 00000001 como primer *host* de la nueva subred. Por tanto, la primera dirección de la segunda subred es:

10101100 00010000 00100000 00000001

O:

172.16.32.1

Procediendo de esta forma se pueden crear las 14 subredes, utilizando el siguiente intervalo de direcciones:

172.16.16.1	-	172.16.31.254
172.16.32.1	-	172.16.47.254
172.16.48.1	-	172.16.63.254
172.16.64.1	-	172.16.79.254
172.16.80.1	-	172.16.95.254

172.16.96.1	-	172.16.111.254
172.16.112.1	-	172.16.127.254
172.16.128.1	-	172.16.143.254
172.16.144.1	-	172.16.159.254
172.16.160.1	-	172.16.175.254
172.16.176.1	-	172.16.191.254
172.16.192.1	-	172.16.207.254
172.16.208.1	-	172.16.223.254
172.16.224.1	-	172.16.239.254

Afortunadamente, no es necesario calcular de forma manual los valores de las direcciones de IP cuando se crean subredes de esta forma. Existen utilidades que permiten especificar una dirección de red y su clase y, a continuación, seleccionar el número de bits a utilizar para el identificador de subred. El programa proporciona las direcciones de IP para las máquinas de las subredes individuales. Existe una utilidad de *software* libre para el cálculo de subredes IP, disponible para descargar en http:/www.wildpackets.com/products/ipsubnetcalculator/.

Apéndice D

Codificación de información analógica y digital.

La codificación es el proceso de transformación de información en una señal con patrones acordados y conocidos tanto por el sistema emisor como por el receptor. Existen cuatro tipos de codificación: digital-digital, digital-analógico, analógico-digital y analógico-analógico (ver Fig. D.1).

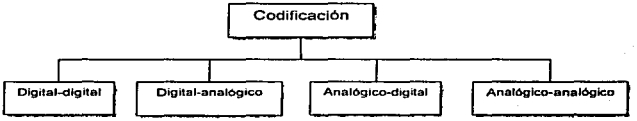


Figura D.1. Esquemas de codificación.

Codificación digital-digital

La codificación digital-digital es la representación de información digital por medio de una señal digital. Por ejemplo, cuando se transmiten datos de una computadora a una impresora, tanto los datos de la computadora como los de al impresora son digitales. En este tipo de codificación, los datos binarios generados por la computadora son traducidos en una secuencia de pulsos de voltaje que pueden propagarse sobre un alambre. La Fig. D.2 muestra la relación entre la información digital, el *hardware* de la codificación digital-digital y la señal digital resultante.

Figura D.2. Codificación digital-digital.

De todos los mecanismos utilizados para la codificación digital-digital, los más comúnmente utilizados en la comunicación de datos, se ubican en tres categorías: unipolar, polar, y bipolar. La Fig. D.3 muestra esta clasificación.

A excepción de la codificación unipolar, para cada una de estas categorías se han desarrollado diferentes métodos de codificación enfocados a solucionar los problemas que los sistemas de transmisión digital enfrentan. La codificación unipolar, aunque primitiva y casi obsoleta en nuestros días, nos permite entender y examinar dichos problemas, los cuales son: componente de DC y sincronización.

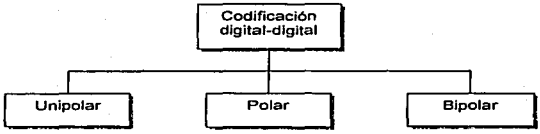


Figura D.3. Familias de codificación digital-digital.

Componente de DC

La amplitud promedio de una señal con codificación unipolar no es cero. Esto genera lo que se conoce como componente de corriente directa. Cuando una señal contiene un componente de DC, no puede viajar a través de medios incapaces de manejar componentes de DC, como es el caso de micro-ondas y transformadores.

