CAPÍTULO 5

Fundamentos de Ethernet

Ethernet, en sus varias formas, es la tecnología de red de área local (LAN) más ampliamente utilizada. Ethernet fue diseñada para llenar el vacío existente entre las redes de larga distancia, las redes de baja velocidad y las redes especializadas en salas de computadoras que transportan datos a altas velocidades y en distancias muy pequeñas.

Ethernet se ajusta también a aplicaciones en las que los medios de comunicación locales deben llevar esporádicamente un tráfico muy denso con tasas de datos altamente empaquetados. Fue diseñada para permitir compartir los recursos a nivel de grupo de trabajo local. Los objetivos de su diseño incluyen la simplicidad, un bajo coste, la compatibilidad, el poco retardo y la alta velocidad.

En este capítulo conocerá la historia de Ethernet y las normas IEEE Ethernet. Este capítulo explica el funcionamiento de Ethernet, el entramado Ethernet y la manipulación de errores, así como los diferentes tipos de colisiones en las redes Ethernet. Además, este capítulo presenta los dominios de colisión y los dominios de difusión. Por último, se describe la segmentación y los dispositivos que se emplean para crear segmentos de red.

Consulte los capítulos e-Lab Activities, Videos y PhotoZooms asociados que encontrará en el CD-ROM que incluye este libro. Los elementos de dicho CD-ROM están diseñados para complementar el material y reforzar los conceptos introducidos en este capítulo.

Historia y evolución de Ethernet

Las redes LAN son redes de alta velocidad y con un nivel muy bajo de errores que cubren un área geográfica relativamente pequeña (unos pocos cientos de metros). Conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un edificio o en un área delimitada geográficamente.

Ethernet es la tecnología LAN dominante a nivel mundial. La mayor parte del tráfico en Internet se origina y finaliza con una conexión Ethernet. Desde su origen a principios de los 70, Ethernet ha evolucionado hasta equipararse con el aumento de demanda en redes LAN de alta velocidad. Cuando se desarrolla un nuevo medio, como la fibra óptica, Ethernet se adapta para beneficiarse del gran ancho de banda de la fibra y de su flujo de datos con muy pocos errores. El mismo protocolo que transportaba datos a 3 megabits por segundo (Mbps) en 1973, transporta ahora datos a 10 gigabits por segundo (Gbps).

El éxito de Ethernet es el resultado de su simplicidad y fácil mantenimiento, de su capacidad para incorporar nuevas tecnologías, de su fiabilidad y de su bajo coste de instalación y actualización. Con la introducción de Gigabit Ethernet, que comenzó como una nueva tecnología LAN, se han extendido ahora los espacios que hacen ya de Ethernet un estándar de área metropolitana e incluso, de red de área amplia. Esta sección proporciona una visión global de Ethernet, incluyendo su historia, la convención de nombres Ethernet y los formatos de tramas Ethernet.

Introducción a Ethernet

La idea original que hizo crecer a Ethernet fue permitir a dos o más usuarios el empleo del mismo medio sin que las señales de cada uno interfiriesen con las del otro. Este problema de acceso a múltiples usuarios que comparten un medio se estudió a principios de los 70 en la Universidad de Hawai. Se desarrolló un sistema que se llamaba Alohanet que permitía la instalación de varias estaciones con acceso estructurado para compartir la banda de radiofrecuencia de la atmósfera en las islas de Hawai. La tecnología actual de Ethernet está basada en ella. Este trabajo formaría tiempo después las bases para el famoso método Ethernet MAC, conocido como **acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, *Carrier Sense Multiple Access Collision Detect***. CSMA/CD se explica con más detalle más adelante en este mismo capítulo.

La versión original de Ethernet fue la primera red LAN del mundo. Fue diseñada hace más de 30 años por Robert Metcalfe y sus compañeros de Xerox. La primera norma Ethernet se publicó mediante un consorcio formado por Digital Equipment Company, Intel y Xerox (DIX) en 1980. Metcalfe quiso que Ethernet fuese una norma compartida de la cual todo el mundo pudiese beneficiarse. Por tanto, DIX hizo de su nueva norma una norma abierta, lo que quiere decir que puede utilizarla cualquier otra empresa. Esto no se había hecho antes en la industria de las computadoras. Los primeros productos desarrollados que usaban la norma Ethernet se vendieron durante principios de los 80. Estos productos transmitían a 10 Mbps sobre un fino cable coaxial (con un diámetro aproximado al del dedo meñique) a una distancia de dos kilómetros. Ethernet fue un éxito instantáneo.

El **Instituto de ingenieros eléctricos y electrónicos (IEEE)** es una organización profesional que define las normas de red. En 1985, el comité de normalización IEEE para las redes locales y metropolitanas publicó sus normas para las redes LAN. Las normas IEEE LAN son las predominantes y más conocidas para las redes LAN actuales. Estas normas comenzaron con el número 802, y la que está basada en Ethernet es la 802.3. El IEEE quiso asegurarse que sus normas eran compatibles y encajaban con el modelo de referencia OSI del ISO. El IEEE divide la capa de enlace de datos OSI en dos subcapas separadas: control de acceso al medio (MAC, *Media Access Control*) y control de enlace lógico (LLC, *Logical Link Control*).

Como resultado, se hicieron algunas pequeñas modificaciones en la norma Ethernet 802.3 original. Existen algunas diferencias entre Ethernet DIX y las especificaciones 802.3. Sin embargo, las diferencias entre las dos normas son tan mínimas que cualquier tarjeta de interfaz de red (NIC, *Network Interface Card*) Ethernet puede recibir Ethernet y paquetes y tramas 802.3. En esencia, Ethernet e IEEE 802.3 son las mismas normas. Recuerde que 802.3 es ahora la norma oficial IEEE Ethernet.

Durante mediados de los 80, el ancho de banda de Ethernet (10 Mbps) era más que suficiente para los PC de aquella época. A principios de los 90, los PC se hicieron mucho más rápidos y los usuarios se empezaron a quejar de cuellos de botella que provocaban el pequeño ancho de banda de las redes LAN Ethernet. En 1995, el IEEE anunció una norma para Ethernet a 100 Mbps. A ésta le siguieron normas para Ethernet Gigabit (mil millones de bits por segundo) en 1998 y 1999. El IEEE aprobó las normas para Ethernet a 10 Gb en junio de 2002. Estas normas modernas son también Ethernet (802.3).

Todas estas nuevas normas son esencialmente compatibles con las originales de Ethernet. Un paquete (o trama) Ethernet que llevase una vieja NIC a 10 Mbps en un PC, eventualmente un *router* la colocaría en un enlace de fibra Ethernet a 10 Gbps, y al terminar en una tarjeta Ethernet a 100 Mbps. Mientras el paquete permanezca en las redes Ethernet, no cambiará, demostrando una de las principales razones del gran éxito de Ethernet. Es muy escalable. Esto quiere decir que el ancho de banda de la red se puede aumentar una y otra vez sin cambiar la tecnología Ethernet subyacente.

El Ethernet original (IEEE 802.3) ha sido renovado varias veces para incorporar nuevos medios de transmisión que permitan velocidades más altas. Sin embargo, es importante comprender que se han mantenido sus cualidades originales. Las normas Ethernet 802.3 pertenecen todas a la misma familia. Existen diferencias entre las normas, pero son mayores sus similitudes. El hecho de mantener el original en cada nueva norma quiere decir que los protocolos de la familia 802.3 son todos compatibles.

Reglas para los nombres Ethernet IEEE

El término "Ethernet" se refiere a una familia de tecnologías de red que incluyen Ethernet, **Fast Ethernet**, **Gigabit Ethernet** (o Gig-E) y **Ethernet a 10 GB** (o 10-G). Estos tipos de Ethernet se explican con detalle en el Capítulo 6.

Las interfaces Ethernet pueden variar de 10 a 100.000 dólares USA. Sus velocidades pueden ser de 10, 100, 1000 ó 10.000 Mbps. Esta sección explora más detalles del Ethernet original (10BASE-T), Fast Ethernet (100BASE-TX y 100BASE-FX), Gigabit Ethernet (100BASE-T y 1000BASE-X) y Ethernet a 10 Gb. Dos funciones de Ethernet permanecen constantes en Ethernet a lo largo de todas sus formas: el formato de trama básico y las subcapas IEEE de la capa 2 OSI.

Cuando Ethernet necesita expandirse para añadir un nuevo medio o capacidad, el IEEE añade un nuevo suplemento para la norma 802.3. El nuevo suplemento recibe la designación de una o dos letras, por ejemplo, 802.3u es Fast Ethernet, y se le asigna también una descripción abreviada (identificador). Los siguientes son ejemplos de algunos suplementos:

- 10BASE2 (IEEE 802.3a).
- 10BASE5 (IEEE 802.3).
- 100BASE-T (IEEE 802.3i).
- 1000BASE-TX (IEEE 802.3X).

Como puede comprobar, la descripción abreviada consiste en:

- Un número que indica la cantidad de megabits que se transmite.
- La palabra BASE, que indica la señal de banda base que se emplea.
- Números (el 2 y el 5) que hacen referencia a la longitud del segmento del cable coaxial (la longitud de 185 m ha sido redondeada a 2, para 200).
- Una o más letras del alfabeto que indican el tipo de medio que se emplea (F = cable de fibra óptica, T = cable de par trenzado sin apantallar).

La señalización de banda base es el método más sencillo de señalización. El ancho de banda total del medio de transmisión se emplea para la señal. Se transmite directamente la señal de datos (un voltaje en UTP o un flash de luz en la fibra) sobre el medio de transmisión. No se necesita ninguna otra señal (señal portadora) especial. Ethernet utiliza la señal de banda base.

Un segundo método de señalización, la señalización de banda ancha, no se utiliza en Ethernet. En esta señalización, la señal de datos nunca se coloca directamente en el medio de transmisión. En su lugar, la señal de datos modula una señal análoga, que se llama señal portadora, y después se transmite. Las difusiones por radio y la TV por cable utilizan este tipo de señalización.

Al igual que la organización internacional para la normalización (ISO), el IEEE es una organización creadora de normas. A los fabricantes de los equipos de red no se les pide que cumplan fielmente con todas las especificaciones de las normas. Los objetivos del IEEE son:

- Proporcionar la información de ingeniería necesaria para la construcción de dispositivos que cumplan con la norma Ethernet.
- No reprimir las innovaciones de los fabricantes.

Si está creando o manteniendo una pequeña red LAN, puede comprar todo el equipo de un fabricante de garantía, y así asegurarse la compatibilidad de todos los dispositivos. Sin embargo, si es el responsable de una gran red formada por redes LAN Ethernet más pequeñas con equipos de más de un fabricante, la situación es diferente. La capacidad de usar equipos de varios fabricantes es un tema muy importante a la hora de la fiabilidad. Desgraciadamente no existe ninguna industria o agencia estatal que pruebe y certifique que un dispositivo cumple perfectamente las normas IEEE. Sin embargo, es una buena forma para que se eduque a sí mismo en las normas y la industria. El hecho es que sólo tiene sus conocimientos, y los de sus compañeros de trabajo, en los que basar sus diseños y decisiones de compras.

IEEE 802.3/Ethernet y el modelo OSI

Las normas de las redes LAN definen el medio físico y los conectores que se emplean para conectar los dispositivos al medio en la capa física del modelo de referencia OSI. Estas normas también definen la forma de comunicar estos dispositivos con la capa de enlace de datos. Además, las normas de las redes definen cómo encapsular el tráfico específico del protocolo de modo que el tráfico que vaya a los diferentes protocolos de capa

pueda utilizar el mismo canal que pasa a través de las capas del modelo OSI. proporcionar estas funciones, la capa de enlace de datos Ethernet IEEE tiene dos

- **Control de acceso al medio (MAC) (802.3)**. Como su nombre indica, la subcapa MAC define el modo de transmitir las tramas por el hilo físico. Manipula el direccionamiento físico asociado a cada dispositivo, la definición de la topología de la red y la disciplina de línea.
- **Control de enlace lógico (LLC) (802.2)**. Como su nombre indica, la subcapa LLC es la responsable de la identificación lógica de los diferentes tipos de protocolos y de su posterior encapsulación. Un código de tipo o un identificador de punto de acceso al servicio (SAP) realizan la identificación lógica. El tipo de trama LLC que emplea una estación depende de lo que el identificador de protocolo de capa superior (como IP) espere. Aunque la **IEEE 802.2** representa un tipo estándar de **encapsulación** de tramas, existen otras, como Ethernet II (que se emplea principalmente con las LAN Ethernet basadas en TCP/IP). Este asunto se explica más adelante en este mismo capítulo.

Como se muestra en la Figura 5.1, la norma **IEEE 802.3** define la capa física (capa 1) y subcapa MAC de la capa de enlace de datos (capa 2).

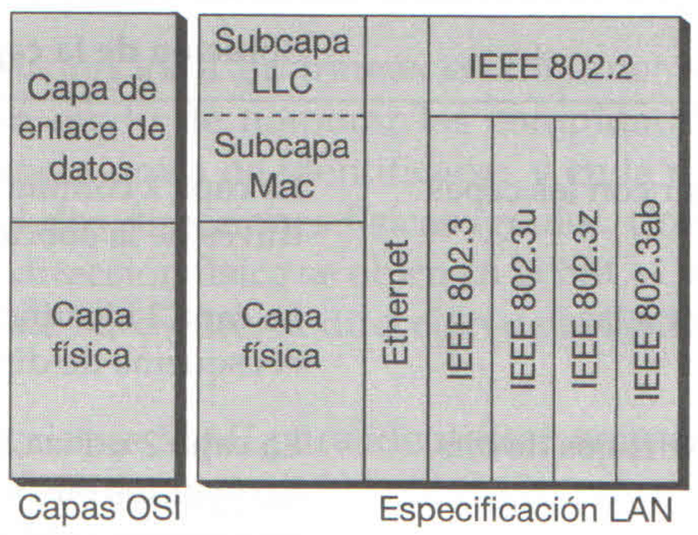

Figura 5.1. Ethernet 802.3 y el modelo OSI.

La Figura 5.2 presenta varias tecnologías para la capa 1 OSI y la mitad inferior de la capa 2. En este libro nos basamos principalmente en la tecnología LAN Ethernet. La capa física, comprende la interfaz con los medios, las señales, los flujos de bits que viajan por los medios, los componentes que colocan señales en los medios y varias tecnologías. La capa física desempeña un papel clave en la comunicación que tiene lugar entre computadoras, pero su esfuerzo en solitario no es suficiente. Cada una de sus funciones tiene sus propias limitaciones. La capa 2 se encarga de esas limitaciones.

Para cada limitación de la capa 1, la capa 2 tiene una solución, como se documenta en la Tabla 5.1.

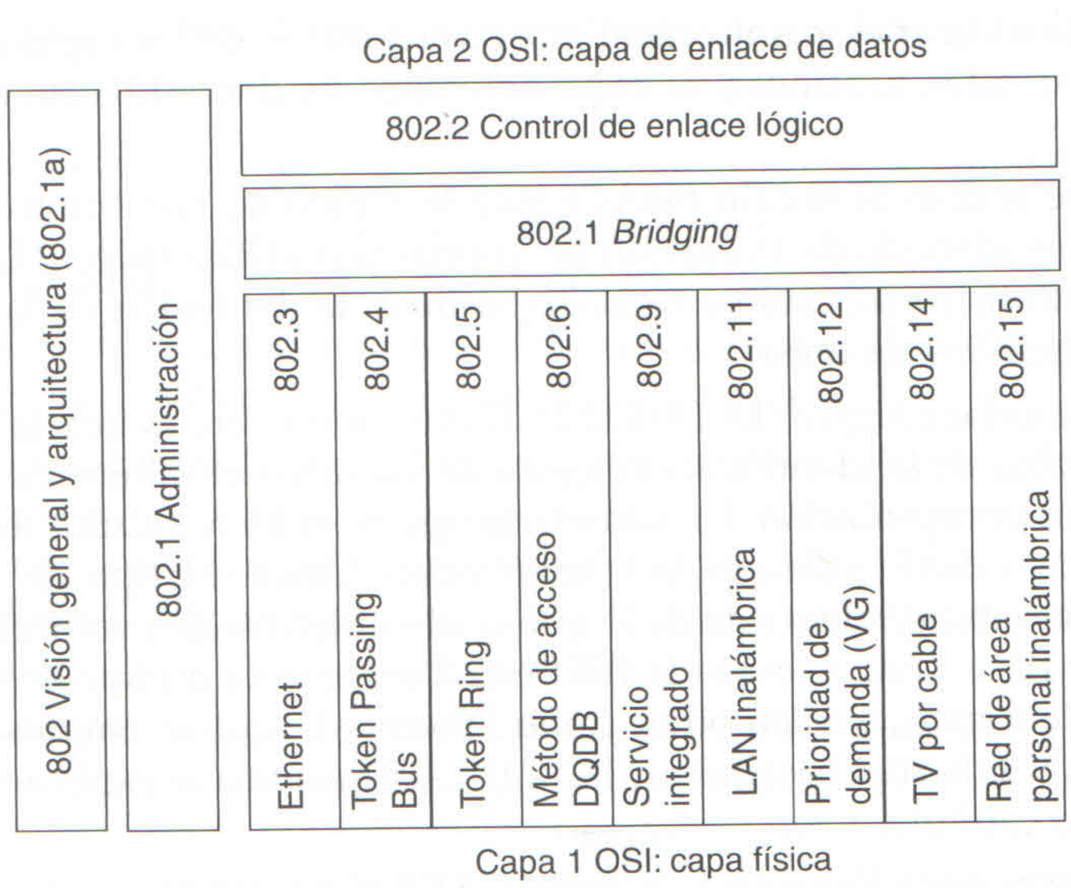

Figura 5.2. Especificaciones LAN y el modelo OSI.

Tabla 5.1. Limitaciones de la Capa 1 frente a Soluciones de la Capa 2

Limitación de la capa 1	Solución de la capa 2
La capa 1 no puede comunicar con las capas de nivel superior.	La capa 2 comunica con las capas superiores a través de la subcapa LLC.
La capa 1 no puede identificar a las computadoras.	La capa 2 identifica las computadoras utilizando el esquema de direccionamiento MAC.
La capa 1 sólo puede describir flujos de bits.	La capa 2 utiliza las tramas para organizar o agrupar los bits. (Finalmente, este proceso proporciona una manera de que los bits confieran sentido.)
La capa 1 no puede decidir qué computadora va a transmitir datos binarios de un grupo que está intentando trasmitir al mismo tiempo.	La capa 2 utiliza la subcapa MAC para alcanzarlos.

Las subcapas de la capa 2, LLC y MAC, son convenios activos y vitales que hacen que la tecnología sea compatible y posibilitan la comunicación entre las computadoras. La subcapa MAC está comprometida con los componentes físicos que se van a utilizar para comunicar una información. Al igual que las otras capas, la LLC permanece relativamente independiente del equipo físico que se va a emplear para el proceso de comunicación. La LLC permite múltiples protocolos de capa 3, como IP e IPX, a los que soporta simultáneamente junto con varios tipos de tramas.

La Figura 5.3 muestra una gran variedad de tecnologías Ethernet en la mitad inferior de la capa 2 OSI, y en toda la capa 1. Aunque existen otras variedades de Ethernet, las descritas son las más empleadas y, por tanto, la base de este curso.

Subcapa de control de enlace lógico 802.3 Control de acceso al medio									
Capa de señalización física	10BASE5 (500 m) 50 Ohm Coaxial N-Style	10BASE2 (185 m) 50 Ohm Coaxial BNC	10BASE-T (100 m) 100 Ohm UTP RJ45	10BASE-TX (100 m) 100 Ohm UTP RJ45	100BASE-FX (228_412 m) MM Fibra SC	1000BASE-T (100 m) 100 Ohm UTP RJ45	1000BASE-SX (220-550 m) MM Fibra SC	1000BASE-LX (550-5000 m) MM Fibra S/C	10BASE-(Various) MM o Sm Fibra SC
Medio físico									

Figura 5.3. Tecnologías Ethernet y el modelo OSI.

Direccionamiento MAC

Para permitir la distribución local de tramas en Ethernet, debe haber un sistema de direccionamiento, o sea, un modo de nombrar las computadoras y las interfaces. Cada computadora tiene una manera única de identificarse, y en la red, tiene una dirección física. No debe haber en la red dos direcciones físicas iguales. Con el nombre de **Control de acceso al medio (MAC)**, la dirección física se ubica en la NIC. Otros términos para la dirección MAC son la dirección de hardware, la dirección de la NIC, la dirección de capa 2 y la dirección Ethernet.

Ethernet utiliza las direcciones MAC para identificar únicamente los dispositivos individuales. Cada dispositivo (PC, *router*, *switch*) con una interfaz Ethernet a la red LAN debe tener una dirección MAC; de cualquier otro modo, los otros dispositivos no podrían comunicarse con él. Una dirección MAC tiene una longitud de 48 bits, y se expresa con 12 dígitos hexadecimales. Los primeros seis dígitos, que están administrados por el IEEE, identifican al fabricante y al distribuidor, comprometiéndose así con el **identificador único de organización (OUI, *organizationally unique identifier*)**. Los seis dígitos restantes corresponden el número de serie de la interfaz, o cualquier otro valor administrativo de un distribuidor específico. A veces, a las direcciones MAC se les conoce como direcciones integradas (BIA, *burned-in addresses*) porque se graban en la memoria de sólo lectura (ROM) y se programan en la memoria de acceso aleatorio (RAM) cuando se inicia la NIC. La Figura 5.4 muestra el formato de una dirección MAC.

Sin las direcciones MAC, la LAN sería sólo un grupo de computadoras sin identificadores y sería imposible enviar una trama Ethernet. Por tanto, en la capa de enlace de datos, se añaden una **cabecera** y una **información final** a los datos de la capa superior. La cabecera y la información final contienen la información de control pensada para la entidad de la capa

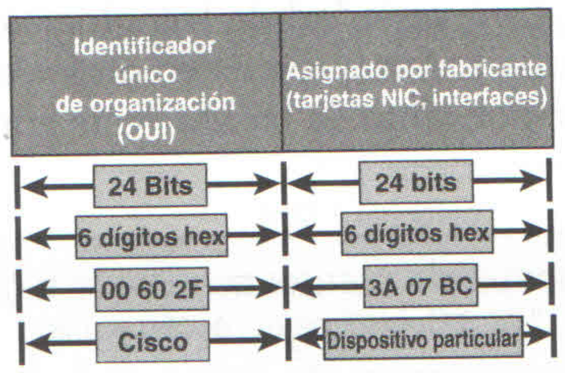

Figura 5.4. Formato de una dirección MAC.

de enlace de datos en el sistema de destino. Los datos de las entidades de capa superior encapsulan en la cabecera y en la información final de la capa de enlace de datos.

Las LAN Ethernet y 802.3 son redes de difusión. Todas las estaciones ven todas las tramas. Cada estación debe examinar cada trama para decidir qué estación va a ser el destino.

En una red Ethernet, cuando un dispositivo quiere enviar datos a otro, puede abrir una ruta de comunicación hasta el otro dispositivo empleando su dirección MAC. Cuando un dispositivo de origen envía datos a la red, éstos llevan la dirección MAC del destino que desean. Mientras esos datos se propagan a lo largo del medio de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección física de destino que lleva la trama de datos. Si no existe coincidencia, la NIC descarta la trama de datos.