Sincronización

Los esquemas de codificación digital utilizan los cambios en los niveles de voltaje para identificar cambios en el tipo de bit. Un cambio de señal, también indica que un bit ha terminado y que uno nuevo ha empezado. Cuando una señal no tiene cambios, el sistema receptor no puede determinar el principio y el fin de cada bit. En el caso de la codificación unipolar, los problemas de sincronización pueden ocurrir frecuentemente cuando una cadena de datos incluye una serie ininterrumpida de 1s o 0s. Supongamos que tenemos una velocidad de transmisión de 1Kbps, si el receptor detecta un voltaje positivo que dure 0.005 segundos, este leerá un bit por cada 0.001 segundo, o cinco 1s. Desafortunadamente, la propagación de retardos puede distorsionar el tiempo de la señal de forma tal que, por ejemplo, cinco 1s se estiren hasta 0.006 segundos ocasionando que el receptor lea un bit 1 extra. Ahora imaginemos que en lugar de un bit 1 extra codificado erróneamente hablamos de *n* bits 1s extras.

La Tabla D.1 muestra la clasificación completa de los métodos de codificación digital-digital más comúnmente utilizados, así como sus ventajas y desventajas.

Tabla D.1. Clasificación de los métodos de codificación digital-digital

Familia	Tipo	Subtipo	Descripción	Ventajas	Desventajas	Comentarios
Unipolar			Sólo uno de los estados binarios, generalmente el 1, es codificado con un voltaje positivo, el otro estado, usualmente el 0, se representa con ausencia de voltaje.		Genera componente de DC y problemas de Sincronía.	Debido a los problemas que genera no tiene aplicación.
Polar	NRZ	NRZ-L	El 1 binario es representado con un voltaje positivo, y el 0 por uno negativo.	Aminora el problema de la componente de DC.	Una cadena consecutiva de 1s o 0s puede afectar a la sincronía.	La línea libre significa que no existe transmisión alguna.
		NRZ-I	Una inversión en el nivel de voltaje representa un 1 binario, y la ausencia de cambio de voltaje representa un 0 binario.	Aminora el problema de la componente de DC y ayuda a la sincronización en caso de que se presente una cadena consecutiva de 1s.	Una cadena consecutiva de 0s puede afectar a la sincronía.	
	RZ		La señal no cambia entre bits sino durante cada bit. Un voltaje positivo significa 1 y uno negativo significa 0, pero a la mitad del camino de cada intervalo de bit, la señal regresa a cero	Aminora el problema de la componente de DC y ayuda a la sincronización en caso de que se presente una cadena consecutiva de 1s o 0s.	Requiere dos cambios de señal para codificar un bit y por lo tanto requiere más ancho de banda.	Es la más efectiva de las tres alternativas de la codificación polar.
	Doble-fase	Manchester	La señal cambia a la mitad del intervalo del bit pero no regresa a cero. En lugar de ello, continua en el polo opuesto. Una transición negativo-a-positivo representa un 1 binario y una transición de positivo-a-negativo representa un 0 binario.	Consigue el mismo nivel de sincronización que RZ pero con sólo dos niveles de amplitud.		Método utilizado en LAN Ethernet
		Manchester diferencial	La señal cambia a la mitad del intervalo del bit pero no regresa a cero. En lugar de ello, continua en el polo opuesto. Una inversión significa 0 binario y la no-inversión significa 1 binario.			Método utilizado por LAN Token Ring
Bipolar	AMI		Utiliza tres niveles de voltaje: positivo, negativo y cero. El nivel cero representa 0 binario, mientras que los voltajes positivo y negativo representan alternadamente 1s binarios.	Elimina la componente de DC y asegura la sincronización en caso de presentarse una cadena consecutiva de 1s.	Una cadena consecutiva de 0s puede afectar a la sincronía.	La alternancia ocurre incluso cuando los 1s no son consecutivos.
	B8ZS		Funciona igual que AMI, con la diferencia de que en caso de presentarse 8 ceros consecutivos, B8ZS introducirá un patrón de bits artificial, llamado violación, basándose en la polaridad del bit 1 anterior.	Elimina la componente de DC y asegura la sincronización en caso de presentarse una cadena consecutiva de 1s o 0s.		Comúnmente utilizado en Norte América.
	HDB3		Funciona igual que B8ZS, con la diferencia de introduce una violación cada 4 ceros consecutivos en lugar de cada 8. Dicha violación se basa en la polaridad del bit 1 anterior y en la cantidad de 1s que han ocurrido en el flujo de bits desde la última sustitución.			Comúnmente utilizado en Europa y Japón.