Si hay coincidencia, la NIC verifica la dirección de destino en la cabecera de la trama para decidir dónde direccionar el paquete. Cuando los datos pasan su estación de destino, la NIC de esa estación hace una copia, saca los datos de su envoltorio y los entrega a la computadora para que ésta los procese mediante los protocolos de capa superior como IP y TCP.

Entramado en general

Los flujos de bits codificados en un medio físico representan un tremendo logro tecnológico, pero por sí solos, no son suficiente para que se produzca la comunicación. El entramado ayuda a obtener información esencial que no podría obtenerse tan sólo con los flujos de bits codificados. Éstos son algunos ejemplos de esta información:

- Qué computadoras se comunican con otras.
- Cuándo comienza y cuándo termina la comunicación entre computadoras.
- Reconocimiento de los errores ocurridos durante la comunicación.
- A cuál le toca el turno de "hablar" en una "conversación" entre computadoras.
- Dónde se ubican los datos en la trama.

Cuando tiene una manera de identificar las computadoras, puede moverse al entramado. El entramado es el proceso de encapsulación de la capa 2. Una trama es la unidad de datos del protocolo de capa 2. La Figura 5.5 ilustra los conceptos de bits y tramas.

Cuando trabaja con bits, el diagrama más adecuado que puede utilizar para visualizarlos es un gráfico que muestre el voltaje y el tiempo. Sin embargo, debido a que

malmente trabaja con una gran cantidad de datos e información sobre control y direccionamiento, este tipo de gráficos puede parecer ridículamente largo y confuso. Otro tipo de diagrama que puede emplear es el diagrama de formato de tramas, que está basado en gráficos de voltaje y tiempo. Se leen de derecha a izquierda, como el gráfico de un osciloscopio. El diagrama del formato de trama muestra diferentes agrupaciones de bits (campos); ciertas funciones están asociadas con diferentes campos.

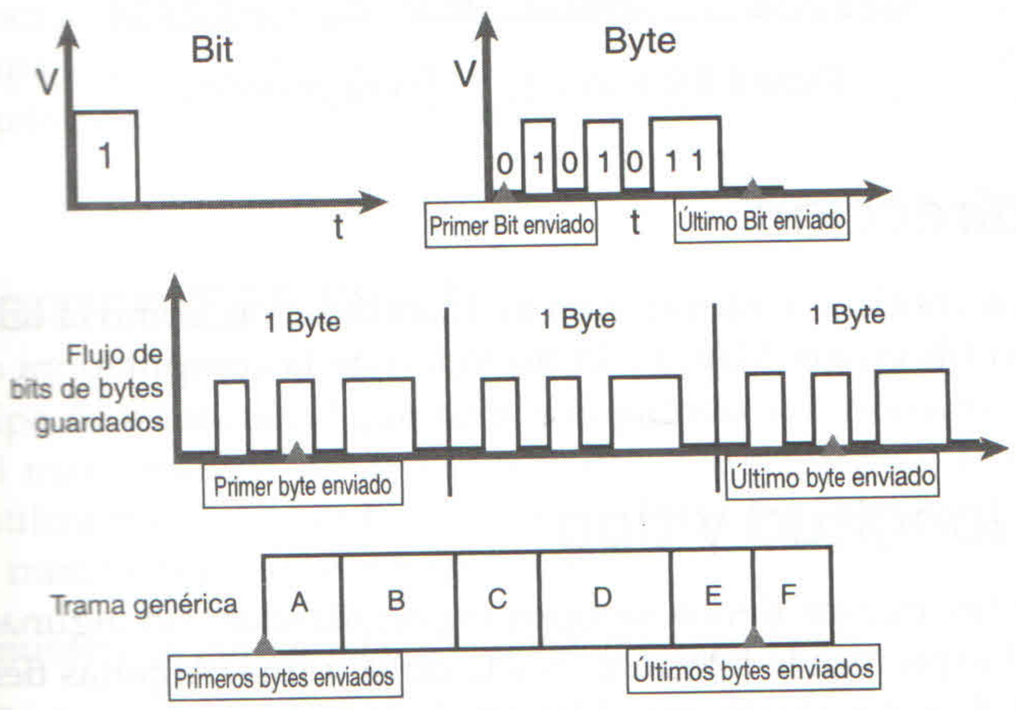

Figura 5.5. De los bits a la trama.

Las normas describen muchos tipos diferentes de tramas. Una trama genérica sencilla tiene secciones denominadas **campos**, que a su vez están compuestos por bytes (véase la Figura 5.6). Los nombres de los campos se encuentran normalmente en una trama de la capa de enlace de datos de la siguiente manera:

- Campo de inicio de la trama.
- Campo de dirección.
- Campo de longitud / tipo / control.
- Campo de datos.
- Campo de secuencia de verificación de trama (FCS, *Frame Check Sequence*).

Las siguientes secciones describen los diferentes campos de las tramas con más detalle.

Campo de inicio de trama

Cuando las computadoras están conectadas a un medio físico, debe haber una manera de que puedan recibir la atención de las otras computadoras para difundir un mensaje, como por ejemplo, "¡Aquí llega una trama!". Existen varias tecnologías que tienen diferentes modos de realizar este proceso, pero, a pesar de la tecnología, todas las tramas tienen una secuencia inicial de bytes de señalización.

Nombres de campo				
A	B	C	D	E
Campo de inicio de trama	Campo de dirección	Campo de longitud/ tipo/ control	Campo de datos	Campo FCS

Figura 5.6. Formato de trama genérico.

Campo de dirección

Todas las tramas contienen información de identificación, como la dirección de la computadora de origen (dirección MAC) y la dirección de la computadora de destino (dirección MAC).

Campos de longitud y tipo

La mayoría de las tramas tienen campos especializados. En algunas tecnologías, un campo de longitud especifica la longitud exacta de la trama. Algunas tienen un campo de tipo que especifica el protocolo de capa 3 haciendo la petición de envío. Existe también un grupo de tecnologías en las que no se emplea ningún campo.

Campo de datos

La razón del envío de tramas es la obtención de datos de la capa superior, los datos de la aplicación del usuario, de la computadora de origen a la computadora de destino. El paquete de datos que desea lanzar incluye el mensaje que quiere enviar (los datos). A veces se rellenan los bytes para que las tramas tengan una longitud mínima. Los bytes de control de enlace lógico (LLC) se incluyen también con los campos de datos en las tramas IEEE. Recuerde que la subcapa LLC añade información de control a los datos del protocolo de red, al paquete de capa 3, para ayudar a enviar ese paquete hacia su destino. La capa 2 se comunica con las capas superiores a través de la LLC.

Campo de secuencia de verificación de trama

Todas las tramas (y los bits, bytes y campos que los contienen) son susceptibles a errores de varias fuentes. El campo de secuencia de verificación de trama (FCS) contiene *un número basado en los datos de la trama; ese número lo calcula la computadora de origen*. Cuando la computadora de destino recibe la trama, vuelve a calcular el número FCS y lo compara con el número FCS incluido en la trama. Si son diferentes, se asume el error y se descarta la trama.

El número de la secuencia de verificación de trama se calcula normalmente mediante el uso de una verificación por redundancia cíclica (CRC, *Cyclic Redundancy Check*), que realiza cálculos polinómicos en los datos.

Estructura de tramas Ethernet

En la estructura de subcapa MAC, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet (10/100/1.000/10.000 Mbps). Gigabit Ethernet 1000BASE-T semidúplex y las versiones "W" de Ethernet a 10 Gb tienen ciertos problemas de temporización que necesitan menores diferencias a la hora de cómo manipular el espaciado entre tramas por la subcapa MAC, pero de todos modos, las velocidades son las mismas. Sin embargo, en la capa física, casi todas las versiones de Ethernet son sustancialmente diferentes unas de otras, y cada velocidad tiene su propio conjunto de reglas de diseño de arquitectura.

Trama Ethernet IEEE 802.3

Además del tipo de trama 802.2 que hemos explicado anteriormente, existe un tipo de trama IEEE 802.3 más sencillo, que fue el primero que desarrolló el IEEE. La 802.2, sin embargo, no se utiliza muy a menudo en las LAN Ethernet actuales. La Figura 5.7 muestra el formato de trama básico Ethernet IEEE 802.3.

La Tabla 5.2 enumera el número de octeto y el nombre de los campos de la trama Ethernet 802.3.

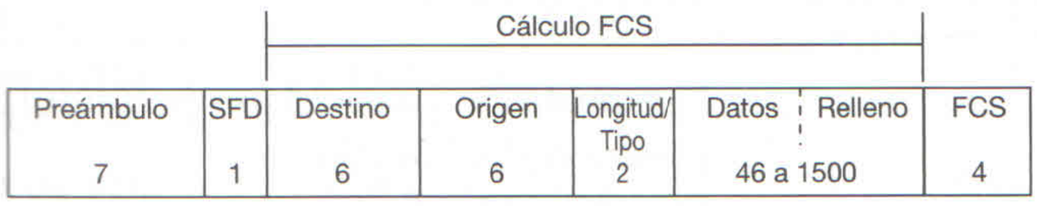

Figura 5.7. Estructura de trama Ethernet IEEE 802.3.

Tabla 5.2. Campos de la trama Ethernet IEEE 802.3

Octetos en cada campo de la trama	Campo de trama
	Preámbulo.
	Delimitador de trama de inicio (SFD).
	Dirección MAC de destino.
	Dirección MAC de origen.
	Campo de longitud/tipo (la longitud si es menor que 0600 en hexadecimal; si no, tipo de protocolo).
	Datos y relleno.
	Secuencia de verificación de datos (CRC; suma de comprobación).

Trama Ethernet II

En la versión DIX de Ethernet que se desarrolló antes de la adopción de la versión IEEE 802.3 de Ethernet, los campos preámbulo y delimitador de trama de inicio (SFD, *Start Frame Delimiter*) se combinaron en un solo campo, aunque los patrones binarios eran idénticos. El campo etiquetado como longitud/tipo fue enumerado sólo como longitud en las primeras versiones del IEEE y sólo como tipo en la versión DIX. Esos dos usos del campo fueron combinados oficialmente en una versión del IEEE posterior, ya que ambos usos del campo eran comunes en la industria. El primer formato de trama Ethernet DIX, también conocido como Ethernet Version2 o Ethernet II, es el tipo de trama más empleado con las LAN Ethernet basadas en TCP/IP. La Figura 5.8 ilustra el formato de trama Ethernet II.

Figura 5.8. Formato de trama Ethernet II.

La Tabla 5.3 lista el número de octeto y el nombre de los campos de la trama Ethernet II.

Tabla 5.3. Campos de la trama Ethernet II.

Octetos en cada campo de trama	Campo de trama
8	Preámbulo (finaliza en el patrón 10101011, el 802.3 SFD).
6	Dirección MAC de destino.
6	Dirección MAC de origen.
2	Campo tipo (46 a 1500 datos; si es menor de 46 octetos se debe añadir un relleno al final).
46 a 1500	Datos y relleno.
4	Secuencia de verificación de trama (CRC; suma de comprobación)

Como se indica en la Tabla 5.3, el uso del tipo de campo Ethernet II se incorpora a la actual definición de trama 802.3. Una estación debe determinar el protocolo de capa superior que está presente en la trama que llegue. Este principio se atiende examinando el campo longitud/tipo. Si el valor de dos octetos es igual o mayor que 600 hex, la trama es de acuerdo con el código de tipo Ethernet II indicado. Si es menor que 600 hex, la trama es una trama 802.3 y se indica su longitud. Se necesitan investigaciones posteriores para determinar su procedencia. Primero se examinan los primeros cuatro octetos del campo de datos 802.3. El valor que se encuentra se analiza para buscar dos únicos valores; si no están presentes, se supone que es una encapsulación (LLC) 802.2 de subcapa de control enlace lógico, y se decodifica de acuerdo con lo que indica la encapsulación LLC 802.2. Uno de los dos valores analizados es AAAA en hexadecimal, que indica una encapsulación

802.2/802 (protocolo de acceso de subred [SNAP, *Subnetwork Access Protocol*]). El otro valor que se comprueba es FFFF en hexadecimal, que puede indicar una encapsulación "en crudo" ("raw") IPX (Intercambio de paquetes entre redes) Novell antigua.

Campos de la trama Ethernet

La lista siguiente muestra la mayoría de los campos que permite o necesita la trama Ethernet 802.3. Vuelva a observar la Figura 5.8 para localizar una trama Ethernet 802.3:

- **Preámbulo**. Este campo contiene un patrón alternativo de 1 y 0 que se utilizó para la sincronización de tiempo en la asíncrona a 10 Mbps y en las implementaciones más lentas de Ethernet. Las versiones más rápidas de Ethernet son síncronas, por lo que la información de temporización es redundante, aunque se mantiene por razones de compatibilidad. El preámbulo tiene siete octetos de longitud y se representa mediante el siguiente patrón binario: 10101010 10101010 10101010 10101010 10101010 10101010 10101010.
- **Delimitador de trama de inicio (SFD)**. Es un campo de un octeto que marca el final de la información de temporización. Se representa mediante el patrón binario 10101011. En la primera forma DIX de Ethernet, este octeto era el último en el preámbulo de ocho octetos. Aunque el antiguo Ethernet DIX describe los primeros ocho octetos de manera diferente que Ethernet IEEE, el patrón y su uso son idénticos. También, la información de temporización que representa el preámbulo y el SFD se descarta, y no se cuenta como tamaño mínimo o máximo de trama.
- **Dirección de destino**. Este campo contiene los seis octetos de la dirección MAC de destino. La dirección de destino puede ser de unidifusión (nodo sencillo), multidifusión (grupo de nodos) o dirección de difusión (todos los nodos).
- **Dirección de origen**. Este campo contiene los seis octetos de la dirección MAC de origen. Esta dirección de origen se supone que es sólo la dirección de unidifusión de la estación Ethernet transmisora. Sin embargo, hay un número creciente de protocolos virtuales en uso, y que a veces emplean y comparten una dirección MAC de origen específica para identificar la entidad virtual.

  En las primeras especificaciones de Ethernet, las direcciones MAC fueron opcionalmente de dos o seis octetos, mientras el tamaño era constante a lo largo del **dominio de difusión**. El direccionamiento de dos octetos se excluyó primero explícitamente en el párrafo 3.2.3, en la versión de 1998 de la 802.3, y no fue soportado más en Ethernet 802.3.
- **Longitud/tipo**. Si el valor es menor que 1536 decimal (0600 hexadecimal), indica longitud. La interpretación de longitud se emplea donde la capa LLC proporciona la identificación del protocolo.
  - **Tipo (Ethernet)**. El tipo especifica el protocolo de capa superior que recibe al dato después de que se haya completado el procesamiento Ethernet.
  - **Longitud (IEEE 802.3)**. La longitud indica el número de bytes de datos que siguen a este campo. Si el valor es igual o superior a 1536 decimal (0600 hexadecimal), indica tipo, y el contenido del campo de datos lo decodifica el proto-

colo indicado. La RFC 1700 tiene una lista de protocolos Ethernet, aproximadamente en la página 168.

- **Datos y relleno**. Este campo puede ser de cualquier longitud que no provoque que la trama exceda su tamaño máximo. La **unidad máxima de transmisión (MTU, *maximun transmision unit*)** para Ethernet es de 1500 octetos, por lo que los datos no deben exceder este tamaño. El contenido de este campo está sin especificar. Se inserta un relleno sin especificar después de los datos del usuario cuando no existen datos del usuario suficientes para que la trama alcance su longitud mínima.

Las figuras de la estructura de una trama describen el campo de datos entre 46 y 1500 octetos. De hecho, Ethernet no especifica eso. La trama que se necesita es de 64 octetos o más de 1518 octetos, sin que se especifique realmente el tamaño del campo de datos. Esto deja al usuario que calcule el tamaño del campo de datos restando el resto de campos del tamaño de la trama. Si necesita seis octetos y emplea las direcciones MAC el tamaño del campo de datos será de entre 46 (rellenado, si lo necesita) y 1500 octetos.

— **Datos (IEEE 802.3)**. Después de haber completado el proceso de la capa física y la capa de enlace de datos, los datos se envían a un protocolo de la capa superior, que debe estar definido dentro de la porción de datos de la trama. Si los datos son insuficientes para llenar la trama en su tamaño mínimo de 64 bytes se insertan bytes de relleno para asegurar el tamaño mínimo de la trama.

- **Secuencia de verificación de trama (FCS)**. Esta secuencia contiene un valor CRC de 4 bytes creado por el dispositivo emisor, y el dispositivo receptor lo vuelve a calcular para comprobar daños en las tramas. El algoritmo matemático resultante de la verificación por redundancia cíclica (CRC) se coloca en el campo de cuatro octetos. La estación emisora calcula la suma total de la trama transmitida, y el valor resultante de los cuatro octetos se añade tras el campo de datos/relleno. La estación o estaciones receptoras realizan el mismo cálculo y comparan la nueva suma de comprobación con la suma de comprobación que se encuentra al final de la trama transmitida. Si coinciden las dos, la trama está bien. Los campos que se emplean en los cálculos lo incluyen todo, desde el comienzo de la dirección de destino hasta el final de los datos/relleno (véase la Figura 5.7). El preámbulo, que se muestra en la Figura 5.8, ilustra que el SFD y los campos de extensión no se incluyen en el cálculo. La FCS es el único campo Ethernet que se transmite en orden no canónico (primero MSB).

  Ya que la corrupción de un bit en cualquier parte desde el principio de la dirección de destino hasta el final del campo FCS hace que la suma de comprobación sea diferente, se autoincluye la cobertura del FCS. No es posible distinguir entre la corrupción de la FCS y la corrupción de cualquier campo precedente que se haya usado en el cálculo

Funcionamiento de Ethernet

Cuando varias estaciones (nodos) deben acceder a un medio físico y a otros dispositivos de red, se emplean varias estrategias de control de acceso al medio. Esta sección explica brevemente las estrategias de control del acceso, centrándose en el método de control del acceso Ethernet (CSMA/CD).

Debe saber que aunque CSMA/CD tiene una importancia histórica y práctica tremenda en la Ethernet original , su implementación está disminuyendo por dos motivos:

- Cuando se utiliza UTP de cuatro pares, existen pares de hilos separados para la transmisión (Tx) y para la recepción (Rx), resultando un UTP de cobre potencialmente libre de colisiones y capaz de realizar la operación dúplex, dependiendo de si se despliega en un entorno compartido (hub) o conmutado.
- Una lógica similar se aplica a los enlaces de fibra óptica, donde se emplean rutas ópticas separadas (una fibra de transmisión y otra de recepción).

Una nueva forma de Ethernet (1000BASE-TX, Gigabit Ethernet por cable) utiliza los cuatro pares de hilos simultáneamente en ambas direcciones, dando como resultado una colisión permanente. En las antiguas formas de Ethernet, dicha colisión permanente imposibilitaba el trabajo del sistema. Aun en 1000BASE-TX, una circuitería sofisticada puede acomodar esta colisión permanente, lo que da como resultado un intento de obtener tantos datos como sea posible sobre UTP.

Control de acceso al medio

El control de acceso al medio (MAC) hace referencia a los protocolos que deciden a qué computadora se le permite transmitir datos en un entorno de medio compartido (dominio de colisión). MAC, con LLC, comprende la versión IEEE de la capa 2. MAC y LLC son subcapas de la capa 2. Existen dos extensas categorías de MAC:

- Determinista (por turnos).
- No determinista (el primero que llega, es el primero que se sirve).

Token Ring y FDDI son deterministas, y Ethernet/802.3 es no determinista (también conocida como probabilista).

Protocolos MAC deterministas

Los protocolos MAC deterministas emplean un modo de crear turnos. La transmisión de tokens (testigos) es un ejemplo de protocolo MAC determinista. Algunas tribus de indios nativos americanos tienen la costumbre de pasarse el "bastón que habla" durante sus reuniones. A cualquiera que tenga el bastón se le permite hablar. Cuando esa persona ha finalizado, se lo pasa a otra.

En esta analogía, el medio que se comparte es el aire, los datos son las palabras del orador, y el protocolo es la posesión del "bastón que habla". A este bastón también se le podría llamar *token*. Esta situación es similar al protocolo de enlace de datos que recibe el nombre de Token Ring. En una red Token Ring, los *hosts* se distribuyen formando un anillo (véase la Figura 5.9). Un *token* de datos especiales circula alrededor del anillo. Cuando un host quiere transmitir, toma un *token*, transmite los datos durante un tiempo limitado, y después coloca el *token* de nuevo en el anillo para que pueda seguir circulando, o para que otro *host* pueda tomarlo.

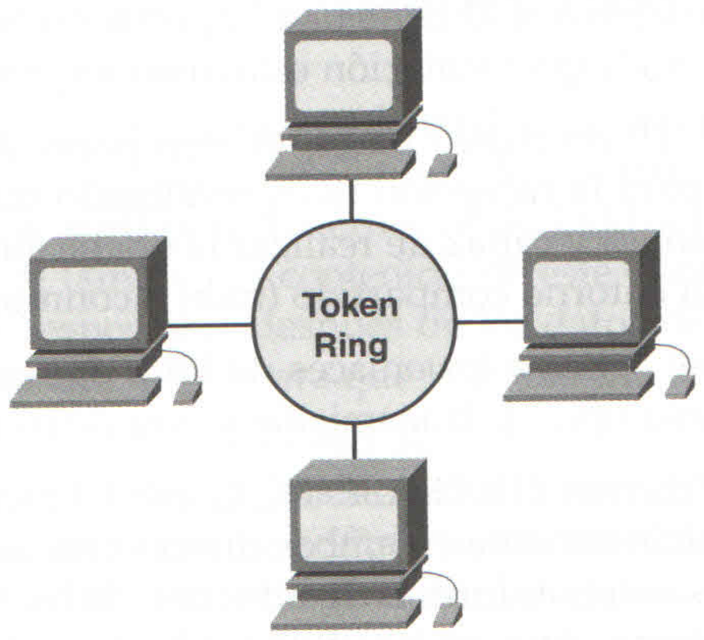

Figura 5.9. Una red Token Ring.

Protocolos MAC no deterministas

Los protocolos MAC no deterministas utiliza la norma de que el primero en llegar es el primero en ser servido (FCFS, *first-come first-served*). CSMA/CD es un ejemplo de protocolo MAC no determinista.

Para emplear esta tecnología de medio compartido, Ethernet permite que los dispositivos de red arbitren su derecho a transmitir. Las estaciones de una red CSMA/CD escuchan cuál es el mejor momento para transmitir. Sin embargo, si dos estaciones transmiten al mismo tiempo, se produce una colisión y ninguna de las transmisiones de las estaciones tiene éxito. El resto de las estaciones de la red escucha también la colisión y esperan en silencio. Las estaciones transmisoras, por turnos, esperan un periodo de tiempo aleatorio (periodo de retardo) antes de transmitir, minimizando así la probabilidad de una segunda colisión.

Tres implementaciones topológicas específicas y sus MAC

Tres tecnologías de capa 2 muy conocidas son Token Ring, FDDI y Ethernet. De ellas, Ethernet es la más común; sin embargo, todas sirven para ilustrar un método diferente de los requisitos LAN. Los tres especifican elementos de capa 2 (por ejemplo, LLC, denominación, entramado y MAC), además de componentes de señalización de capa 1 y cuestiones con los medios. Las tecnologías específicas para cada uno son las siguientes:

- **Ethernet**. Topología de bus lógica (la información fluye en un bus lineal) y estrella física o extendida (cableada como una estrella).
- **Token Ring**. Topología de anillo lógica (dicho de otro modo, la información fluye controlada en un anillo) y topología de estrella física (cableada en forma de estrella).
- **FDDI**. Topología de anillo lógica (la información fluye controlada en un anillo) y topología de anillo doble (cableada como un anillo doble).

Ethernet MAC

Ethernet es una tecnología de difusión de medio compartido. El método de acceso CSMA/CD que se emplea en Ethernet realiza tres funciones:

- Transmitir y recibir paquetes de datos.
- Decodificar paquetes de datos y comprobar las direcciones válidas antes de pasarlos a las capas superiores del modelo OSI.
- Detectar errores en los paquetes de datos o en la red.

En el método de acceso CSMA/CD, los dispositivos de red con datos para transmitir por los medios de red trabajan en modo "escuchar antes de transmitir" (CS = detección de portadora, *carrier sense*). En Ethernet compartida, esto significa que cuando un dispositivo quiere enviar datos, primero debe comprobar si el medio de red está ocupado. Después debe comprobar dónde hay señales en el medio de red. Y, finalmente, si el medio de red no está ocupado, comenzar a retransmitir los datos. Mientras transmite los datos en forma de señales, el dispositivo también escucha para asegurarse que ninguna otra estación está transmitiendo datos por el medio de red al mismo tiempo. Si esto sucediese, se produciría una colisión, como se muestra en la mitad superior de la Figura 5.10. Cuando ha finalizado su transmisión de datos, el dispositivo vuelve al modo de escucha. Con la Ethernet compartida tradicional, los dispositivos sólo pueden transmitir de uno en uno. Esto no sucede con la Ethernet conmutada, que explicaremos en el Capítulo 6.

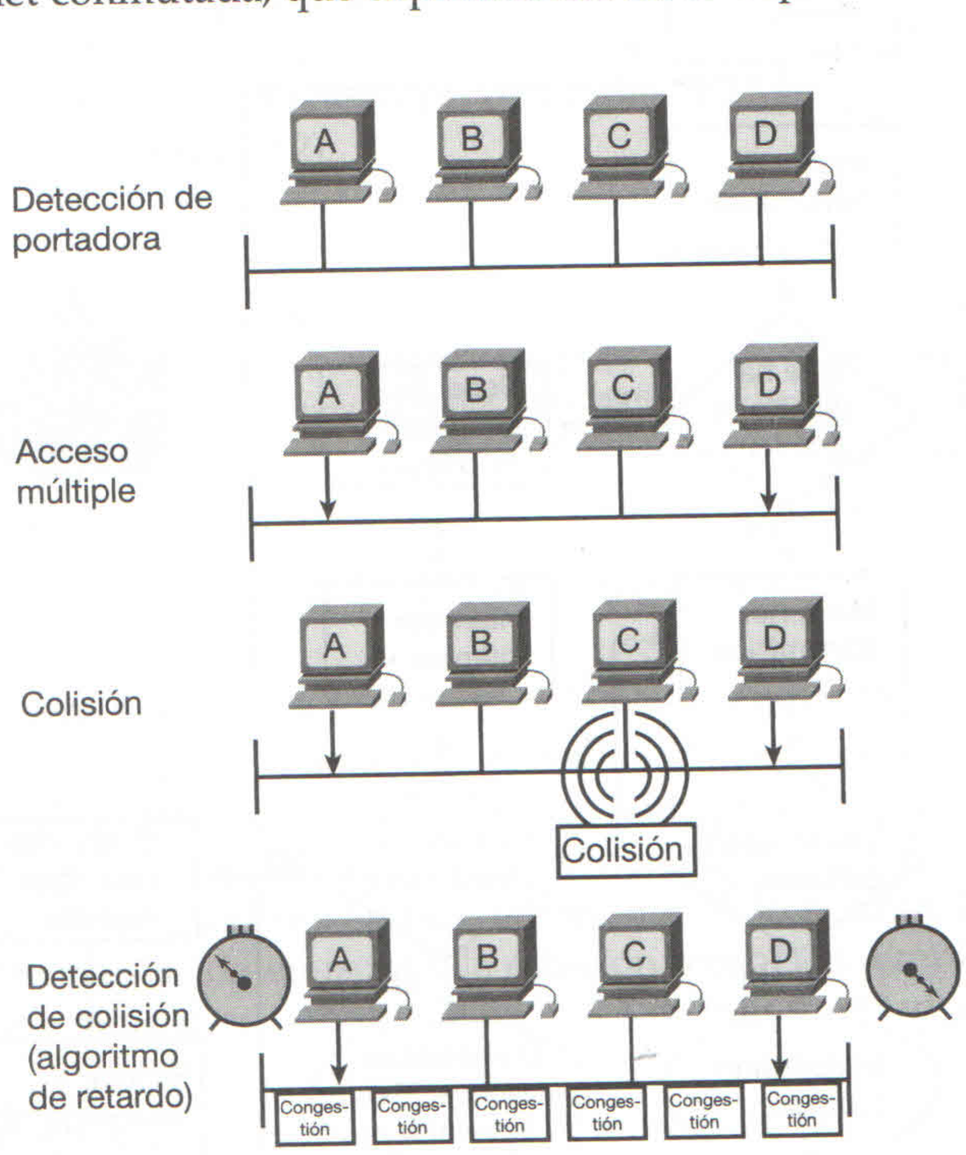

Figura 5.10. CSMA/CD.

Los dispositivos de red son capaces de detectar cuándo se ha producido una colisión, ya que aumenta la amplitud de la señal de los medios de red (CD = detección de colisión, *collision detect*). Cuando se produce una colisión, cada dispositivo que transmite continúa transmitiendo datos durante un corto espacio de tiempo, para asegurarse de que todos los dispositivos ven la colisión. Cuando todos los dispositivos la han visto, cada dispositivo transmisor llama a un algoritmo, conocido como **algoritmo de retardo**. Cuando todos los dispositivos de la red se han retardado durante cierto periodo de tiempo (aleatorio y, por tanto, diferente en cada uno de ellos), cualquier dispositivo puede intentar de nuevo el acceso a la red. Cuando la transmisión de datos continúa, los dispositivos que se han visto involucrados en la colisión no tienen prioridad para transmitir. La Figura 5.11 resume el proceso CSMA/CD.

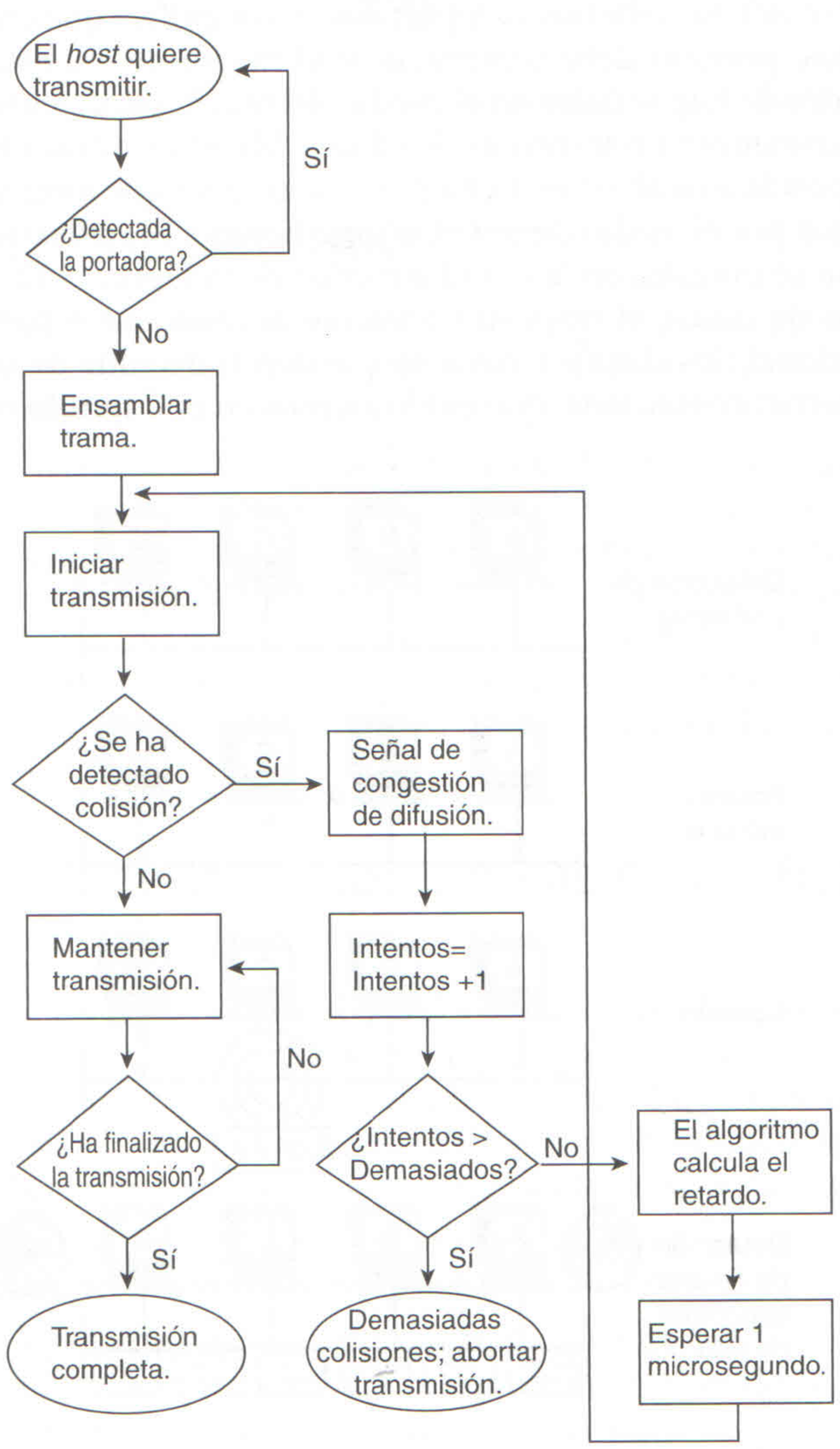

Figura 5.11. Proceso CSMA/CD.

Ethernet es una tecnología de transmisión por **difusión**. Esto quiere decir que todos los dispositivos de una red pueden ver todas las tramas que pasan por los medios de red. Sin embargo, no todos pueden procesar datos. Sólo los dispositivos cuyas direcciones MAC coinciden con las direcciones MAC de destino transportadas por las tramas copian la trama en su búfer. Ethernet no se preocupa de las direcciones de red de la capa 3, como IP o IPX. Si las direcciones MAC coinciden, se copia la trama y se deja pasar a la capa 3 para comprobar si coinciden la dirección de destino IP o la dirección IPX.

Después de que el dispositivo ha verificado la dirección de destino MAC y la dirección IP que llevan los datos, comprueba si hay errores en el paquete da datos. Si el dispositivo detecta errores, el paquete de datos se descarta. El dispositivo de destino no notifica al dispositivo de origen, sin importarle si el paquete ha llegado con éxito. Ethernet es una arquitectura de red **sin conexión** y se conoce como sistema de máximo esfuerzo de entrega.

Funcionamiento unidireccional, semidúplex y dúplex

Los canales de datos por los que se envían las señales sólo pueden operar de tres modos: unidireccional, semidúplex o dúplex. Se distinguen entre ellos por cómo viaja una señal.

La **transmisión unidireccional**, como su nombre indica, es sencilla. Se llama unidireccional porque la señal sólo viaja en una dirección, como el tráfico fluye por una calle de sentido único. La transmisión de la televisión o la radio son ejemplos de comunicaciones unidireccionales (véase la Figura 5.12).

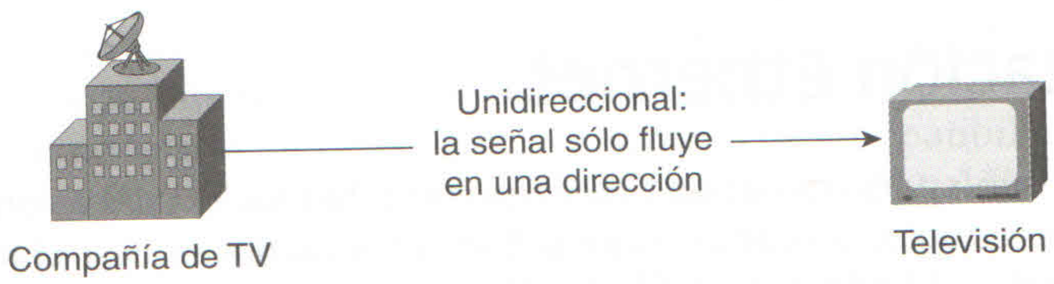

Figura 5.12. Transmisión unidireccional.

La **transmisión semidúplex** es una mejora de la transmisión unidireccional; el tráfico puede viajar en ambas direcciones. La transmisión semidúplex permite que las señales viajen en cualquier dirección, pero no ambas al mismo tiempo, como puede ver en la Figura 5.13. Ethernet semidúplex, que se define en la Ethernet 802.3 original, sólo utiliza un hilo, con una señal digital que lo recorre en ambas direcciones. Esto permite la transmisión sólo en una dirección entre la estación emisora y la estación receptora. Emplea también el protocolo CSMA/CD para ayudar en la prevención de colisiones y retransmitir si es que ocurren.

La **transmisión dúplex**, como puede ver en la Figura 5.14, funciona como una calle de dos direcciones. El tráfico puede viajar en ambas direcciones al mismo tiempo. El funcionamiento de Ethernet dúplex es posible utilizando la tecnología de conmutación, que se

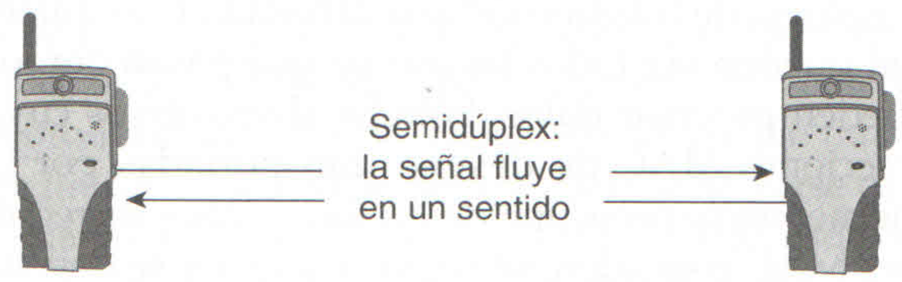

Figura 5.13. Transmisión semidúplex.

explica en profundidad en el Capítulo 6. La tecnología de red dúplex conmutada aumenta el rendimiento porque los datos se pueden enviar y recibir al mismo tiempo. Ethernet dúplex usa dos pares de hilos, que permiten la transmisión simultánea de datos entre la estación emisora y la estación receptora. No sucede ninguna colisión en Ethernet dúplex porque la tecnología de conmutación crea un circuito virtual de dos estaciones punto a punto, o "microsegmentos", cuando dos dispositivos necesitan comunicarse. Se supone que Ethernet dúplex ofrece el 100% de eficacia en ambas direcciones. Esto quiere decir que puede obtener 20 Mbps con Ethernet a 10 Mbps en una operación dúplex. Un *switch* a 100 Mbps puede ofrecer 200 Mbps a una estación en el modo dúplex.

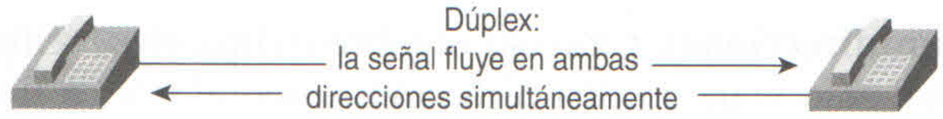

Figura 5.14. Transmisión dúplex.

Temporización Ethernet

Ethernet se diseñó para operar en una estructura de bus, lo cual es una manera técnica de decir que cada estación siempre escucha todos los mensajes casi al mismo tiempo. La designación oficial es CSMA/CD. CSMA/CD se puede interpretar de un modo sencillo diciendo que cuando dos estaciones se dan cuenta que están hablando al mismo tiempo, se supone que tienen que parar y esperar cierto periodo de tiempo antes de intentarlo otra vez.

Las reglas y especificaciones básicas para la instalación adecuada de Ethernet no son complejas, aunque algunas de las implementaciones más rápidas de la capa física llegan a serlo. A pesar de su simplicidad básica, cuando sucede algún problema en Ethernet a menudo es difícil aislar la fuente de dicho problema. Debido a la arquitectura de bus común de Ethernet (que se puede describir como un punto de fallo distribuido), el impacto del problema está normalmente en todas las estaciones del dominio de colisión que están conectadas al segmento. Cuando se utilizan repetidores, pueden incluirse estaciones de hasta cuatro segmentos.

Según las normas, cualquier estación de una red Ethernet que quiere transmitir un mensaje, primero escucha para asegurase que no hay ninguna otra estación transmitiendo

en ese momento. Si el cable está tranquilo, la estación comienza su transmisión de inmediato. Pera como las señales eléctricas necesitan una pequeña cantidad de tiempo para viajar a través del cable (se llama **retardo de propagación**), y cada repetidor que encuentren introduce una pequeña latencia en el envío de la trama de un puerto al siguiente, es posible que más de una estación comience a transmitir al mismo tiempo, provocando una colisión.

Si la estación conectada opera en modo dúplex, puede enviar y recibir simultáneamente, por lo que no debería haber colisiones. La operación dúplex elimina también las consideraciones de la temporización y el concepto de tiempo de ranura (*slot time*). Esta operación también permite los diseños de grandes arquitecturas de red, ya que se han eliminado las restricciones de la temporización para la detección de colisiones.

En la operación semidúplex, suponiendo que no ocurre ninguna colisión, la estación emisora transmite 64 bits de información para la sincronización de la temporización, que a menudo se conoce como preámbulo. Su contenido es el siguiente:

- Información de direccionamiento MAC de origen y de destino.
- Cierta información de cabecera.
- La carga útil actual de los datos.
- Una suma de comprobación (FCS) utilizada para asegurarse de que el mensaje no se ha dañado por el camino.

Las estaciones que reciben la trama recalculan la FCS para decidir si el mensaje entrante es válido, y entregan mensajes válidos a la siguiente capa superior en la pila de protocolos.

Para Ethernet a 10 Mbps y versiones más lentas, que son asíncronas, cada estación receptora usa los ocho octetos de la información de temporización para sincronizar su circuito de recepción para los datos y entonces descartarlos. Las implementaciones de alta velocidad a 100 Mbps de Ethernet son síncronas, por lo que la información de temporización no es realmente necesaria. Sin embargo, por razones de compatibilidad, el preámbulo y el SFD están presentes. Toda la información que sigue al SFD al final de la información de temporización se pasa a la siguiente capa superior. Se calcula una nueva suma de comprobación y se compara con la suma de comprobación que se encuentra la final de la trama recibida. Si la trama está intacta, se debe interpretar de acuerdo con las reglas para cualquier protocolo indicado por el campo longitud/tipo o el protocolo de capa LLC que indican los primeros octetos de los datos.

En las versiones de 1998 y 2000 se introdujeron un gran número de cambios en la estructura básica de la norma Ethernet. Un cambio significativo fue la exclusión de las direcciones de dos octetos, aunque fueron incluidas en todas las versiones anteriores. El valor máximo para el campo longitud/tipo 802.3 cuando se emplea para la longitud fue especificado como 1536 (600 hex), cuando antes se había asumido que coincidiese con el tamaño máximo de los datos MTU, que es de 1500 (5DC hex).

Para todas las velocidades de transmisión Ethernet a, o por debajo de, 1000 Mbps, la norma describe cómo la transmisión no puede ser menor que el tiempo de ranura. El tiempo de ranura para Ethernet a 10 y 100 Mbps es de 512 tiempos de bit (64 octetos). El tiempo de ranura para Ethernet a 1000 Mbps es de 4096 tiempos de bit (512 octetos, incluyen-

do la extensión). No se ha definido el tiempo de ranura para Ethernet a 10 Gbps porque no permite la operación semidúplex. El tiempo de ranura es mayor que el mayor tiempo de retardo de ida y vuelta posible cuando se emplea la máxima longitud del cable en la arquitectura de red válida más larga, y todos los tiempos de retardo de propagación del hardware tienen un máximo válido; la señal de congestión (*jam*) de 32 bits se emplea cuando se detectan colisiones. Es decir, el tiempo de ranura es mayor que el tiempo que teóricamente se necesita para ir desde un extremo a otro en el dominio de colisión Ethernet válido más largo, chocar con otra transmisión en el menor instante posible y, después, hacer que retornen los fragmentos de la colisión hasta la estación emisora para que los detecte. Para que el sistema funcione, la primera estación debe enterarse de la colisión antes de que termine de enviar la trama válida más pequeña. Para permitir que Ethernet a 1000 Mbps opere en semidúplex, se añade el campo de extensión cuando se envían las tramas pequeñas, sencillamente para mantener al transmisor lo suficientemente ocupado mientras regresa el fragmento de colisión. Este campo se presenta sólo en enlaces semidúplex a 1000 Mbps, y permite que las tramas con un tamaño mínimo de 64 octetos se estiren hasta coincidir con las peticiones de tiempo de ranura. La estación receptora descarta los bits de la extensión.

Para examinar este elemento brevemente, considere lo siguiente: en Ethernet a 10 Mbps, 1 bit en la subcapa MAC necesita 100 nanosegundos (ns) para transmitir. A 100 Mbps, el mismo bit necesita 10 ns para transmitir, y a 1000 Mbps, sólo necesita un 1 ns. La Tabla 5.4 resume los diferentes tipos de tiempo de bit de Ethernet.

Tabla 5.4. Tiempo de bit.

Velocidad Ethernet	Tiempo de bit
10 Mbps	100 nanosegundos
100 Mbps	10 nanosegundos
1000 Mbps = 1 Gbps	1 nanosegundo
10.000 Mbps = 10 Gbps	0,1 nanosegundo

Como estimación, se utilizan 8 pulgadas (20,3 cm) por nanosegundo para calcular el retardo de propagación en un cable UTP. Para 100 m de UTP, esto significa que está por debajo exactamente 5 tiempos de bit para que una señal 10BASE-T recorra una longitud de 100 m de cable (casi 4,92 tiempos de bit). Moviendo simplemente la coma decimal obtenemos 49,2 tiempos de bit a 100 Mbps, y 492 tiempos de bit a 1000 Mbps.

Para que funcione Ethernet CSMA/CD, la estación emisora debe ser consciente de la colisión antes de que se haya completado la transmisión de una trama de tamaño mínimo. A 100 Mbps, la temporización del sistema apenas es capaz de acomodar cables de 100 m. A 1000 Mbps, se necesitan ajustes especiales (muy poco eficientes) porque se ha transmitido una trama de tamaño mínimo antes de que el primer bit alcanzase el extremo de los primeros 100 metros de cable UTP. Es fácil ver por qué el modo semidúplex no está permitido en Ethernet a 10 GB.

Espacio intertrama y retardo

La Tabla 5.5 muestra el espacio mínimo entre dos paquetes que no chocan, conocido también como espacio intertrama, desde el último bit del campo FCS de la primera trama hasta el primer bit del preámbulo de la segunda trama.

Tabla 5.5. Espacio intertrama.