Nomenclatura:

NRZ (Non-Return to Zero)	No regreso a cero.
RZ (Return to Zero)	Regreso a cero.
NRZ-L (Non-Return to Zero, Level)	No regreso a cero, nivel.
NRZ-I (Non-Return to Zero, Invert)	No regreso a cero invertido.
AMI (Alternate Mark Inversion)	Inversión de marca alternada.
B8ZS (Bipolar 8-Zero Substitution)	Substitución del 8° cero.
HDB3 (High-Density Bipolar 3)	Código bipolar de alta densidad con máximo 3 ceros consecutivos.

Codificación analógico-digital.

La codificación analógica-digital es la representación de información analógica por medio de una señal digital. O en otras palabras, es la representación de la información contenida en forma de onda como una serie de pulsos digitales. La Fig. D.4 ilustra esquemáticamente este tipo de codificación.

Figura D.4. Codificación analógica-digital.

Hasta ahora, los sistemas de codificación que hemos examinado se han enfocado en el formato de la señal que se desea transportar. La codificación analógica-digital puede hacer uso de cualquiera de las señales digitales citadas anteriormente. La estructura de la señal que se desea transportar no es el problema, el problema es como traducir la información de un número infinito de valores a un número discreto de valores sin sacrificar sentido y calidad.

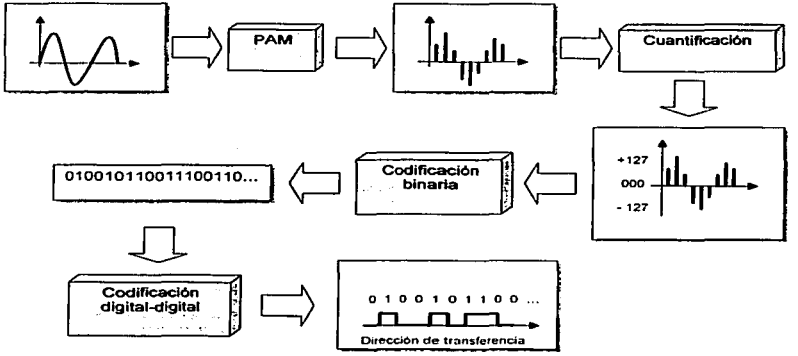


Figura D.5. Proceso de codificación analógica-digital con PCM.

El método de codificación analógico-digital más conocido es el de modulación por codificación de pulsos (*PCM, Pulse Code Modulation*), y consta de 4 etapas:

1. Muestreo de la señal analógica (*PAM, Pulse Amplitude Modulation*).
2. Cuantificación de los pulsos.
3. Codificación binaria.
4. Codificación digital-digital.

La Fig. D.5 muestra gráficamente el proceso completo de la codificación analógica-digital con PCM.

Tasa de muestreo

La precisión de la reproducción digital de una señal analógica depende del número de muestras que se tomen. Utilizando PCM, podemos reproducir una onda de forma exacta, tomando una infinidad de muestras, o un bosquejo de onda si tomamos sólo tres muestras. La pregunta entonces es, cuántas muestras son suficientes?

De acuerdo con el *teorema de Nyquist*, para asegurar la precisión de la reproducción de una señal analógica, la tasa de muestreo debe ser al menos el doble de la frecuencia más alta de la señal original. Por ejemplo, si deseamos digitalizar una señal de voz sobre una línea telefónica cuya frecuencia máxima es de 3,300 Hz, necesitaremos una velocidad de 6,600 muestras por segundo, aunque en la práctica se realizan 8,000 muestras por segundo para compensar las imperfecciones de procesos posteriores.

Codificación digital-analógica.

La codificación digital analógica es la representación de información digital por medio de una señal analógica. La Fig. D.6 muestra la relación entre la información digital, el *hardware* de codificación digital-analógico y la señal analógica resultante.

Figura D.6. Codificación digital-analógica.