Velocidad	Espacio intertrama	Tiempo que necesita
10 Mbps	96 tiempos de bit	9,6 µsec
100 Mbps	96 tiempos de bit	0,96 µsec
1 Gbps	96 tiempos de bit	0,096 µsec
10 Gbps	96 tiempos de bit	0,0096 µsec

Después de haber enviado una trama, a todas las estaciones Ethernet a 10 Mbps se les pide que esperen un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir de forma válida la siguiente trama. En las versiones más rápidas de Ethernet, el espacio no varía: 96 tiempos de bits. Sin embargo, el tiempo necesario para que ese intervalo aumente es el más pequeño que le corresponda (véase la Tabla 5.6). Este intervalo alternativo que se conoce como espacio intertrama, hueco intertrama y hueco interpaquete, está pensado para dejar a las estaciones lentas tiempo para procesar la trama anterior y prepararse para la siguiente.

Tabla 5.6. Parámetro del tiempo de ranura.

Velocidad	Tiempo de ranura*	Intervalo de tiempo
10 Mbps	512 tiempos de bit	51,2 µsec
100 Mbps	512 tiempos de bit	5,12 µsec
1 Gbps	4096 tiempos de bit	4,096 µsec
10 Gbps	No se aplica	—

*El tiempo de ranura sólo se aplica en enlaces semidúplex Ethernet.

Sin embargo, se espera que un repetidor regenere los 64 bits de la información de temporización (preámbulo y SFD) en el inicio de cualquier trama, sin importar la pérdida potencial de alguno de los bits del preámbulo del comienzo para reducir la sincronización. De esta manera, al forzar la reintroducción de los bits de temporización, no sólo se puede hacer una pequeña reducción en el hueco intertrama, sino que se espera. Algunos conjuntos de chips Ethernet son sensibles al acortamiento del espacio intertrama y comienzan a fallar mientras se reduce el hueco. Con el incremento de potencia de proceso, sería muy fácil para una computadora personal saturar un segmento Ethernet con tráfico antes de que se consuma el tiempo de retardo del espacio intertrama. Con los años, algunos fabricantes han reducido deliberadamente el hueco intertrama para mejorar los resultados de las pruebas de

do la extensión). No se ha definido el tiempo de ranura para Ethernet a 10 Gbps porque no permite la operación semidúplex. El tiempo de ranura es mayor que el mayor tiempo de retardo de ida y vuelta posible cuando se emplea la máxima longitud del cable en la arquitectura de red válida más larga, y todos los tiempos de retardo de propagación del hardware tienen un máximo válido; la señal de congestión (*jam*) de 32 bits se emplea cuando se detectan colisiones. Es decir, el tiempo de ranura es mayor que el tiempo que teóricamente se necesita para ir desde un extremo a otro en el dominio de colisión Ethernet válido más largo, chocar con otra transmisión en el menor instante posible y, después, hacer que retornen los fragmentos de la colisión hasta la estación emisora para que los detecte. Para que el sistema funcione, la primera estación debe enterarse de la colisión antes de que termine de enviar la trama válida más pequeña. Para permitir que Ethernet a 1000 Mbps opere en semidúplex, se añade el campo de extensión cuando se envían las tramas pequeñas, sencillamente para mantener al transmisor lo suficientemente ocupado mientras regresa el fragmento de colisión. Este campo se presenta sólo en enlaces semidúplex a 1000 Mbps y permite que las tramas con un tamaño mínimo de 64 octetos se estiren hasta coincidir con las peticiones de tiempo de ranura. La estación receptora descarta los bits de la extensión.

Para examinar este elemento brevemente, considere lo siguiente: en Ethernet a 10 Mbps, 1 bit en la subcapa MAC necesita 100 nanosegundos (ns) para transmitir. A 100 Mbps, el mismo bit necesita 10 ns para transmitir, y a 1000 Mbps, sólo necesita un 1 ns. La Tabla 5.4 resume los diferentes tipos de tiempo de bit de Ethernet.

Tabla 5.4. Tiempo de bit.

Velocidad Ethernet	Tiempo de bit
10 Mbps	100 nanosegundos
100 Mbps	10 nanosegundos
1000 Mbps = 1 Gbps	1 nanosegundo
10.000 Mbps = 10 Gbps	0,1 nanosegundo

Como estimación, se utilizan 8 pulgadas (20,3 cm) por nanosegundo para calcular el retardo de propagación en un cable UTP. Para 100 m de UTP, esto significa que está por debajo exactamente 5 tiempos de bit para que una señal 10BASE-T recorra una longitud de 100 m de cable (casi 4,92 tiempos de bit). Moviendo simplemente la coma decimal obtenemos 49,2 tiempos de bit a 100 Mbps, y 492 tiempos de bit a 1000 Mbps.

Para que funcione Ethernet CSMA/CD, la estación emisora debe ser consciente de la colisión antes de que se haya completado la transmisión de una trama de tamaño mínimo. A 100 Mbps, la temporización del sistema apenas es capaz de acomodar cables de 100 m. A 1000 Mbps, se necesitan ajustes especiales (muy poco eficientes) porque se ha transmitido una trama de tamaño mínimo antes de que el primer bit alcanzase el extremo de los primeros 100 metros de cable UTP. Es fácil ver por qué el modo semidúplex no está permitido en Ethernet a 10 GB.

Espacio intertrama y retardo

La Tabla 5.5 muestra el espacio mínimo entre dos paquetes que no chocan, conocido también como espacio intertrama, desde el último bit del campo FCS de la primera trama hasta el primer bit del preámbulo de la segunda trama.

Tabla 5.5. Espacio intertrama.

Velocidad	Espacio intertrama	Tiempo que necesita
10 Mbps	96 tiempos de bit	9,6 µsec
100 Mbps	96 tiempos de bit	0,96 µsec
1 Gbps	96 tiempos de bit	0,096 µsec
10 Gbps	96 tiempos de bit	0,0096 µsec

Después de haber enviado una trama, a todas las estaciones Ethernet a 10 Mbps se les pide que esperen un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier estación pueda transmitir de forma válida la siguiente trama. En las versiones más rápidas de Ethernet, el espacio no varía: 96 tiempos de bits. Sin embargo, el tiempo necesario para que ese intervalo aumente es el más pequeño que le corresponda (véase la Tabla 5.6). Este intervalo alternativo que se conoce como espacio intertrama, hueco intertrama y hueco interpaquete, está pensado para dejar a las estaciones lentas tiempo para procesar la trama anterior y prepararse para la siguiente.

Tabla 5.6. Parámetro del tiempo de ranura.

Velocidad	Tiempo de ranura*	Intervalo de tiempo
10 Mbps	512 tiempos de bit	51,2 µsec
100 Mbps	512 tiempos de bit	5,12 µsec
1 Gbps	4096 tiempos de bit	4,096 µsec
10 Gbps	No se aplica	—

*Tiempo de ranura sólo se aplica en enlaces semidúplex Ethernet.

Sin embargo, se espera que un repetidor regenere los 64 bits de la información de temporización (preámbulo y SFD) en el inicio de cualquier trama, sin importar la pérdida potencial de alguno de los bits del preámbulo del comienzo para reducir la sincronización. De esta manera, al forzar la reintroducción de los bits de temporización, no sólo se puede hacer una pequeña reducción en el hueco intertrama, sino que se espera. Algunos conjuntos de chips Ethernet son sensibles al acortamiento del espacio intertrama y comienzan a fallar mientras se reduce el hueco. Con el incremento de potencia de proceso, sería muy fácil para una computadora personal saturar un segmento Ethernet con tráfico antes de que se cumpla el tiempo de retardo del espacio intertrama. Con los años, algunos fabricantes han violado deliberadamente el hueco intertrama para mejorar los resultados de las pruebas de

rendimiento en comparaciones de productos competitivos. En buena parte, este tiempo en el espacio intertrama no ha causado problemas, aunque sí tiene potencial para hacerlo.

Después de producirse una colisión y de que todas las estaciones permitan que el cable se vuelva inactivo (cada una espera la totalidad del espacio intertrama), las estaciones que están en conflicto deben esperar un periodo de tiempo adicional (y potencialmente más largo progresivamente) antes de intentar retransmitir la trama conflictiva. El periodo de tiempo se ha diseñado intencionadamente para que sea semialeatorio y que dos estaciones no puedan demorarse la misma cantidad de tiempo antes de retransmitir; si no, el resultado sería más colisiones. Esto se consigue en parte expandiendo el intervalo del que es seleccionado el tiempo de retransmisión aleatorio en cada intento de retransmisión. El periodo de espera se mide en incrementos del parámetro de tiempo de ranura.

La retransmisión está controlada por esta fórmula:

$$0 = r < 2k$$

Donde r es un número aleatorio de tiempos de ranura y k es el número de intentos de retardo (hasta un máximo de 10 por valor de retardo). El tiempo de retardo se define como sigue:

$$r * \text{tiempo de ranura}$$

El número máximo total de intentos de retransmisión es 16, aunque el valor del retardo sigue siendo 10 para los siguientes intentos. La fórmula especifica el periodo de espera mínimo para un intento de retransmisión. Es bastante aceptable, aunque no necesariamente deseable, para una estación que introduce demoras extras que degradan su propio rendimiento.

Como ejemplo, tras la quinta colisión consecutiva sin ser capaz de poder transmitir la trama 10BASE-T actual, el tiempo de espera tiene un intervalo de demora aleatorio entre 0 y 32 tiempos de ranura ($0 = r < 25$). Si es reiterado, la demora puede ser un número aleatorio de 51,2 microsegundos, fluctuando de un reintento inmediato a otro hasta microsegundos después.

Si la subcapa MAC sigue sin poder enviar la trama después de 16 intentos, se genera un error en la capa superior siguiente. Es bastante extraño que esto suceda, y sólo bajo cargas de red muy extremas o cuando existiese un problema físico en la red.

En una situación especial, la subcapa MAC sufre fallos más frecuentes para enviar una trama a pesar de los 16 intentos, y normalmente el problema se encuentra en los entornos conmutados. Esto se conoce como efecto captura o efecto inanición del paquete. Cuando dos dispositivos (*switches*, estaciones o ambos) se conectan en modo semidúplex e intentan mandar un gran bloque de tráfico, es seguro que provocan una colisión. Cualquier estación que "gane" la primera transmisión tiene una gran posibilidad de transmitir en cada colisión subsiguiente. Suponga que ha tenido lugar una segunda colisión. La primera estación, que fue capaz de trasmitir la primera trama, selecciona de nuevo el retardo aleatorio de intervalos de tiempo de entre 0 y 1, mientras que ahora la segunda estación selecciona intervalos de tiempo de entre 0, 1, 2, y 3. Es muy probable que la primera estación seleccione de nuevo un tiempo de retardo más corto y sea capaz de transmitir. La primera estación probablemente gane la transmisión debido a 16 intentos consecutivos de la segunda. Ésta se rinde y descarta la trama, y registra un error de colisiones excesivo. Este tipo de errores se revela normalmente utilizando el **protocolo SNMP** (Protocolo simple de administración de redes) para preguntar a un puerto de *switch*, y a menudo se encuentra

...rte, este timo en el ...para hacerlo.

...rmitan que el cable ..., las estaciones que ...otencialmente más ...tiva. El periodo de ... que dos estaciones ...nitir; si no, el resul... ...ervalo del que se ha ...e retransmisión. El ...e ranura.

... de intentos de retar... ...e define como sigue...

...e el valor del retardo ...iodo de espera más... ...necesariamente dese... ...propio rendimiento...

...e poder transmitir la ...demora aleatoria de ...puede ser un núme... ...ediato a otro 16384...

...6 intentos, se rinde y ...e esto suceda, y sería ...a físico en la red.

...ntes para enviar una ...uentra en los enlaces ...del paquete. Cuando ... semidúplex e inter... ...a colisión. Cualquier ...lad de transmitir con... ...la colisión. La prime... ...nuevo el retardo ale... ...gunda estación selec... ...e la primera estación ...ransmitir. La primera ...secutivos de la segun... ...es excesivo. Este tipo ...(Protocolo simple de ...menudo se encuentra...

...fuso donde sólo hay un dispositivo conectado al puerto afectado. Como Ethernet es ...intrínsecamente a ráfagas, puede informar a los puertos con una utilización media relativamente baja.

Manipulación de errores

La más común (y normalmente la primera) condición de error en Ethernet es la colisión. Las colisiones son el mecanismo para resolver la contención en el acceso a la red. Estas colisiones proporcionan una manera simple, suave y de baja sobrecarga para que los nodos de la red arbitren la contención para los recursos de red. Cuando la red no puede operar adecuadamente debido a varios problemas, las colisiones pueden ser un gran impedimento para conseguir un funcionamiento de red útil. Las colisiones sólo son posibles en los segmentos semidúplex.

Las colisiones derrochan tiempo de dos maneras: en primer lugar, la pérdida del ancho de banda de la red es igual a la transmisión inicial y a la señal de congestión de la colisión. Se conoce como retardo de consumo, y afecta a todos los nodos de la red. Un retardo de consumo significativo puede reducir el rendimiento de la red. Tras cada intento de transmisión satisfactorio o fallido hay un tiempo de inactividad (periodo de retardo) para todas las estaciones, llamado espacio intertrama (o hueco intertrama), que impacta además en el rendimiento. El segundo tipo de retardo es el resultado de este algoritmo de retardo de la colisión. Los retardos no suelen ser muy largos.

La mayor parte de las colisiones se producen al principio de las tramas, antes del SFD, y no se reportan a las capas superiores, como si la colisión no hubiese ocurrido. Tan pronto como se detecta una colisión, la estación o estaciones de envío transmiten una señal de congestión de 32 bytes que implementa la colisión. Esto se hace para que todas las estaciones tengan la oportunidad de detectar la colisión si cualquier dato que se haya transmitido completamente está corrupto.

En la Figura 5.15, dos estaciones están escuchando para asegurarse que el cable está libre y pueden transmitir. La norma 802.3 proporciona límites "en el peor de los casos" en cualquier componente del sistema que pueda retrasar una señal. El máximo retardo de ida y vuelta para un dominio de colisión a 10 Mbps es de 512 tiempos de bit, un valor que determina el tamaño mínimo de la trama. La estación 1 es la primera estación en transmitir, por lo que esta estación envía la mayoría de los datos antes de detectarse la colisión. La estación 2 sólo es capaz de enviar unos cuantos bits antes e detectar la colisión.

Examine atentamente la Figura 5.15. La estación 1 puede transmitir un porcentaje significativo de la trama antes de que la señal alcance el último segmento de cable. La estación 2 no recibe el primer bit de la transmisión antes de comenzar la suya propia. La estación 2 sólo puede enviar varios bits antes de que la NIC sienta la colisión. Esta estación detiene inmediatamente la transmisión actual y reemplaza la señal de congestión de 32 bits en su lugar; después cesa todas las transmisiones. Durante la colisión y el evento de congestión que experimenta la estación 2, los fragmentos de la colisión rehacen su camino a través del dominio de colisión repetido hacia la estación 1. La estación 2 completa la transmisión de la señal de congestión de 32 bits y entra en silencio antes de que la colisión se vuelva propagar de nuevo a la estación 1. Ésta, todavía sin advertir la colisión, continúa

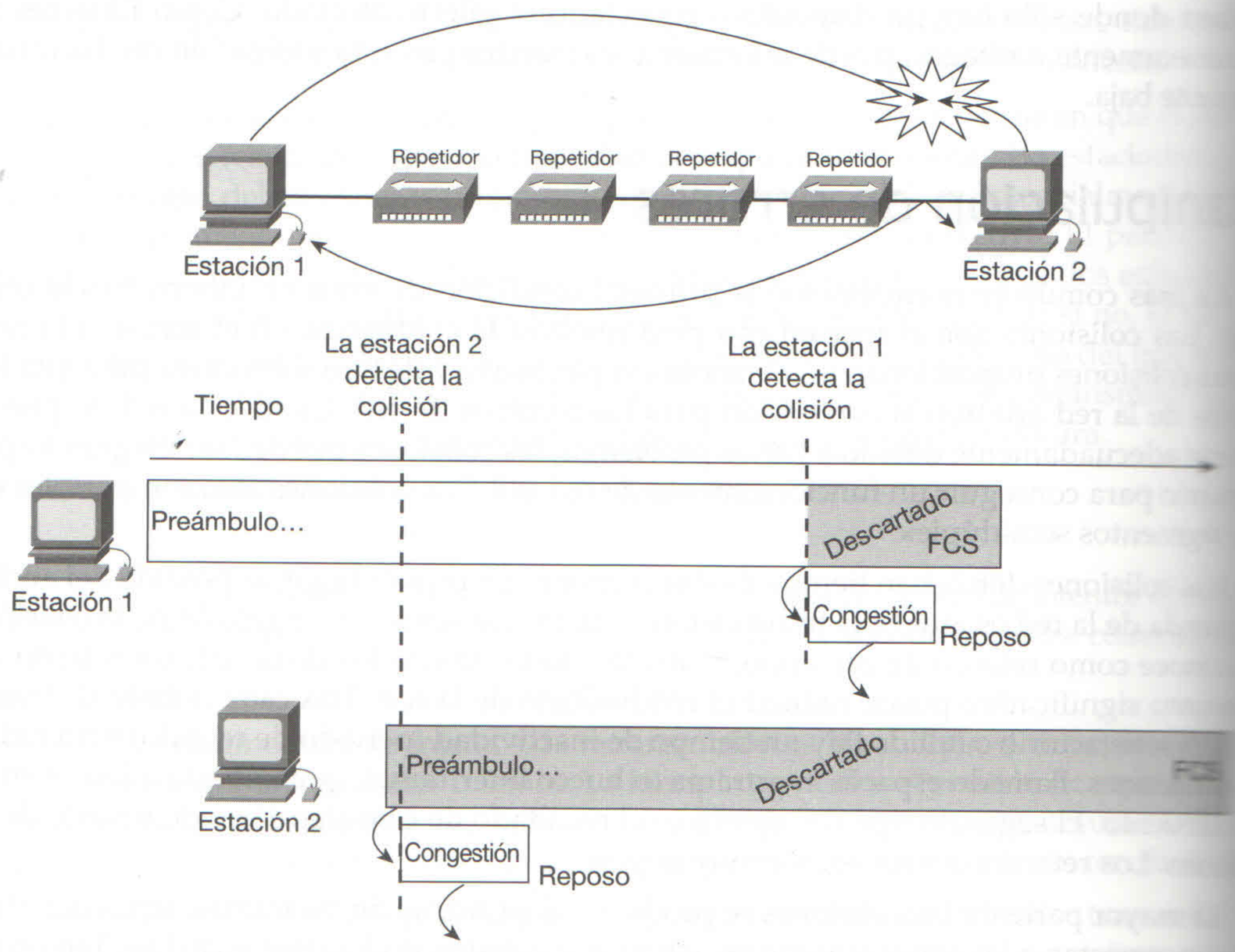

Figura 5.15. Manipulación rutinaria de errores en un dominio de colisión a 10 Mbps

trasmitiendo. Cuando los fragmentos de la colisión finalmente alcanzan la estación 1, ésta detecta la transmisión actual y reemplaza una señal de congestión de 32 bits en lugar del resto de la trama que se estaba transmitiendo. Una vez enviada la señal de congestión de 32 bits, la estación 1 cesa todas las transmisiones.

Una señal de congestión puede estar compuesta de datos binarios mientras no tenga una suma de comprobación para la porción de la trama que ya se ha transmitido. El patrón de datos que se observa más a menudo es un 1, 0, 1, 0 repetitivo, el mismo que el del preámbulo. Cuando lo visualiza un analizador de protocolos, este patrón aparece como una secuencia hexadecimal repetitiva de 5 ó A. A los mensajes corruptos, parcialmente transmitidos, se les llaman a menudo fragmentos de la colisión y, en ocasiones, coloquialmente, *runts*. Comparadas con las últimas colisiones, las colisiones normales tienen una longitud inferior a 64 octetos y, por tanto, ambas fallan la prueba de longitud mínima y de suma de comprobación FCS.

Tipos de colisiones

Las colisiones normalmente tienen lugar cuando dos o más estaciones Ethernet transmiten simultáneamente dentro de un dominio de colisión. La mayoría de las herramien

de diagnóstico informan de las colisiones mediante cómputos de eventos, pero también pueden informar de ellas de forma separada como colisiones sencillas, o como varias colisiones cuando a un *switch* u otra estación se le pregunta con SNMP. Una colisión sencilla es una colisión detectada mientras se intenta transmitir una trama, pero, al siguiente intento, la trama se ha transmitido bien. Varias colisiones indican que la misma trama colisiona repetidamente antes de ser transmitida correctamente. Esto es diferente para las tramas con transmisiones diferidas, porque la trama de la transmisión diferida no colisiona. El medio estaba ocupado cuando la estación o el *switch* pretendía transmitir, y se le pidió que esperase su turno. Debido a las repetidas colisiones de la misma trama, no pudo ser transmitida, y se informó que se abortó la transmisión debido a las repetidas colisiones.

El resultado de las colisiones (tramas parciales o totalmente corruptas que tienen menos de 64 octetos y un FCS no válido) se les llaman a menudo fragmentos de la colisión. Algunos analizadores de protocolo y monitores de red les llaman *runts*, pero es un término impreciso.

Los principales tipos de errores con tramas Ethernet que se pueden capturar mediante una sesión de análisis de protocolo son la colisión local, la colisión remota y la colisión atrasada. La Figura 5.16 ilustra estos tipos de colisiones. Las secciones que siguen describen brevemente cada tipo de error de trama.

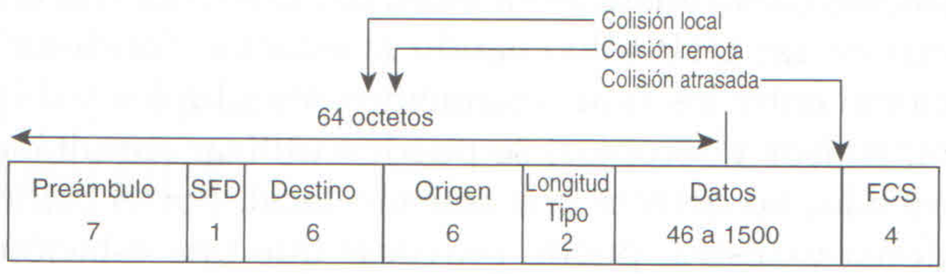

Figura 5.16. Resumen de los tipos de colisiones: local, remota y atrasada.

Colisión local

Para crear una colisión local en un cable coaxial (10BASE2 y 10BASE5), la señal viaja por el cable hasta que se encuentra una señal de otra estación. Las ondas entonces se solapan, cancelando algunas partes de la señal y reforzando (doblando) otras. El doblado lleva el nivel del voltaje más allá del máximo permitido. Todas las estaciones en el segmento de cable local sienten esta condición de sobretensión como una colisión. Un circuito especial en las NIC monitoriza esta condición de sobretensión. El umbral de la sobretensión está alrededor de los 1,5 voltios, medido en el cable coaxial. La Figura 5.17 muestra una trama media en colisión 10BASE2/10BASE5 capturada por el osciloscopio de almacenamiento digital.

En la Figura 5.17, el comienzo de una onda representa datos codificados Manchester normales. Unos cuantos ciclos en la muestra y la amplitud de la onda se dobla. Es el comienzo de la colisión, donde las ondas se solapan. Justo antes del fin de la muestra, la amplitud vuelve a la normalidad cuando la primera estación detecta la colisión y deja de transmitir, y se observa todavía una congestión de la segunda estación.

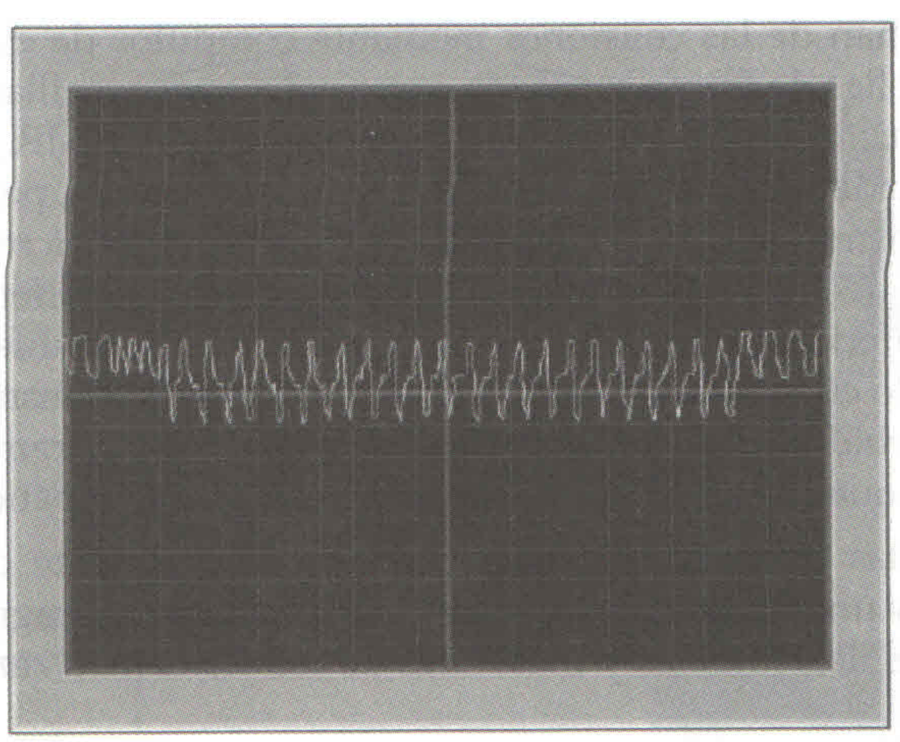

Figura 5.17. Colisión local 10BASE2/10BASE5.

En un cable UTP (como 10BASE-T, 100BASE-TX y 1000BASE-T), la colisión se detecta sólo en el segmento local cuando una estación detecta una señal en el par RX (recibir) al mismo tiempo que se envía por el par TX (transmitir). Como las dos señales están en pares diferentes, no hay cambios característicos en ellas, como se muestra en la Figura 5.17. Las colisiones se reconocen en un UTP sólo cuando la estación funciona en semidúplex. La única diferencia funcional entre los funcionamientos semidúplex y dúplex a este respecto es si ambos pares (transmisor y receptor) se pueden utilizar simultáneamente. Si la estación no está transmitiendo, no detecta una colisión local. Por el contrario, un fallo en el cable, como una diafonía excesiva, puede provocar que una estación perciba su propia transmisión como una colisión local.

Colisión remota

Las características de una colisión remota son una trama que tiene menos de la longitud mínima y tiene una suma de comprobación FCS no válida, y además no exhibe síntomas de colisión local, de sobretensión o de una actividad RX/TX simultánea. Esta clase de colisión se da como resultado de otras colisiones que suceden en un lado lejano de una conexión repetida. Un repetidor no enviará un estado de sobretensión y no puede hacer que una estación tenga activados los pares TX y RX al mismo tiempo. La estación tiene que transmitir para que los dos pares estén activados, y eso constituye una colisión local. En las redes UTP, es el caso más típico de colisión. Casi todas las herramientas de monitorización que informan de colisiones, como analizadores de protocolo software y pruebas de monitorización remota (RMON), sólo detectan las colisiones remotas porque son dispositivos de escucha pasivos.

Colisión atrasada

No existe ninguna posibilidad para una colisión normal después de que se hayan transmitido los primeros 64 octetos de datos por la estación o estaciones de envío. Los

ticos para los tiempos de propagación de red legales se han excedido antes. Las colisiones que ocurren después de los primeros 64 octetos se llaman colisiones atrasadas. La diferencia más significativa entre las colisiones atrasadas y las colisiones que se producen tras los primeros 64 octetos es que la NIC Ethernet transmite automáticamente una trama ficticia, pero no transmite automáticamente una trama que colisione más tarde. Respecto a la NIC, todo va bien, y las capas superiores de la pila de protocolos deben deducir que la trama se ha perdido. Aparte de la retransmisión, una estación que detecta una colisión atrasada la manipula del mismo modo que una colisión normal.

En todos los casos menos en uno, la norma 802.3 permite a una estación el intento de transmitir una trama que colisione más tarde, pero no lo necesita. Gigabit Ethernet niega explícitamente la transmisión de tramas atrasadas que colisionan.

Una colisión atrasada remota se produce después de que el tiempo de ranura ha transcurrido y en el lado lejano del repetidor. Sin embargo, como el repetidor debe prevenir la observación de los síntomas de colisión local de un estado de sobretensión o de eventos transmitir/recibir simultáneos, es necesaria una monitorización del hardware en el segmento distante para detectar una colisión atrasada y enviar la información a la estación que lo monitoriza. También puede deducir que una colisión atrasada remota ha tenido lugar en alguna parte del otro lado del repetidor analizando los últimos octetos de una trama en mal estado y buscando la presencia del patrón asociado a una señal de congestión. Normalmente, este tipo de colisiones se detecta en el segmento local sencillamente como un error FCS.

Errores Ethernet

¿Por qué aprender acerca de los errores Ethernet? Porque Ethernet es una tecnología LAN dominante y se necesita un conocimiento más profundo de los errores típicos para comprender el funcionamiento y la resolución de errores de Ethernet.

Mientras que las colisiones local y remota se consideran parte normal del funcionamiento de Ethernet, la colisión atrasada se considera un error. La presencia de errores en Ethernet garantiza una investigación en profundidad. La severidad del problema indica la urgencia de la resolución de problemas para resolver los errores detectados. Un puñado de errores detectados durante muchos minutos o muchas horas tiene baja prioridad. Cientos detectados en pocos minutos reclaman una atención urgente. Las situaciones que se consideran errores Ethernet son:

- La transmisión simultánea se produce antes de que el tiempo de ranura haya transcurrido (colisión o *runt*).
- La transmisión simultánea se produce después de transcurrido el tiempo de ranura (colisión atrasada).
- Transmisión excesiva o ilegalmente larga (error, trama larga y errores de rango).
- Transmisión ilegalmente corta (trama corta, fragmento de colisión o *runt*).
- Transmisión corrupta (error FCS).
- Número de bits transmitido insuficiente o excesivo (error de alineación).

- Desigualdad en el número de octetos de la trama actual y el informado (error de rango).
- Preámbulo inusualmente largo o evento de congestión (*ghost* o error).

Cada situación se define por separado. Normalmente, las tramas asociadas con condiciones de error se descartan, pero no siempre. Las colisiones normales se incluyen para proporcionar una lista más completa, pero actualmente no se consideran errores. Las secciones que siguen describen brevemente algunos de ellos.

Error (*jabber*)

El **error** se define en varios lugares de la norma 802.3 como una transmisión de al menos 20.000 a 50.000 tiempos de bit de duración. Sin embargo, la mayoría de herramientas de diagnóstico informan de un error cada vez que detectan una transmisión que exceda del tamaño máximo legal de la trama (que es considerablemente menor que los tiempos de bit de 20.000 a 50.000). Esto presenta una definición bastante complicada porque el dispositivo que informa **puede** o **no puede** considerar una trama de 1518 octetos con un etiquetado VLAN añadido, que es más larga que el límite legal. Además, no existe ninguna indicación de que el error tenga un FCS bueno o malo. La mayoría de referencias a errores se llaman más adecuadamente tramas largas.

Trama larga

Una **trama larga** es la que tiene una longitud mayor que el tamaño máximo legal y se supone que está etiquetada. Si no lo está, se supone que tiene una suma de comprobación FCS válida. Este error normalmente es significativo cuando alguien ha detectado un error en la red. La Figura 5.18 ilustra que una trama larga es mayor de 1518 octetos.

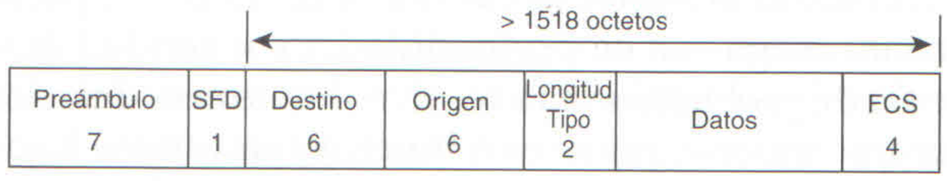

Figura 5.18. Trama larga.

Los errores y las tramas largas exceden ambos el tamaño máximo de la trama, aunque los errores sean bastante más largos. Si la trama está etiquetada como 802.1q, normalmente no se cuenta como longitud ilegal. La norma IEEE 802.1Q define el funcionamiento de los puentes LAN virtuales (VLAN) que permiten la definición, funcionamiento y administración de topologías VLAN dentro de una infraestructura LAN con puentes. La norma IEEE 802.1Q se desarrolló para lidiar con el problema de cómo romper redes largas en puentes más pequeñas para que el tráfico de multidifusión y difusión no ocupase más ancho de banda del necesario.

Trama corta

Una trama corta es una trama más pequeña que el tamaño mínimo legal de 64 octetos, con una buena secuencia de verificación de trama. Algunos analizadores de protocolo y monitores de red las llaman *runts*, pero este término es impreciso. En general, las tramas cortas no se suelen ver, y su presencia no garantiza que la red esté fallando.

Las tramas cortas están adecuadamente formadas en todos menos un aspecto, y tienen sumas de comprobación FCS válidas: sin embargo, son menores que el tamaño de trama mínimo (64 octetos). La Figura 5.19 ilustra una trama corta menor a 64 octetos.

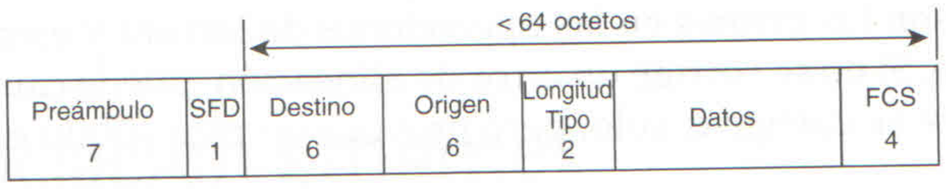

Figura 5.19. Trama corta.

Runt

El término ***runt*** es un término coloquial general e impreciso que significa algo que es menor que el tamaño de trama legal. Puede hacer referencia a tramas cortas con una suma de comprobación FCS válida. Normalmente se refiere a los fragmentos de la colisión. La norma Ethernet describe un atributo administrativo SNMP llamado *runt* que es un poco más grande que 74 tiempos de bit, pero menor que el tamaño mínimo de trama (64 octetos a velocidades de 10/100 Mbps, o el evento de transmisión mínimo semidúplex de 517 octetos a 1000 Mbps). **No es** una colisión local.

Errores FCS

Una trama que se recibe con una secuencia de comprobación de datos mala (también conocida como suma de comprobación o error CRC) tiene al menos 1 bit de diferencia respecto a cuando fue transmitida. En una trama con un error FCS, la información de cabecera probablemente sea correcta (el direccionamiento, etc.), pero la suma de comprobación calculada por la estación receptora no coincide con la suma de comprobación añadida al final de la trama por la estación emisora. Confiar en la exactitud del direccionamiento en una trama sencilla no es una buena idea, pero si muchas tramas tienen la misma dirección de origen, existe una buena posibilidad de que la dirección de origen sea correcta.

Un gran número de errores FCS procedentes de una sola estación indica normalmente una NIC defectuosa o controladores de software corruptos o defectuosos, o también una mala conexión de cable de la estación a la red. Los errores FCS se asocian con muchas estaciones, y generalmente se identifican por un mal cableado, una versión defectuosa de un controlador NIC, un puerto de *hub* defectuoso, o ruido inducido en el sistema de cables.

Los errores FCS se dan a conocer cuando por lo menos 1 bit de la transmisión es diferente. Cuando se calcula una nueva suma de comprobación en la estación receptora y se

compara con la suma de comprobación del campo FCS y no coinciden, la trama se descarta.

Error de alineación

Un mensaje que no finaliza en su límite de octetos se conoce como **error de alineación**. Es decir, en lugar del número correcto de bits binarios para formar grupos completos de octetos, faltan algunos bits adicionales (menos de ocho). Como una trama se trunca en el límite de octeto más cercano, si la suma de comprobación FCS falla, se informa de un error de alineación. A menudo esto se debe a controladores software en mal estado o a una colisión, y frecuentemente va acompañado también por un fallo en la suma de comprobación FCS. Otros motivos son los errores en las operaciones de lectura y escritura causados por errores en el software. Si no se corrige un error de alineación, puede causar una caída. Normalmente, el software se corrige el solo, pero provoca un pico súbito en los recursos de la CPU del *router*.

Error de rango

Una trama que tiene un valor de tamaño legal en el campo de longitud pero que no coincide con el número actual de octetos contados en el campo de datos de la trama recibida se conoce como **error de rango**. Este error aparece también cuando el valor del campo de longitud es menor que el mínimo legal del tamaño sin rellenar del campo de datos. Un error parecido, fuera de rango, se produce cuando el valor del campo de longitud indica un tamaño de datos demasiado largo para ser legal.

Ghost

Las redes *fluke* han acuñado el término ***ghost*** para referirse a la energía (ruido) que se detecta en un cable y que parece ser una trama pero sin un SFD válido. Para que se la clasifique como *ghost*, esa "trama" debe tener al menos 72 octetos de longitud (incluido el preámbulo); en caso contrario, se clasifica también como colisión remota. Debido a la particular naturaleza de los *ghosts*, es importante que observe que los resultados de los análisis dependen de donde se haga la medida del segmento.

Algunos tipos de ruido engañan a los nodos de un segmento de red y les lleva a pensar que han recibido una trama. Sin embargo, la trama percibida nunca aparece, por lo que no se pasa ningún dato a la NIC para su proceso. Tras un breve espacio de tiempo, la transmisión percibida cesa y la NIC continúa mandando sus mensajes. Las diferentes interfaces de red actúan de un modo diferente, y ninguna norma define cómo o cuándo debe reaccionar una NIC ante un segmento con ruido. Normalmente, los repetidores propagan dichas señales de ruido a otros segmentos del dominio de colisión.

Un síntoma visible de *ghosts* es una red que se ralentiza sin motivo aparente. Los servidores de archivos están ociosos, el equipo de monitorización de red muestra muy poca utilización de la misma y los usuarios se quejan de que la red va muy lenta o se ha venido abajo. Este síntoma puede estar limitado geográficamente, con un extremo en un segmento largo que parece estar operativo y el otro parece que va lento o que se ha venido abajo.

Los bucles a tierra y otros problemas de cableado normalmente son la causa de los *ghosts*. Éstos hacen que muchos repetidores respondan como si hubiesen recibido una trama. Como el repetidor reacciona sólo ante un voltaje AC del cable, no existe ninguna trama válida que pasar a los otros puertos. Sin embargo, el repetidor transmite su energía al resto de puertos. El *ghost* transmitido puede aparecer como un patrón de congestión o como un preámbulo muy largo.

La mayoría de herramientas de monitorización de red no reconocen la existencia de los *ghosts*, por la misma razón que no reconocen las colisiones de preámbulo (se basan completamente en lo que el conjunto de chips les cuenta). Los analizadores de protocolo exclusivamente software, muchos analizadores de protocolo basados en hardware, muchas herramientas de diagnóstico *hand-held* y la mayoría de pruebas RMON no informan de estos eventos.

Autonegociación Ethernet

Mientras Ethernet crecía de 10 a 100 y a 1000 Mbps, uno de los objetivos fue hacer cada tecnología interoperable, incluso hasta el punto de que las interfaces de 10, 100 y 1000 pudiesen estar conectadas directamente. Se desarrolló un proceso que se llama autonegociación (de velocidades y semidúplex o dúplex). Mientras se introducía Fast Ethernet, la norma incluía un método para configurar automáticamente una interfaz para que coincidiese en velocidad y capacidades con el socio de enlace. Este proceso define cómo dos socios de enlace pueden negociar automáticamente una configuración que ofrezca el mejor nivel de rendimiento común. Tiene la ventaja adicional de involucrar tan sólo a la parte más baja de la capa física.

10BASE-T necesita que cada estación transmita un pulso de enlace casi cada 16 milisegundos siempre que la estación no esté ocupada transmitiendo un mensaje. La autonegociación adopta esta señal y la renombra como pulso de enlace normal (NLP, *Normal Link Pulse*). Cuando se envían series de NLP en un grupo para la autonegociación, el grupo se llama ráfaga de pulso de enlace rápido (FLP, *Fast Link Pulse*). Cada ráfaga FLP se envía en el mismo intervalo de tiempo que un NLP y se ha proyectado para permitir que los dispositivos 10BASE-T antiguos operen con normalidad si reciben una de esas ráfagas. La figura 5.20 ilustra la temporización NLP y FLP.

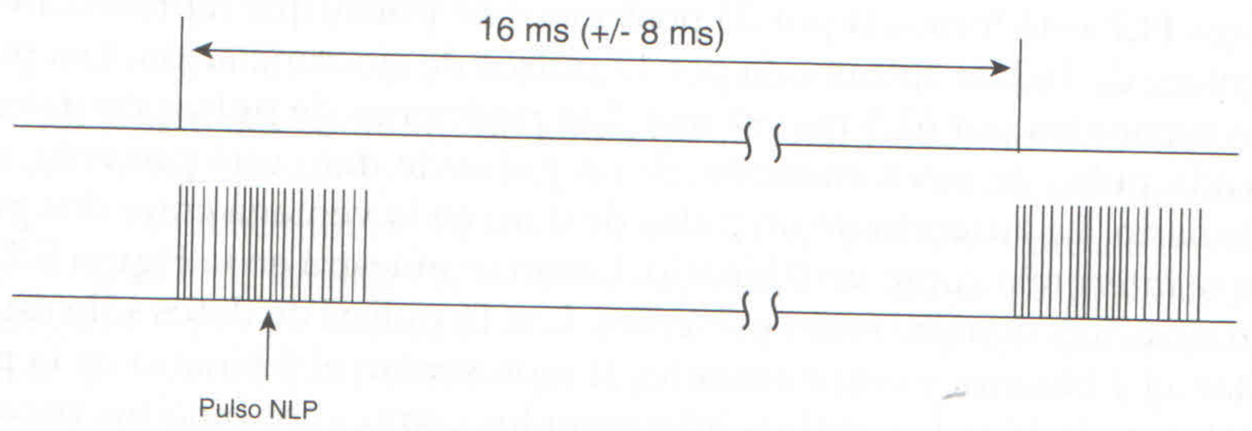

Figura 5.20. Temporización NLP frente a FLP.

Las transmisiones 10BASE-T utilizan una señalización entre +1 y –1 voltios, para una señal diferencial pico-a-pico de 2 voltios. La señalización NLP sólo usa un intervalo de +1 voltios. La duración de un pulso NLP es de 100 ns. La Figura 5.21 muestra dos pulsos NLP. El pulso de la izquierda es muy limpio y brusco, y es de una interfaz capaz de operar a 1000 Mbps. El pulso de la derecha es de un antiguo dispositivo capaz de operar únicamente a 10/100 Mbps, por lo que no necesita la precisión de una señal.

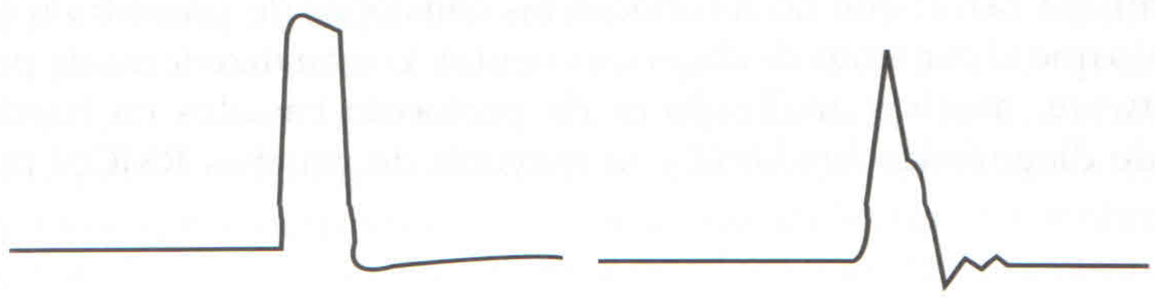

Figura 5.21. Pulsos NLP.

La autonegociación se consigue transmitiendo una ráfaga de pulsos de enlace 10BASE-T desde cada uno de los dos socios de enlace. La ráfaga comunica las capacidades de la estación de transmisión a su socio de enlace. Después de que las dos estaciones han interpretado lo que ofrece el otro socio, ambas cambian a la configuración común de mayor rendimiento y establecen un enlace a esa velocidad. Si algo interrumpe la comunicación y se pierde el enlace, los dos socios de enlace intentan primero enlazarse otra vez a la última velocidad negociada. Si esto falla, o si ha pasado mucho tiempo desde que se perdió el enlace, el proceso de autonegociación finaliza. El enlace se puede haber perdido por influencias externas, como un error en el cable, o debido a que uno de los socios envió un *reset*.

La Figura 5.22 muestra la ráfaga de autonegociación FLP actual. La ráfaga FLP está constituida por varios pulsos de enlace NLP.

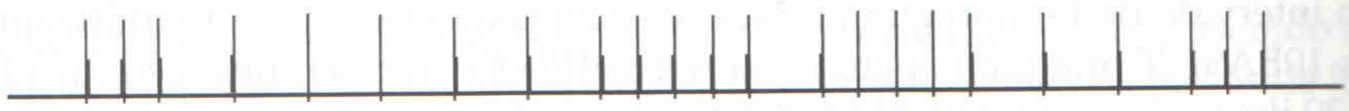

Figura 5.22. Ráfaga de autonegociación FLP.

Una ráfaga FLP está formada por 33 posiciones de pulso, que representan una palabra código de enlace de 16 bits entramada por 17 pulsos de sincronización. Los pulsos de una ráfaga están separados por 62,5 ms (±7 ms). Las posiciones de pulsos de datos se encuentran entre cada pulso de sincronización. Si un pulso de dato está presente, se interpreta como un 1 binario. La ausencia de un pulso de dato en la ventana entre dos pulsos de sincronización se interpreta como un 0 binario. Como se muestra en la Figura 5.23, los 17 pulsos de sincronización siempre están presentes. Los 16 pulsos de datos sólo están presentes si representan el 1 binario, y están ausentes si representan el 0 binario en la palabra codificada de datos de 16 bits. Los pulsos interpretados como unos binarios para los datos se resaltan en gris.