Existen muchos mecanismos para codificar datos digitales en una señal analógica, pero para efectos de este documento, sólo nos referiremos a aquellos que se usan más frecuentemente en la comunicación de datos: desplazamiento de amplitud (*ASK, Amplitude Shift Keying*), desplazamiento de frecuencia (*FSK, Frequency Shift Keying*), desplazamiento de fase (*PSK, Phase Shift Keying*), y modulación de amplitud en cuadratura (*QAM, Quadrature Amplitude Modulation*), siendo esta última la más eficiente de estas opciones y el mecanismo implementado en todos los módems modernos (ver Fig. D.7).

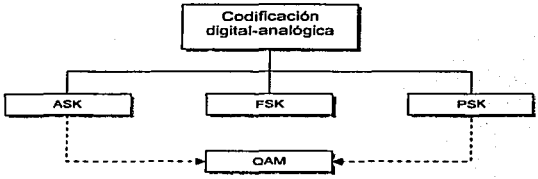


Figura D.7. Tipos de codificación digital-analógica.

Bit rate y Baud rate

Con frecuencia los términos *bit rate* y *baud rate* se utilizan de forma indistinta, lo cual es incorrecto. *Bit rate* es el número de bits transmitidos durante un segundo. Mientras que *Baud rate* es el número de unidades de señal transmitidas por segundo, que se requieren para representar los bits. La razón de esta confusión, es que los primeros módems transmitían un bit por *baud*, es decir, un módem de 1,200 *bauds* transmitía 1,200 bps. Sin embargo con el tiempo, fue necesario transmitir a una tasa mayor de bits, por lo que se diseñaron técnicas para "empaquetar", tantos bits como fuera posible, en un *baud*.

Desde un punto de vista eficiencia de computadoras, el *bit rate* es más importante, ya que lo interesante es saber cuanto tiempo tomará procesar cada pieza de información. En la transmisión de datos, sin embargo, es más interesante saber como podemos mover datos de un punto a otro de forma eficiente. A menor requerimiento de unidades de señal (*bauds*), mayor eficiencia del sistema y menor ancho de banda requerido para transmitir más bits: de modo que lo importante en este caso es el *baud rate*. De hecho el *baud rate* determina el ancho de banda que se requiere para enviar una señal. Por lo anterior, la cantidad de bps puede calcularse de la siguiente manera:

Bit rate = *Baud rate* * el número de bits por *baud*

Señal portadora

En la transmisión analógica el dispositivo emisor genera una señal de alta frecuencia que actúa como base para la señal de información. Esta señal base es llamada señal portadora o frecuencia portadora. El dispositivo receptor está sintonizado a la frecuencia de la señal portadora que espera del emisor. La señal de información es entonces decodificada de la señal portadora modificando una o más de sus características (amplitud, frecuencia o fase). Este tipo de modificación es llamado modulación y la señal de información es llamada señal moduladora.

La Tabla D.2 concentra las descripciones de los diferentes tipos de modulación utilizados en al codificación digital-analógica.

Tabla D.2. Características de la modulación ASK, FSK, PSK y QAM.

Tipo	Descripción	Ventajas	Desventajas	Ancho de banda
ASK	La amplitud de la señal varía para representar 1s y 0s. Tanto la frecuencia como la fase permanecen constantes. La velocidad de transmisión está limitada por las características físicas del medio de transmisión.		Es muy susceptible a interferencias causadas por ruido.	Igual al *baud rate* de la señal.
FSK	La frecuencia de la señal varía para representar 1s y 0s binarios. Tanto la amplitud como la fase permanecen constantes.	FSK elimina la mayoría de los problemas de ruido.	FSK está limitado por las capacidades físicas de la señal portadora.	Igual al *baud rate* de la señal más el desplazamiento de la frecuencia.
PSK	La fase de la señal varía para representar 1s y 0s binarios. Tanto la amplitud como la frecuencia permanecen constantes.	No es susceptible a la degradación por ruido que afecta a ASK ni a las limitaciones de ancho de banda de FSK.		Igual al *baud rate* de la señal. Pero con la diferencia de que su *bit rate* puede ser 2, 4 u 8 veces mayor al de ASK.
QAM	Es la combinación de ASK y PSK, donde se tienen *x* variantes de fase y *y* variantes en amplitud. El número de desplazamientos de amplitud siempre será menor que el número de desplazamientos de fase, debido a que los cambios en amplitud son susceptibles al ruido.	Ofrece la posibilidad de transmitir datos a una tasa mayor que PSK, ASK o FSK. Es decir, cada *baud* puede representar 2, 3, 4, etc. bits (4-QAM, 8-QAM, 16-QAM respectivamente). Además, es poco susceptible al ruido.		Igual al *baud rate* de la señal. Pero con la diferencia de que su *bit rate* puede ser mucho mayor al de FSK, ASK y PSK.