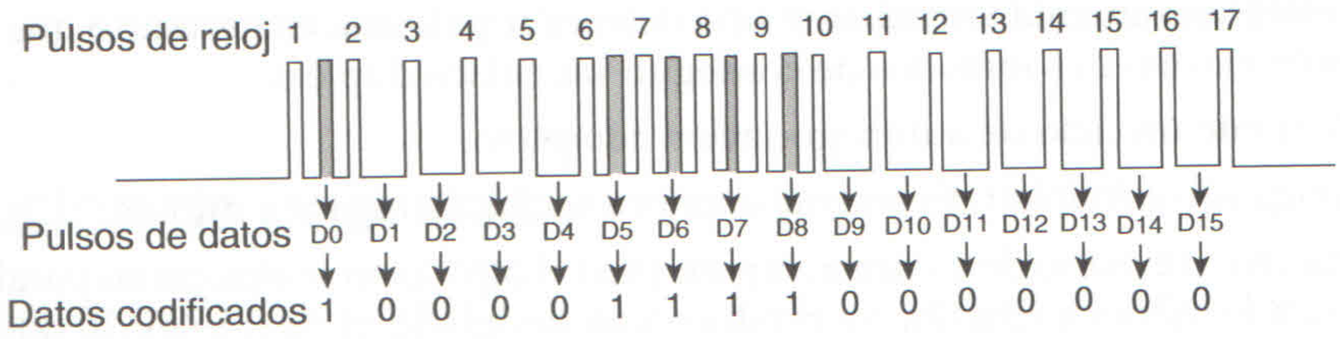

Figura 5.23. Interpretación de un pulso de autonegociación.

Cuando se implementa la autonegociación, se puede añadir información adicional usando el concepto de páginas. Las páginas son bits adicionales que representan unos parámetros de enlace y negociación más sofisticados.

Después que un dispositivo ha decodificado la palabra código del enlace que ofrece su socio de enlace, reconoce la recepción de la palabra actual enviando al menos tres ráfagas FLP con el conjunto de bits de reconocimiento. Después de que ambos socios de enlace reconozcan la palabra código del enlace FLP actual intercambiada de este modo, los socios de enlace se mueven a la página siguiente o activan la configuración convenida e intentan el enlace en consecuencia. Los socios de enlace pueden enviar cualquier número de páginas siguientes siguiendo la configuración inicial de página base y cualesquiera páginas siguientes que fuesen necesarias asociadas con la página base.

Establecimiento de enlace y semidúplex/dúplex

A los socios de enlace sólo se les permite saltar ofreciendo las configuraciones que sean capaces de ofertar, pero no tienen permitido incluir configuraciones que no son capaces de ofrecer. Esto permite al administrador de la red obligar a los puertos a seleccionar la velocidad y la configuración dúplex, sin desactivar la autonegociación.

La autonegociación es opcional en la mayoría de implementaciones Ethernet. Gigabit Ethernet necesita su implementación, aunque el usuario puede desactivarla. La autonegociación fue definida originalmente para las implementaciones UTP de Ethernet. Se extendió para trabajar con otras implementaciones de fibra óptica mediante el uso de conjuntos /C/ ordenados en lugar de ráfagas FLP.

Cuando una estación autonegocia los primeros intentos de enlace, se supone que activa las partes 10BASET del conjunto de chips frontal para intentar establecer inmediatamente un enlace. Si está presente la señalización 10BASET y la estación soporta 10BASET, intenta establecer un enlace sin negociar. Si cualquier señalización produce un enlace, o si se reciben las ráfagas FLP, la estación procede con esta tecnología. Si un socio de enlace no ofrece una ráfaga FLP, pero en su lugar ofrece NLP, se asume automáticamente que ese dispositivo es una estación 10BASET. Durante este intervalo inicial de prueba de otras tecnologías, la ruta de transmisión envía ráfagas FLP. La norma no permite detección paralela de ninguna otra tecnología.

Si se establece un enlace mediante una detección paralela, es necesario que sea semidúplex. Sólo existen dos métodos de conseguir un enlace dúplex:

- Mediante un ciclo de autonegociación completo.
- Obligando administrativamente a ambos socios de enlace a dúplex.

Si se fuerza a un socio de enlace a dúplex, pero el otro socio se detecta en paralelo mientras intentan la autonegociación, se produce una desigualdad de dúplex, lo que da como resultado colisiones y errores en este enlace. Si fuerza un extremo, **debe** forzar el otro. La excepción a esto es que 10 Gigabit Ethernet no soporta semidúplex.

Muchos fabricantes implementan su hardware de modo que efectúa ciclos por todos los estados posibles. Transmite ráfagas FLP para autonegociar durante un instante, entonces se autoconfigura para Fast Ethernet e intenta el enlace durante otro instante, y finalmente escucha durante un tiempo. Algunos fabricantes no ofrecen ningún intento de transmisión con el enlace hasta que la interfaz escuche primero una ráfaga FLP o algún otro esquema de señalización. En un estado de escucha en silencio, una computadora portátil es capaz de conservar suficiente energía para permanecer completamente útil, aunque la norma no soporta este modo.

Funcionamiento dúplex Ethernet

Existen dos modos de dúplex: semi y completo (o simplemente dúplex). Para los medios compartidos, el modo semidúplex es el principal. Todas las implementaciones coaxiales son inherentemente semidúplex por naturaleza y no pueden operar en dúplex. Las implementaciones UTP y de fibra pueden operar en semidúplex, pero este modo es una imposición administrativa. Todas las implementaciones a 10 Gbps están especificadas únicamente para dúplex.

En semidúplex, sólo puede transmitir una estación en cada momento. En las implementaciones coaxiales, si una segunda estación transmite provocaría que las señales se solapasen y chocasen, volviéndose corruptas. Como la fibra y el UTP normalmente transmiten por pares separados, las señales no tienen la oportunidad de solaparse y corromperse. Ethernet ha establecido normas arbitrarias para resolver conflictos que surgen cuando más de una estación intenta transmitir al mismo tiempo. A ambas estaciones en un enlace dúplex punto a punto se les permite transmitir en cualquier momento, sin importar si la otra está transmitiendo al mismo tiempo.

La autonegociación evita la mayoría de las situaciones en las que una estación en un enlace punto a punto transmite bajo normas semidúplex y la otra opera bajo normas dúplex. Sólo existen dos modos de lograr una conexión dúplex a velocidades inferiores a los 10 Gigabit Ethernet:

- Usando la autonegociación.
- Forzando administrativamente el modo de interfaz.

Si una estación en un enlace punto a punto autonegocia y la otra no, a la estación que autonegocia se le pide que seleccione semidúplex. Así, si se fuerza un extremo de un enlace, es obligado que se fuerce también el otro extremo. Si se produce un fallo al forzar ambos extremos, resulta un nivel de errores artificialmente elevado y un rendimiento

esario que sea semi-

úplex.

cta en paralelo mien-
plex, lo que da como
ebe forzar el otro. La

ctúa ciclos por todas
te un instante, entre-
otro instante, y final-
n ningún intento de
a ráfaga FLP o algún
na computadora per-
etamente útil, aunque

te dúplex). Para los
nplementaciones que
perar en dúplex. Las
ero este modo es una
tán especificadas uni-

mento. En las imple-
ría que las señales se
P normalmente tran-
solaparse y comu-
ctos que surgen cuan-
bas estaciones en un
momento, sin impor-

e una estación en un
a opera bajo normas
locidades inferiores a

no, a la estación que
n extremo de un enla-
uce un fallo al forzar
do y un rendimiento

sobre del enlace. La desigualdad en el modo dúplex es quizá el problema más común en las redes conmutadas.

Resolución de prioridad

En el evento en que los socios de enlace comparten más de una tecnología en común, se emplea la siguiente lista para decidir qué tecnología se debe elegir de las configuraciones que se ofrecen. Dicho de otro modo, es deseable para las versiones a 10/100/1000 Mbps de Ethernet basadas en el cobre que estén de acuerdo automáticamente en el mejor modo para las dos interfaces a enlazar. La lista se ha creado por orden de prioridad, con la configuración de enlace más deseable en la parte superior:

- Dúplex.
- Semidúplex.
- Dúplex.
- Semidúplex.
- Dúplex.
- Semidúplex.

Las implementaciones Ethernet de fibra óptica no se incluyen en esta resolución de prioridad porque las interfaces electrónicas y las ópticas no permiten una reconfiguración fácil entre implementaciones. Se supone que la configuración de la interfaz es fija. Si las dos interfaces son capaces de autonegociar, ya están empleando la misma implementación Ethernet, aunque quedan un buen número de opciones de configuración, como la configuración dúplex o qué estación actuará como maestra para temas de sincronización.

Dominios de colisión y dominios de difusión

Esta sección presenta temas relacionados con la colisión y los dominios de difusión. Las difusiones excesivas y las colisiones pueden afectar al rendimiento de la red. Esta sección explica el modo de reducir el impacto de las difusiones y colisiones en el rendimiento de la red. Se define el término **segmento** y se explican los diferentes tipos de segmentación.

Redes conectadas directamente

Para comprender los dominios de colisión, primero es necesario examinar qué es una colisión y cómo se produce. Para ayudar a explicar las colisiones, es muy útil repasar los medios y las topologías de la capa 1.

Como puede ver en la Figura 5.24, algunos de los distintos tipos de redes conectadas directamente son:

- **Entorno de medio compartido**. Un entorno de medio compartido se produce cuando varios *hosts* tienen acceso a los mismos medios. Por ejemplo, si varios PC están conectados al mismo hilo físico o fibra óptica, o comparten el mismo espacio aéreo, están compartiendo el mismo entorno de medios. En este caso, se dice que comparten el mismo dominio de colisión. La Ethernet clásica basada en bus (cable coaxial) y la Ethernet basada en *hub* (cable UTP) son entornos de medio compartido.
- **Entorno de medio compartido extendido**. Es un tipo especial de entorno de medio compartido en que los dispositivos de red pueden extender el entorno para que se puedan acomodar varios accesos o cables de distancias más largas. El uso de repetidores Ethernet o varios *hubs* puede crear un entorno de medio compartido extendido. Esto a su vez crea un dominio de colisión extendido.
- **Entorno de red punto a punto**. Se utiliza ampliamente en las conexiones de red de acceso telefónico; es la más familiar para el usuario doméstico. Es un entorno de medio compartido en el que un dispositivo sólo se conecta a otro único dispositivo; es como conectar una computadora a un proveedor de servicios de Internet mediante un módem y una línea de teléfono. Debido a esta conexión punto a punto especializada, no existe riesgo potencial de colisión. No hay ningún otro dispositivo que comparta el enlace.

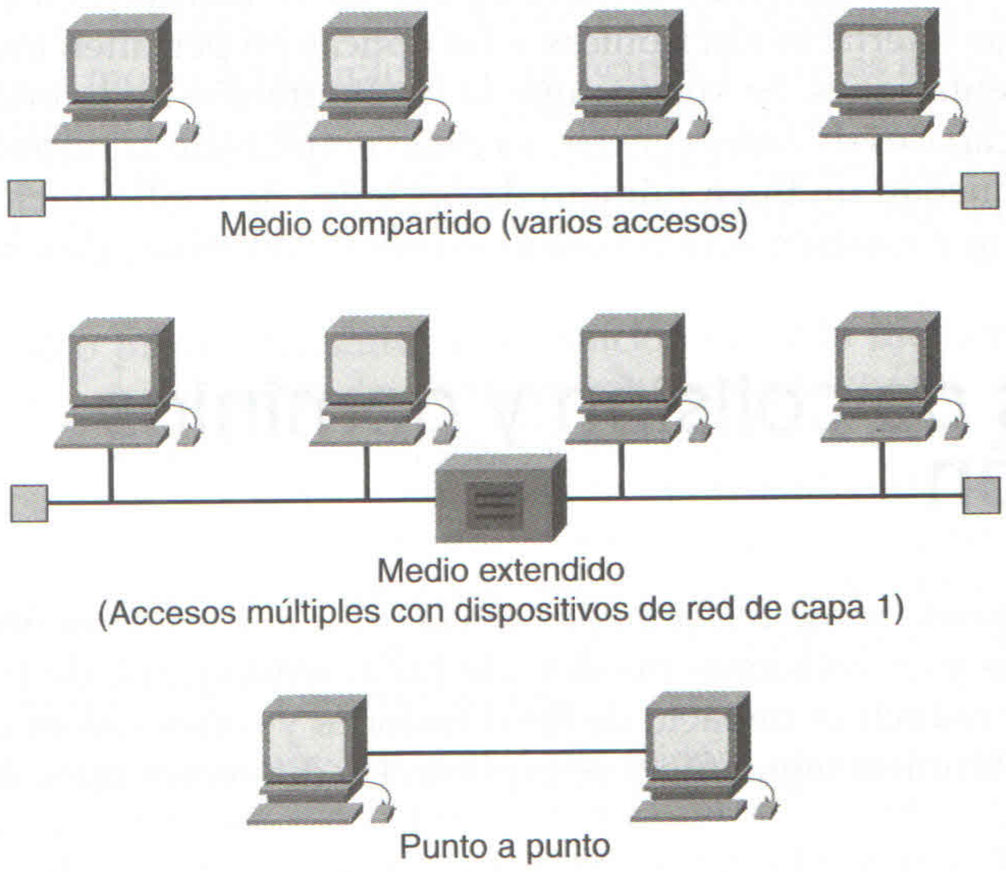

Figura 5.24. Redes conectadas directamente.

Redes indirectamente conectadas

Algunas redes están conectadas indirectamente, lo que significa que existe algún dispositivo de red de capa superior o hay alguna distancia geográfica entre los dos hosts.

municación. La Figura 5.25 muestra también dos tipos de redes conectadas indirectamente, que se describen del modo siguiente:

- **Circuito conmutado**. Una red conectada indirectamente en la que los circuitos eléctricos reales se mantienen mientras dure la comunicación. La conmutación de circuitos establece una conexión física extremo a extremo entre los puntos finales. El ancho de banda se dedica a esta conexión punto a punto. El sistema telefónico actual es todavía, en parte, de conmutación de circuitos, aunque los sistemas telefónicos en muchos países cada vez se concentran menos en las tecnologías de conmutación de circuitos. Como no es un entorno compartido, no hay colisiones.
- **Paquete conmutado**. En lugar de dedicar un enlace como circuito de conexión exclusivo entre dos *hosts* en comunicación, el origen envía los mensajes en paquetes. Cada paquete contiene la información suficiente para ser enrutado al *host* de destino adecuado. Las redes de conmutación de paquetes comparten medios físicos con frecuencia, pero como se crean conexiones punto a punto lógicas, no existen colisiones.

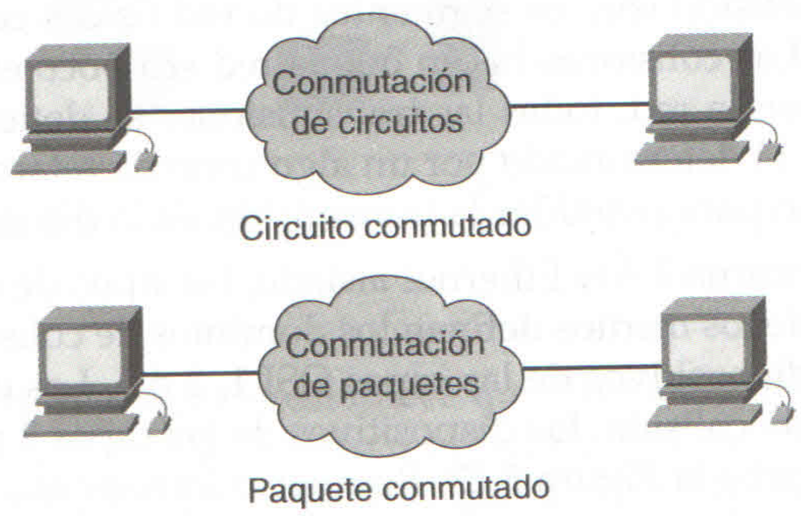

Figura 5.25. Redes conectadas indirectamente.

Colisiones y dominios de colisión

importante identificar el medio como entorno compartido porque este entorno compartido provoca colisiones. Puede darse una situación similar con un automóvil en la autopista. Si sólo hay un coche, no hay nada que choque contra él. Sin embargo, si hay más de un automóvil que intenta utilizar la misma sección de carretera al mismo tiempo, como se muestra en la Figura 5.26, se produce una colisión. Lo mismo pasa con las redes: si más de una computadora intenta transmitir datos por el mismo segmento de red al mismo tiempo, se produce una colisión.

Una **colisión** puede producirse cuando 2 bits se propagan al mismo tiempo y en la misma red. Una red pequeña y lenta puede funcionar como un sistema que sólo permite que dos computadoras envíen mensajes, con ambas de acuerdo para esperar su turno. El problema surge cuando muchas computadoras están conectadas a redes grandes, con cada una de ellas deseando comunicar millones de bits.

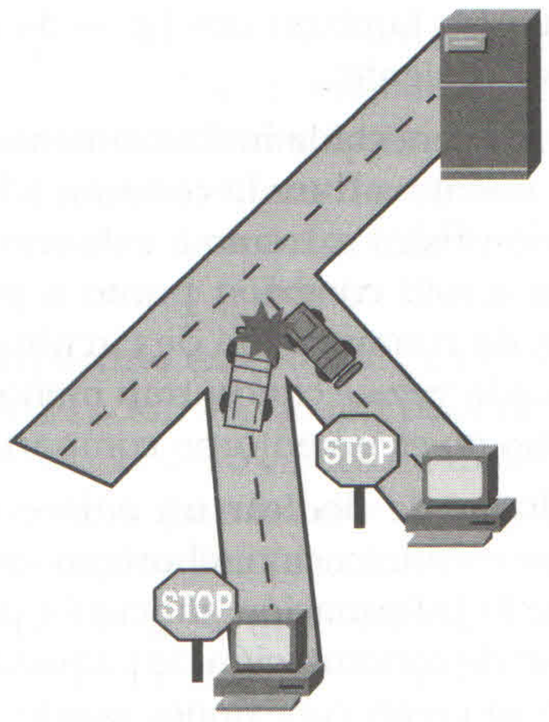

Figura 5.26. Colisión.

Los dominios de colisión son los segmentos de red físicos conectados donde pueden ocurrir las colisiones. Las colisiones hacen que la red sea poco eficiente. Cada vez que se produce una colisión en la red, todas las transmisiones se detienen por un tiempo. Este tiempo es variable y está determinado por un algoritmo de retardo en cada dispositivo de la red, el cual es necesario para reanudar la transmisión de la difusión.

Excepto para un entorno LAN Ethernet aislado, los tipos de dispositivos que interconectan los segmentos de los medios definen los dominios de colisión. Estos dispositivos se han clasificado como dispositivos de las capas OSI 1, 2 ó 3. Los dispositivos de capa 1 no rompen los dominios de colisión; los dispositivos de las capas 2 y 3 rompen los dominios de colisión, como describe la Figura 5.27. Romper o incrementar el número de dominios de colisión con los dispositivos de capa 2 y 3 se llama **segmentación**.

Aplicación	
Presentación	
Sesión	
Transporte	
Red	Rompe el dominio de colisión
Enlace de datos	Rompe el dominio de colisión
Física	Un dominio de colisión

Figura 5.27. Segmentación del dominio de colisión.

Los dispositivos de capa 1, como repetidores y *hubs*, sirven para la función principal de extender los segmentos de cable Ethernet. Al extender la red, se pueden añadir más hosts. Sin embargo, cada *host* que se añade incrementa la cantidad de tráfico potencial en la red.

Como los dispositivos de capa 1 pasan cualquier cosa que se envíe por el medio, cuanto mayor sea el tráfico transmitido por un dominio de colisión, mayor probabilidad de colisión hay. El resultado final es la disminución del rendimiento de la red, el cual es aún más pronunciado si todas las computadoras de la red requieren grandes anchos de banda. Los dispositivos de capa 1 extienden los dominios de colisión, como se muestra en la Figura 5.28, pero la longitud de una LAN también se puede sobreextender y provocar otros problemas de colisión.

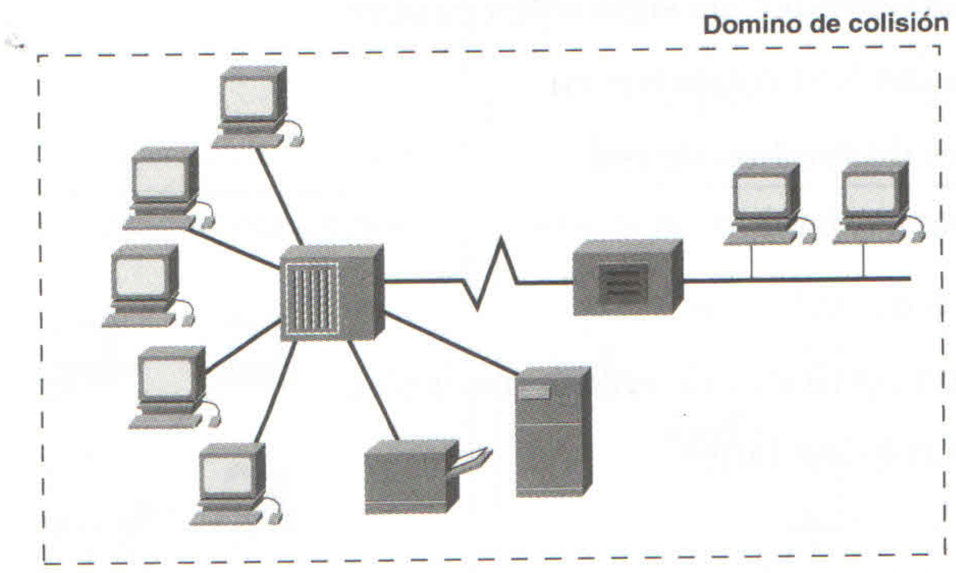

Figura 5.28. Un repetidor aumenta el dominio de colisión.

La regla de los cuatro repetidores establece que no puede haber entre dos computadoras cualesquiera de la red más de cuatro repetidores o cuatro *hubs* de repetición, como se muestra en la Figura 5.29. Para confirmar que una red 10BASET funciona correctamente, el cálculo del retardo de ida y vuelta debe hacerse bajo ciertos límites; en caso contrario, todas las estaciones de trabajo no serán capaces de escuchar todas las colisiones de la red.

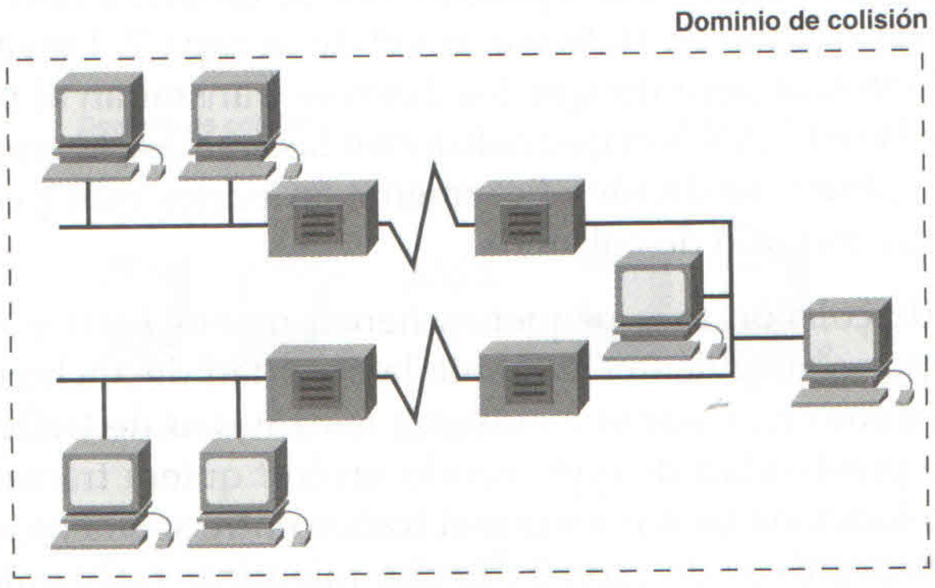

Figura 5.29. Un repetidor aumenta el dominio de colisión.

La latencia del repetidor, el retardo de propagación y la latencia de la NIC contribuyen a la regla de los cuatro repetidores. No seguir esta regla puede llevar a violar el máximo límite de retardo. Cuando se excede este límite, aumenta dramáticamente el número de colisiones atrasadas. Una colisión atrasada se produce cuando sucede una colisión después de haberse transmitido los primeros 64 bytes de la trama. El conjunto de chips de la NIC no se necesita para transmitir automáticamente cuando se produce una colisión atrasada. Estas tramas de colisión atrasada añaden un retardo que se denomina retardo de consumo. Mientras este retardo de consumo y la latencia aumenten, disminuirá el rendimiento de la red. Esta regla Ethernet se conoce también como regla 5-4-3-2-1. Esto quiere decir que no se deben exceder las siguientes pautas:

- Las secciones del *host* consisten en:
  - **5** secciones de medios de red.
  - **4** repetidores o *hubs*.
  - **3** secciones de red.
- **2** secciones son secciones de enlace (no *hosts*).
- **1** dominio de colisión largo.

Segmentación

Para un profesional de las redes, una habilidad importante es la destreza de reconocer dominios de colisión. Conectar varias computadoras a un medio de acceso compartido que no tiene otros dispositivos de red conectados crea un dominio de colisión. Esta situación limita el número de computadoras que pueden emplear el medio, también conocido como **segmento**. Como se puede ver en la Figura 5.30, los dispositivos de capa 1 se extienden, pero no controlan los dominios de colisión.

Los dispositivos de capa 2 segmentan o dividen los dominios de colisión. Controlando la propagación de trama, empleando la dirección MAC asignada a cada dispositivo Ethernet, se realiza esta función. Los dispositivos de capa 2, puentes y *switches*, hacen un seguimiento de las direcciones MAC y del segmento donde están. Al hacer esto, estos dispositivos pueden controlar el flujo de tráfico al nivel de la capa 2. Esta función hace que las redes sean más eficientes, al permitir que los datos se transmitan al mismo tiempo a diferentes segmentos de la red LAN, sin que colisionen las tramas. Al emplear puentes y *switches*, el dominio de colisión se divide eficazmente en partes más pequeñas, siendo cada una de ellas su propio dominio de colisión.

Estos dominios de colisión más pequeños tienen menos *hosts* y menos tráfico que el dominio original y, por consiguiente, aumenta la cantidad de ancho de banda disponible para cada *host* en el dominio. Cuanto menor sea la cantidad de tráfico en un dominio de colisión, mayor es la posibilidad de que cuando un *host* quiera transmitir datos, el medio esté disponible. Esto funciona bien mientras el tráfico entre segmentos no sea excesivo. De caso contrario, los dispositivos de capa 2 pueden ralentizar realmente la comunicación al convertirse ellos mismos en un cuello de botella.

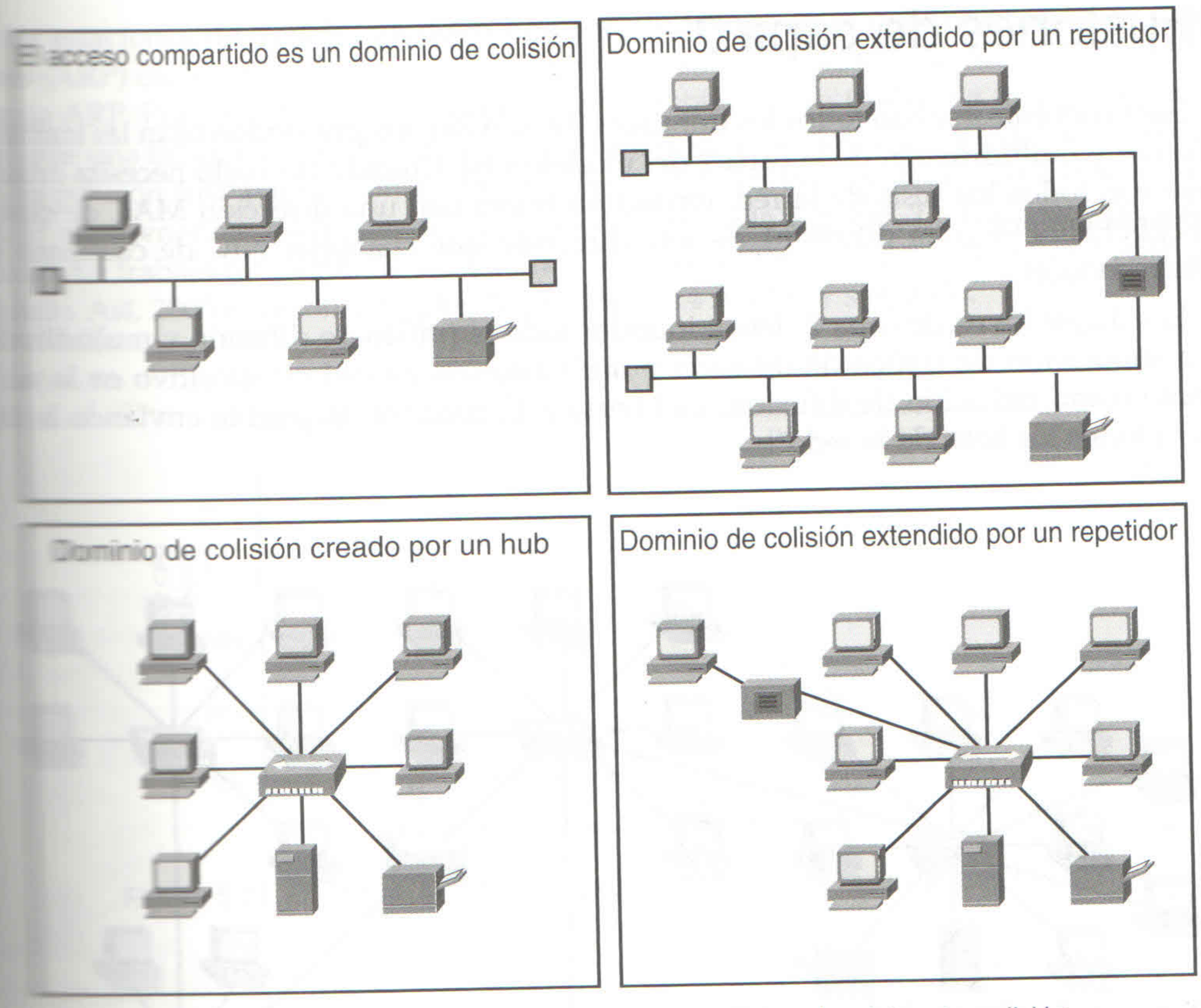

Figura 5.30. Dispositivos de capa 1 extendiendo los dominios de colisión.

dispositivos de capa 3, al igual que los dispositivos de capa 2, no fomentan las colisiones. Debido a esto, el uso de dispositivos de capa 3 en una red tiene el efecto de dividir los dominios de colisión en otros más pequeños. Los dispositivos de capa 3 realizan más funciones que la de dividir un dominio de colisión. Estos dispositivos y sus funciones se explican más en profundidad en la sección "Dominios de difusión". La Figura 5.31 ilustra cómo los dispositivos de las capas 2 y 3 pueden dividir un dominio de colisión.

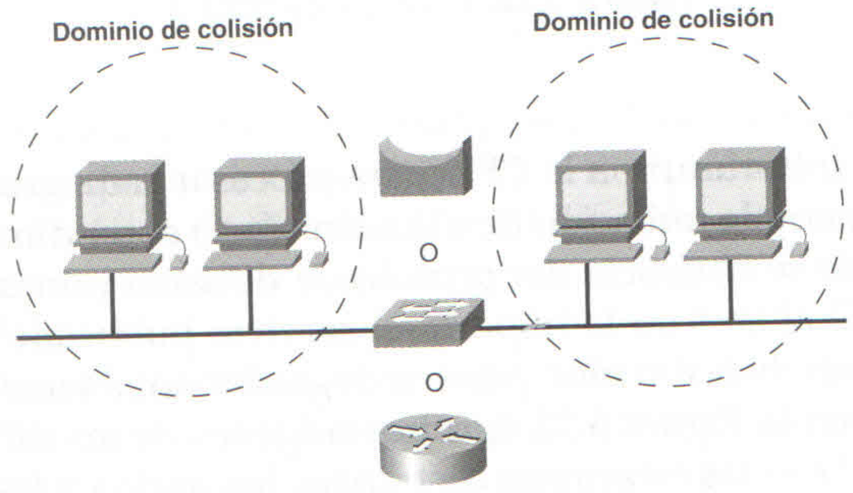

Figura 5.31. Límites al dominio de colisión.

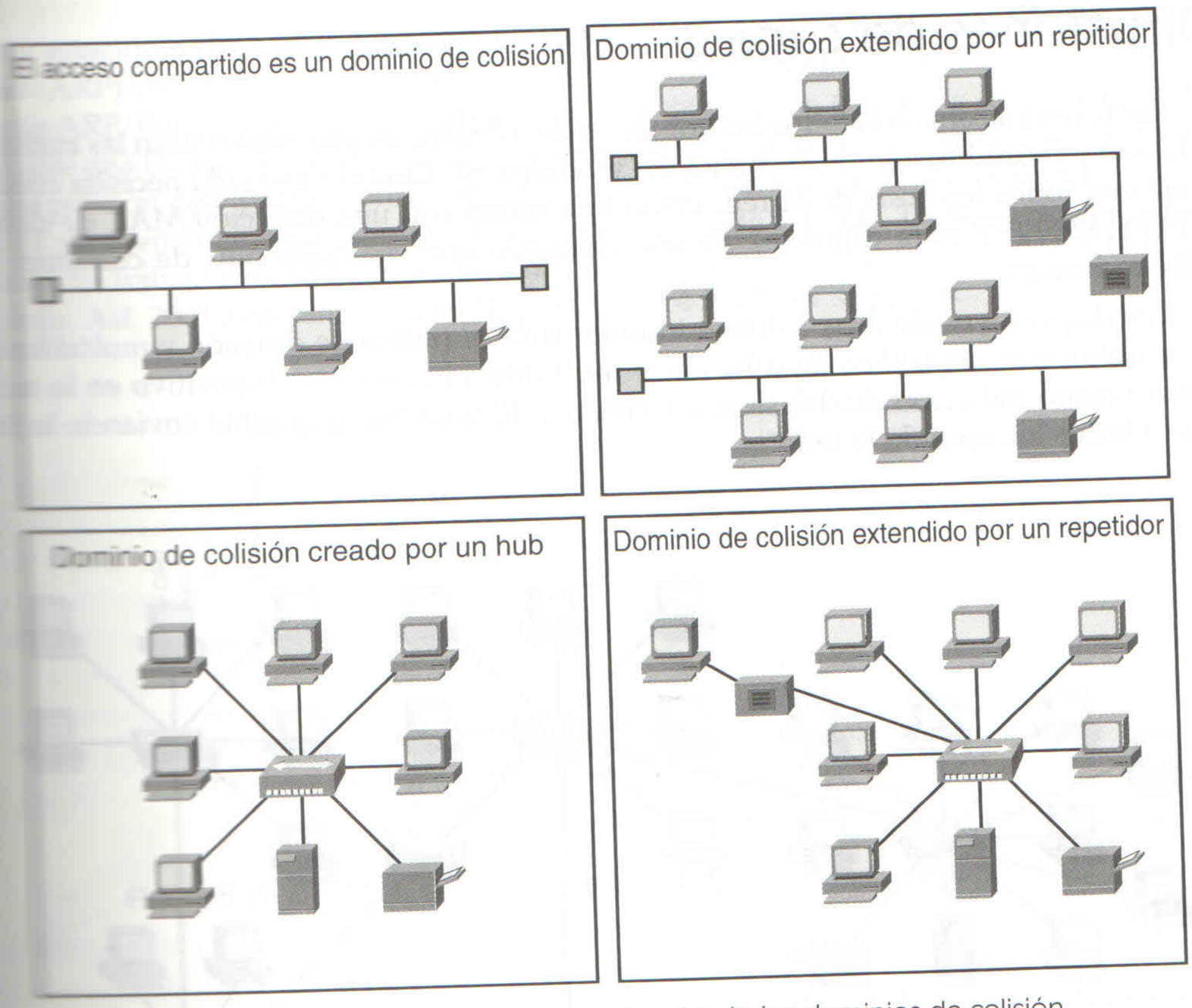

Figura 5.30. Dispositivos de capa 1 extendiendo los dominios de colisión.

Los dispositivos de capa 3, al igual que los dispositivos de capa 2, no fomentan las colisiones. Debido a esto, el uso de dispositivos de capa 3 en una red tiene el efecto de dividir los dominios de colisión en otros más pequeños. Los dispositivos de capa 3 realizan más funciones que la de dividir un dominio de colisión. Estos dispositivos y sus funciones se verán más en profundidad en la sección "Dominios de difusión". La Figura 5.31 ilustra cómo los dispositivos de las capas 2 y 3 pueden dividir un dominio de colisión.

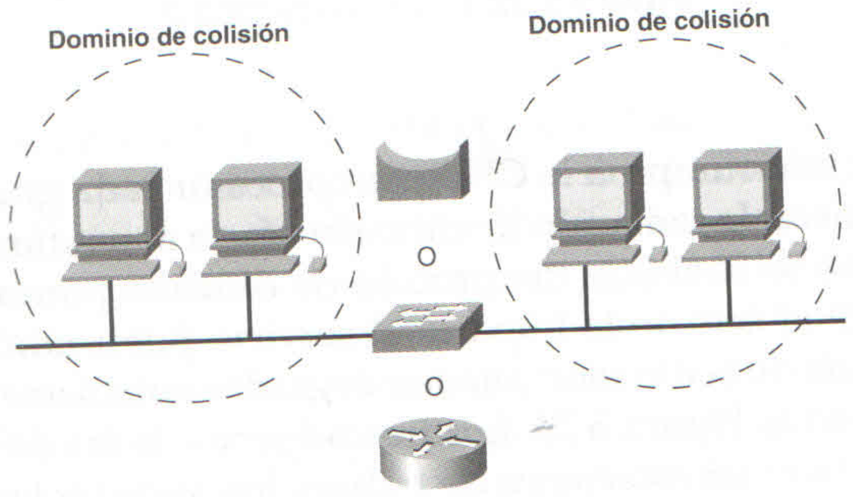

Figura 5.31. Límites al dominio de colisión.

Difusiones de capa 2

Para comunicarse con todos los dominios de colisión, los protocolos usan las tramas de difusión y multidifusión de la capa 2 del modelo OSI. Cuando un nodo necesita comunicarse con todos los *hosts* de la red, envía una trama con una dirección MAC de destino 0xFFFFFFFFFFFF (una difusión). Es una dirección que cualquier NIC de cualquier red debe reconocer.

Los dispositivos de capa 2 deben inundar todo el tráfico de difusión y multidifusión. La acumulación de tráfico de difusión y multidifusión de cada dispositivo en la red se conoce como radiación de difusión. La Figura 5.32 muestra un puente enviando la difusión a todos los *hosts* de la red.

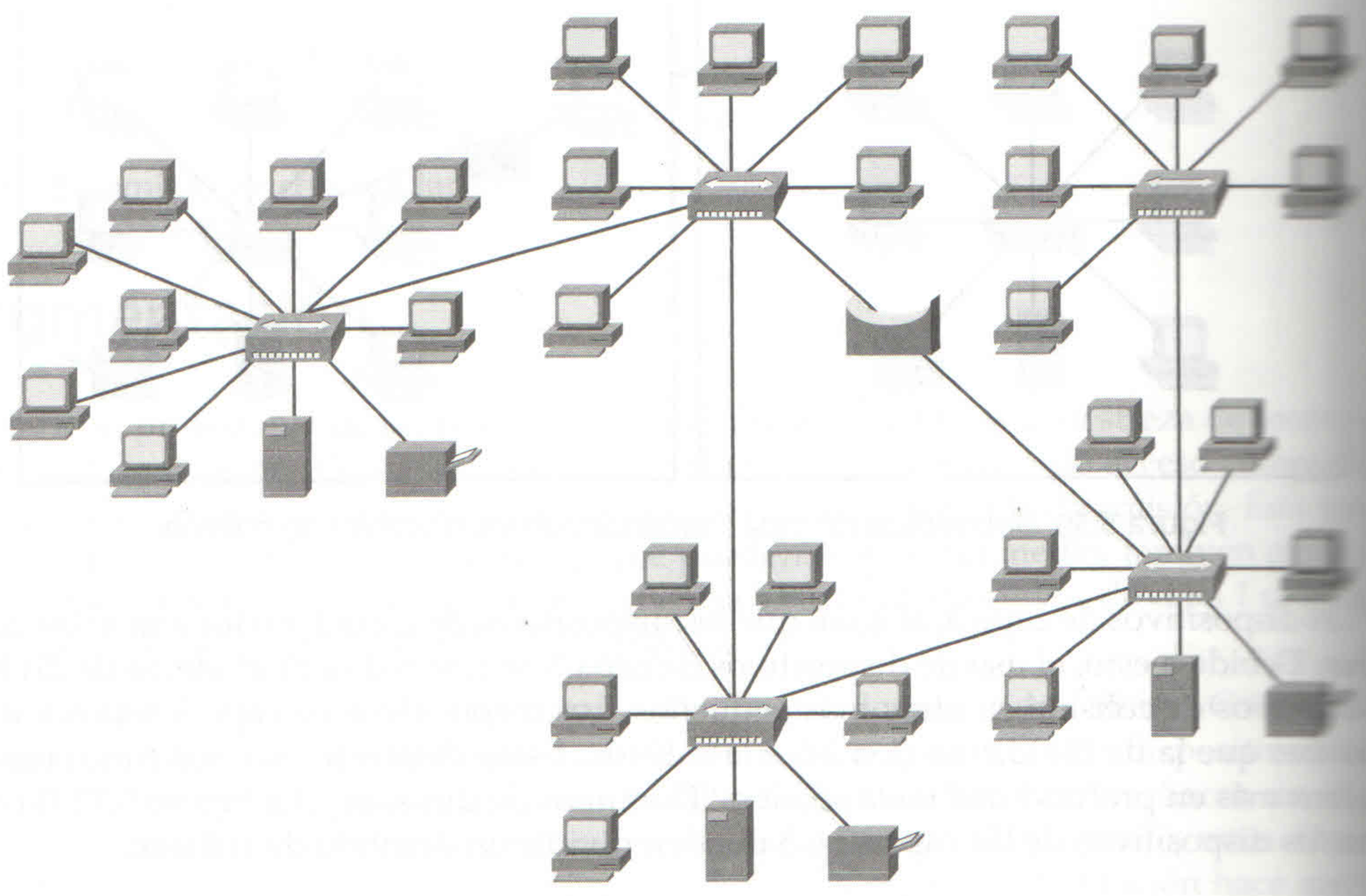

Figura 5.32. Difusión de capa 2.

Como la NIC debe interrumpir a la CPU para procesar cada grupo de difusión o multidifusión al que pertenece, la radiación de difusión afecta al rendimiento de los hosts de la red. Peor aún, el *host* no se beneficia del proceso de difusión porque no se ha buscado la dirección de destino. O al *host* no le importa el servicio publicado o ya lo conoce. Los niveles altos de radiación de la difusión pueden degradar notablemente el rendimiento del *host*, como se muestra en la Figura 5.33. Los tres orígenes de las difusiones y las multidifusiones en las redes IP son las estaciones de trabajo, los *routers* y las aplicaciones de multidifusión.

Las estaciones de trabajo difunden una solicitud de protocolo de resolución de direcciones (ARP) cada vez que necesitan localizar una dirección MAC que no se encuentra en la caché ARP. Por ejemplo, el comando telnet mumble.com se traduce a una dirección IP mediante una búsqueda DNS (sistema de denominación de dominio), y después se difunde una petición ARP para encontrar la estación actual. Normalmente, las estaciones de trabajo IP almacenan en caché de 10 a 100 direcciones cada 2 horas. La tasa ARP para una estación de trabajo típica puede ser de unas 50 direcciones cada 2 horas, o 0,007 ARP por segundo. Así, 2000 estaciones finales IP producen 14 ARP por segundo.

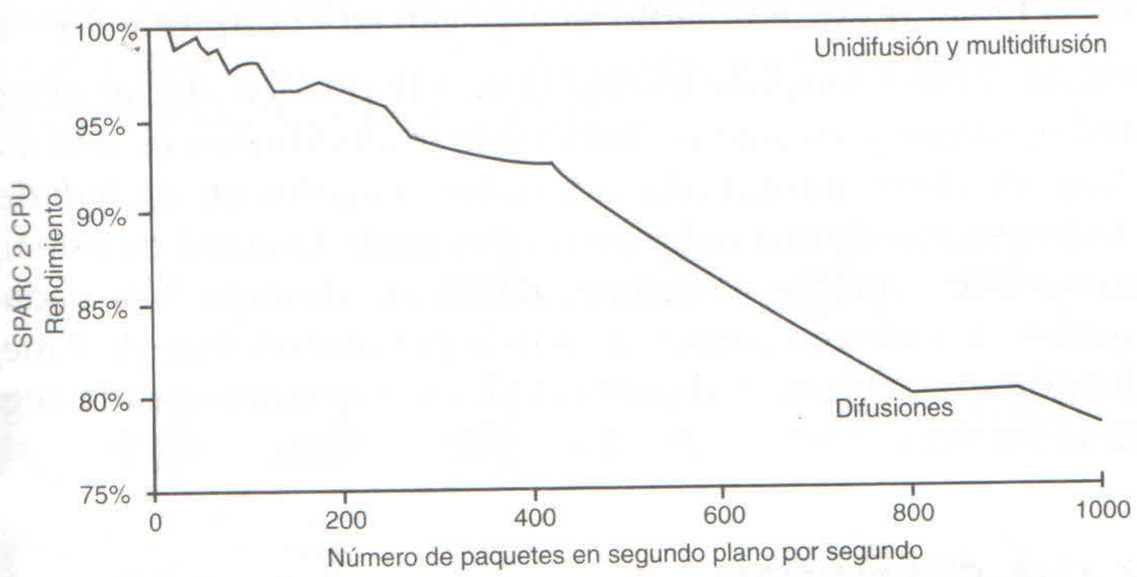

Figura 5.33. Efecto de la radiación de la difusión en los *hosts* de una red IP.

La Tabla 5.7 enumera el número medio de difusiones y multidifusiones para las redes

Tabla 5.7. Número medio de difusiones y multidifusiones para las redes IP.

Número de *hosts*	Porcentaje medio de pérdida CPU por *host*
	0,14
	0,96
	9,15

Aunque los números de la Tabla 5.7 puedan parecer bajos, representan un promedio de una red IP bien diseñada que no está ejecutando el Protocolo de información de enrutamiento (RIP). Cuando el tráfico de difusión y multidifusión alcanza el máximo nivel debido a un comportamiento tormentoso, pueden ordenarse pérdidas de CPU máximas de una magnitud superior a la media. Las tormentas de difusión pueden estar motivadas por un dispositivo que solicite información de una red que ha crecido demasiado. Por tanto, se reciben demasiadas respuestas a la petición original que el dispositivo no puede procesar, o puede ser que la primera petición active peticiones similares de otros dispositivos que bloquean el flujo normal de tráfico en la red.