NOTA: El término ruido se refiere a la introducción no intencional de voltajes en la línea debido a varios fenómenos como calor o inducción electromagnética generada por otras fuentes.

Codificación analógica-analógica

La codificación analógica-analógica es la representación de información analógica por medio de una señal analógica. La Fig. D.8 ilustra la relación que existe entre la información analógica, el *hardware* codificador analógico-analógico, y la señal analógica resultante.

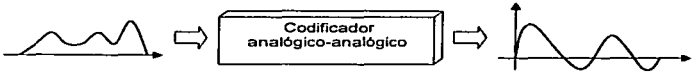


Figura D.8. Codificación analógica-analógica.

La codificación analógica-analógica puede llevarse a cabo de tres formas: amplitud modulada (AM), frecuencia modulada (FM), y fase modulada (PM), como se ilustra en la Fig. D.9.

Figura D.9. Tipos de codificación analógico-analógica.

La Tabla D.3 describe brevemente en que consiste cada una de estas técnicas.

Tabla D.3. Características de AM, FM y PM.

Tipo	Descripción	Ancho de banda	Comentarios
AM	La señal portadora es modulada por los cambios de amplitud de la señal de información (señal moduladora). Tanto la frecuencia como la fase de la señal portadora permanecen constantes.	El doble del ancho de banda de la señal moduladora, cubriendo un rango centrado alrededor de la frecuencia portadora.	La Comisión Federal de Comunicaciones autoriza un ancho de banda 10 Khz. por estación AM. Las frecuencias de las estaciones AM se ubican entre los 530 y 1700 Khz.
FM	La frecuencia de la señal portadora es modulada con base a los cambios de nivel de voltaje (amplitud) de la señal moduladora. Tanto la amplitud como la fase de la señal portadora permanecen constantes.	10 veces el ancho de banda de la señal moduladora, cubriendo un rango centrado alrededor de la frecuencia portadora.	La Comisión Federal de Comunicaciones autoriza 200 Khz. por cada estación FM. Las frecuencias de las estaciones FM se ubican entre los 88 y 108 MHz.
PM	La fase de la señal portadora es modulada siguiendo los cambios del nivel de voltaje (amplitud) de la señal moduladora. Tanto la frecuencia como la amplitud de la señal portadora permanecen constantes.		

Bibliografía

Teare, Diane, 1999. *Designing Cisco Networks*. Indianápolis: Editado por Cisco.

Craig Zacker, 2002. *Redes, manual de referencia*. España: Editado por Mc Graw-Hill.

Anders Olsson, 1997. *Understanding Telecommunications 1*. Suecia: Editado por Ericsson Telecom, Telia y Studentlittelatur.

Ericsson Telecom, 1999. *Datacom Networking*. Suecia: Editado por Telefonaktiebolaget LM Ericsson

Behrouz A. Forouzan, 2000. *TCP/IP Protocol Suite*. Editado por Mc Graw-Hill.

Dr. Sydney Feit, 1997. *TCP/IP Arquitecturas, protocolos e implementación con IPv6 y seguridad de IP*. Editado por Mc Graw-Hill.

William Stallings, 1997. Data *and Computer Communications*. Prentice Hall.

Behrouz A. Forouzan, 1998. *Introduction to data Communications and Networking*. Mc Graw-Hill.

Paul e. Green Jr., 1988. Network Interconnection and Protocol Conversion. Editado por la IEEE.

Spraging Hammond Paulikowski, 1994. Telecommunications, Protocols and Design. Addison-Wesley Publishing Company.

Gilbert Herd, 1993. Data communications Networking Devices. John Wiley & Sons.

Martha Steenstrup, 1995. Routing in Communications Networks. Prentice Hall.