Un *router* IP es un *router* o una estación de trabajo que funciona con cualquier protocolo de enrutamiento por vector de distancia. Algunos administradores configuran todas las estaciones de trabajo para que ejecuten RIP (un protocolo de enrutamiento) como una política de alcance y redundancia. Cada 30 segundos, RIP utiliza difusiones para transmitir la tabla de enrutamiento RIP completa a otros *routers* RIP. Si se han configurado muchos *routers* para ejecutar RIP y se necesita un promedio de 50 paquetes para transmitir la tabla de enrutamiento, los *routers* pueden generar 3333 difusiones por segundo. La mayoría de los administradores de redes configura sólo un pequeño número de *routers* (normalmente de cinco a diez) para ejecutar RIP. Para una tabla de enrutamiento con un tamaño de 50 paquetes, 10 *routers* RIP generan alrededor de 16 difusiones por segundo. (Los protocolos de enrutamiento y la tabla de enrutamiento se explican en el Capítulo 8.)

Por el contrario, las aplicaciones de multidifusión IP pueden afectar al rendimiento de las redes conmutadas, largas y escaladas. Aunque la multidifusión es una manera eficiente de enviar un flujo de datos multimedia a muchos usuarios en un *hub* de medio compartido, afecta a todo usuario de una red plana conmutada. Una red de este tipo es una red de *switches* interconectados que no utiliza enrutamiento de capa 3 ni nada similar. Una aplicación de paquetes de vídeo en particular puede generar un flujo de 7 megabytes (MB) de datos multidifusión que, en una red conmutada, se enviarían a cada segmento, generando una congestión severa.

Dominios de difusión

Un **dominio de difusión** es una agrupación de dominios de colisión conectados por dispositivos de capa 2. Dividir una red LAN en varios dominios de colisión mejora la eficacia de la red permitiendo varias transmisiones simultáneas de datos en dominios de colisión separados. Pero como las difusiones viajan a través de los dispositivos de capa 2, si son excesivas, pueden reducir la eficacia de la LAN entera. Se deben controlar las difusiones en la capa 3, porque los dispositivos de las capas 1 y 2 no pueden controlarlas. El tamaño total del dominio de colisión se puede identificar comprobando todos los dominios de colisión que la misma trama de difusión está procesando. Dicho de otro modo, todos los nodos forman parte del segmento de red limitado por un dispositivo de capa 3. Los dominios de difusión se controlan en la capa 3 porque los *routers* no envían difusiones. En la Figura 5.34, el *router* no enviará la difusión desde la estación de trabajo resaltada (se encuentra a la parte izquierda) hasta los *hosts* que están a la derecha.

Los *routers* realmente funcionan en las capas 1, 2 y 3. Al igual que todos los dispositivos de capa 1, tienen una conexión física y transmiten datos a los medios. Tienen una encapsulación de capa 2 en todas las interfaces y funcionan como cualquier otro dispositivo de capa 2. La capa 3 permite al *router* segmentar los dominios de difusión.

Para enviar un paquete a través de un *router*, se debe procesar dicho paquete en la capa 2 y despojar la información de la trama. El envío de capa 3 está basado en la dirección IP de destino, no en la dirección MAC. Para enviar el paquete, éste debe contener una dirección IP fuera del intervalo de direcciones asignado al segmento LAN, y el *router* debe tener una dirección de destino para enviar el paquete específico a su propia tabla de enrutamiento.

Introducción al flujo de datos

El flujo de datos en el contexto de la colisión y los dominios de difusión se centra en cómo las tramas de datos se propagan por la red. Hace referencia al movimiento de datos a través de los dispositivos de las capas 1, 2 y 3, y a cómo deben encapsularse los datos para efectuar este viaje de forma eficaz. Recuerde que los datos se encapsulan en la capa de red con una dirección de origen y de destino IP, y en la capa de enlace de datos con una dirección de origen y de destino MAC.

La regla básica que seguimos aquí es que un dispositivo de capa 1 siempre envía la trama, un dispositivo de capa 2 quiere enviarla (es decir, envía a no ser que algo se lo impida) y un dispositivo de capa 3 no envía a no ser que tenga que hacerlo. El uso de esta regla ayuda a identificar el flujo de datos en la red.

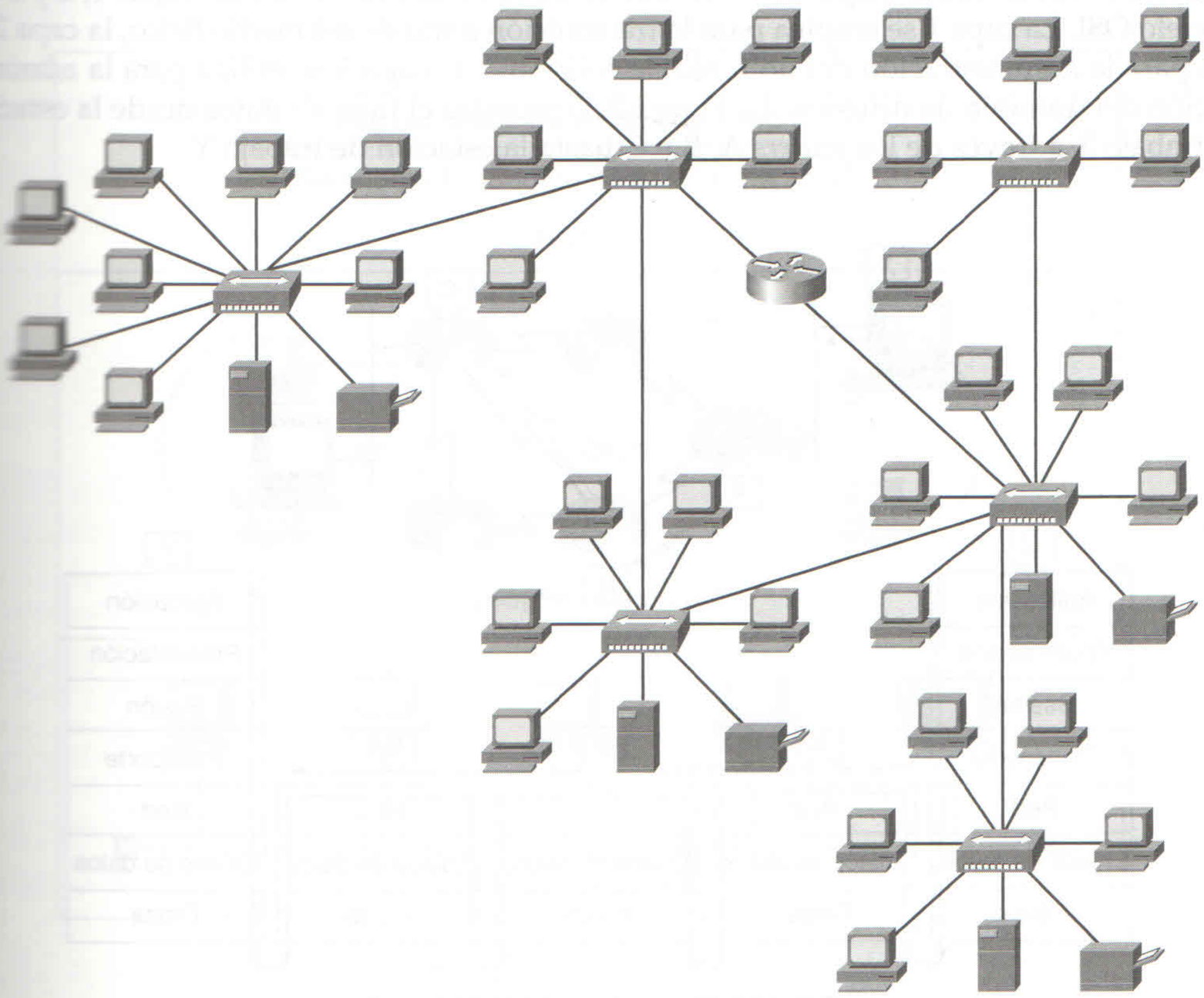

Figura 5.34. Segmentación del dominio de difusión.

Los dispositivos de capa 1 (repetidores y *hubs*) no filtran, por lo que todo lo que recibe pasa al siguiente segmento. La trama sólo se regenera y se vuelve a sincronizar, volviendo así a su calidad de transmisión original. Cualquier segmento conectado por dispositivos de capa 1 forma parte del mismo dominio, ya sea de colisión o de difusión.

Los dispositivos de capa 2 (puentes y *switches*) filtran tramas de datos en base a la dirección MAC de destino. La trama se envía si va a un destino desconocido (fuera del dominio de colisión). La trama también se envía si su difusión, multidifusión o unidifusión queda fuera del dominio de colisión local. La única vez que no se envía una trama es cuando el dispositivo de capa 2 descubre que el *host* de envío y el *host* de recepción se encuentran en el mismo dominio de colisión. Un dispositivo de puente (capa 2) crea varios dominios de colisión, pero sólo mantiene un dominio de difusión.

Los dispositivos de capa 3 (*routers* y algún *switch* de gama alta) filtran los paquetes de datos en base a las direcciones de destino IP. La única forma de enviar un paquete de datos es que su dirección IP de destino se encuentre fuera del dominio de difusión y que el *router* tenga una ubicación identificada para enviar el paquete. Un dispositivo de capa 3 crea varias colisiones y dominios de difusión.

Un flujo de datos a través de una red basada en IP enrutado involucra al movimiento de datos a través de los dispositivos de administración del tráfico en las capas 1, 2 y 3 del modelo OSI. La capa 1 se emplea para la transmisión a través del medio físico, la capa 2 se usa para la administración del dominio de colisión, y la capa 3 se utiliza para la administración del dominio de difusión. La Figura 5.35 muestra el flujo de datos desde la estación de trabajo X a través de los *routers* A, B y C hasta la estación de trabajo Y.

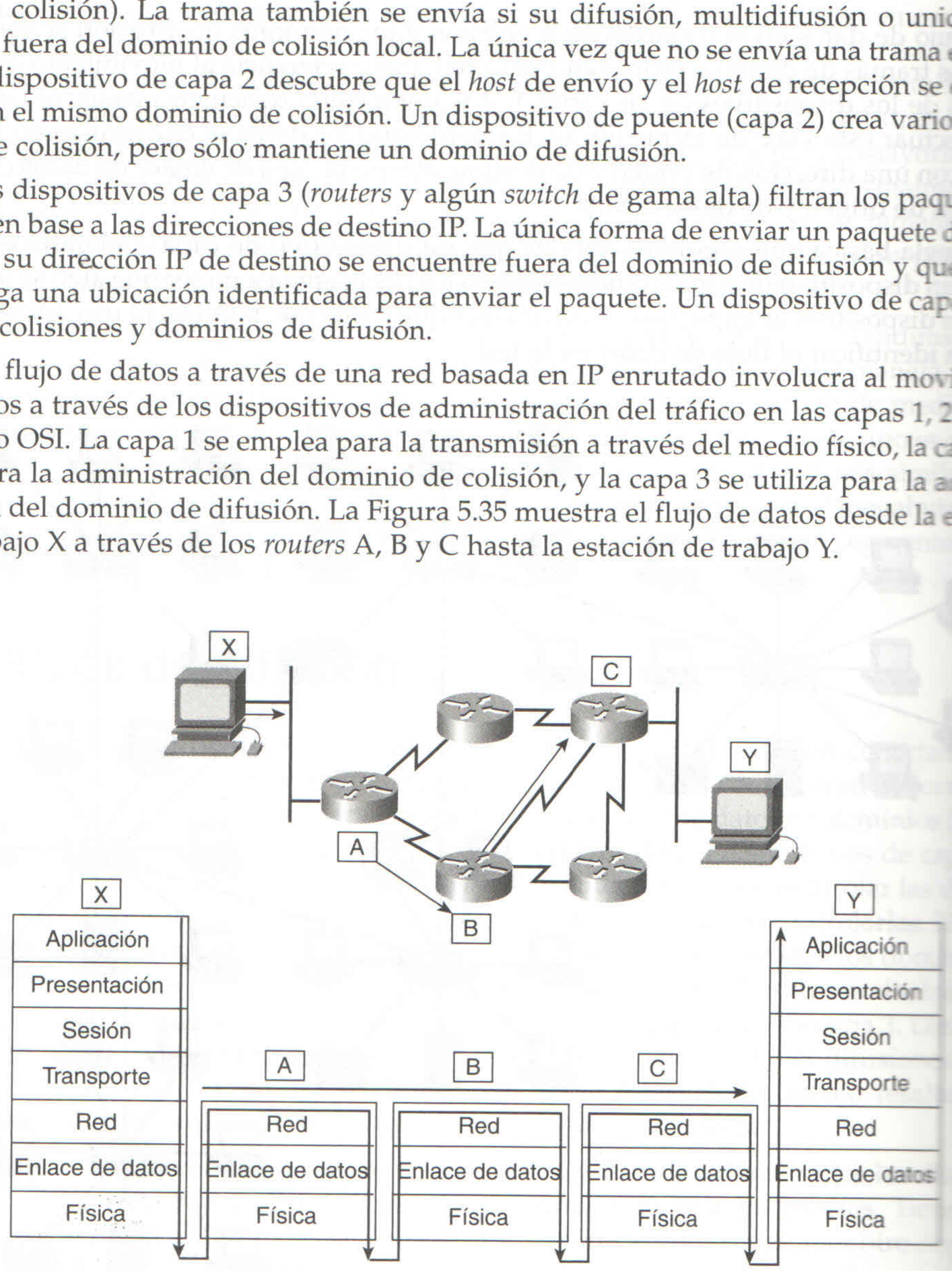

Figura 5.35. Flujo de datos en la red.

Segmento de red

Como sucede con muchos términos y acronismos, **segmento** tiene varios significados. La definición del diccionario para el término es:

- Una pieza separada de algo.
- Una de las partes en las que se divide o acota una entidad o cantidad.

En el contexto de la comunicación de datos se utilizan las siguientes definiciones:

- Sección de una red limitada por puentes, *routers* o *switches*.
- En una LAN con topología de bus, circuito eléctrico continuo que se conecta a menudo con otros segmentos con repetidores.
- Término que se emplea en la especificación TCP para describir una unidad de información simple de capa de transporte. Los términos datagrama, trama, mensaje y paquete se emplean también para describir los agrupamientos de información lógicos en varias capas del modelo de referencia OSI y en varios círculos tecnológicos.

La Figura 5.36 ilustra las tres definiciones del término **segmento** dentro del contenido de la comunicación de datos.

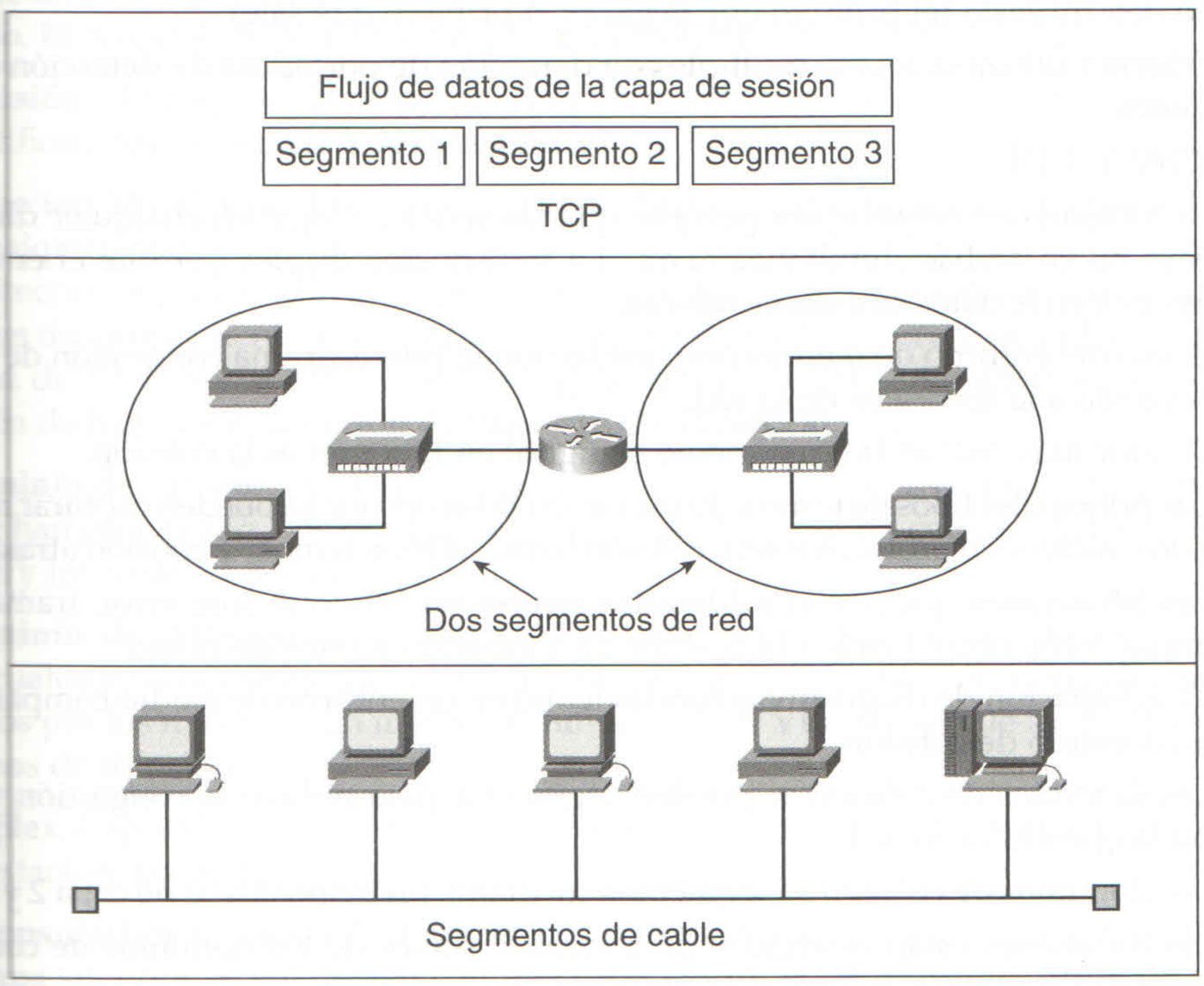

Figura 5.36. Segmentos.

Para definir el término **segmento** con propiedad, se debe presentar el contexto de su uso con la palabra. Si **segmento** se utiliza en el contexto de TCP, se define como porción segmentada de los datos. Si segmento se emplea en el contexto de un medio de red físico en una red enrutada, es una parte o sección del total de la red.

Resumen

En esta sección se han presentado los siguientes puntos clave:

- El Instituto de ingenieros electrónicos y eléctricos (IEEE) es una organización profesional que define las normas de la red. Las normas LAN IEEE se conocen como normas de comunicación IEEE y son las normativas predominantes para las LAN en la actualidad.
- El IEEE divide la capa de enlace de datos OSI en dos subcapas separadas: Control de acceso al medio (MAC) y Control de enlace lógico (LLC).
- Ethernet utiliza la dirección MAC, que es una dirección física ubicada en una NIC.
- El entramado ayuda a obtener información esencial que no podría obtenerse sólo con flujos de bits codificados.
- Existen dos categorías de Control de acceso al medio: determinista (por turnos) y no determinista (el primero que llega, es el primero que sale).
- Ethernet utiliza el acceso múltiple con detección de portadora de detección de colisiones
- (CSMA/CD).
- La transmisión semidúplex permite que las señales viajen en cualquier dirección, pero no en ambas simultáneamente. La transmisión dúplex permite el envío y la recepción de datos simultáneamente.
- El uso del entorno de medio compartido puede provocar una congestión de tráfico, llevando a la ineficacia de la red.
- El error más común (normalmente benigno) en Ethernet es la colisión.
- Los principales tipos de errores de tramas en Ethernet que se pueden capturar mediante los análisis de protocolos son: colisión local, colisión remota y colisión atrasada.
- Las situaciones que son consideradas errores en Ethernet son: error, trama larga, trama corta, *runts*, errores FCS, error de alineación y error de rango.
- La agrupación de dispositivos fundamental en un entorno de medio compartido es un dominio de colisión.
- Los dominios de colisión se pueden segmentar para reducir la congestión y mejorar la eficacia de la red.
- Los dominios de colisión se segmentan mediante los dispositivos de capa 2 y capa
- Las difusiones están diseñadas para viajar a través de los dominios de colisión y pueden ser motivo de ineficacia en la red.
- Los dominios de difusión se pueden segmentar usando los dispositivos de capa
- El flujo de datos se controla mediante la encapsulación de datos en conjunción con los dispositivos de capa 2 y capa 3.
- Las definiciones de los términos y acrónimos de red deben definirse según el contexto, no como términos aislados.
- Como complemento a todo lo aprendido en este capítulo, consulte el capítulo específico de Videos, PhotoZooms y e-Lab Activities del CD-ROM que incluye el libro.

Términos clave

Cabecera. Información de control situada antes de los datos cuando se encapsulan para la transmisión por la red.

Colisión. En Ethernet, resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando coinciden en el medio físico. Véase también **dominio de colisión**.

CSMA/CD (acceso múltiple con detección de portadora de detección de colisiones, *carrier sense multiple access collision detect*). Mecanismo de acceso al medio en que los dispositivos que están preparados para transmitir datos comprueban primero el canal buscando una portadora. Si no se descubre una durante un periodo específico de tiempo, el dispositivo puede transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por los dispositivos que colisionan. Esta colisión produce a su vez retardos en las transmisiones de dichos dispositivos durante un periodo de tiempo aleatorio. El acceso CSMA/CD se emplea en Ethernet e IEEE 802.3.

Difusión. Un paquete de datos que se envía a todos los nodos de la red. Las difusiones se identifican por la dirección de difusión.

Dirección MAC. Una dirección normalizada de la capa de enlace de datos necesaria para cualquier dispositivo que se conecte a una LAN. Otros dispositivos de la red usan estas direcciones para localizar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen una longitud de 6 bytes y el IEEE es el encargado de controlarlas. También se conoce como dirección de hardware, dirección de capa MAC o dirección física.

Dominio de colisión. En Ethernet, área de la red en la que las tramas que han colisionado se han propagado. Los repetidores y los *hubs* propagan las colisiones; los *switches*, los puentes y los *routers* LAN no.

Dominio de difusión. Conjunto de dispositivos que reciben la difusión de tramas desde cualquier dispositivo del conjunto. Los dominios de difusión normalmente están limitados por los *routers* (o, en una red conmutada, por VLAN) porque los *routers* no envían tramas de difusión.

Dúplex. Capacidad para transmitir datos simultáneamente entre una estación emisora y una estación receptora.

Encapsulación. Cubierta de datos en una cabecera de protocolo. Por ejemplo, los datos de la capa superior se envuelven con una cabecera Ethernet específica antes de transitar por la red. También, y cuando se puentean redes diferentes, la trama completa desde una red se puede colocar detrás de la cabecera utilizada por el protocolo de la capa de enlace de datos de la otra red.

Error de alineación. Mensaje que no finaliza en un límite de octetos.

Error de rango. Trama que tiene un valor de tamaño legal en el campo de longitud pero que no coincide con el número real de octetos contados en el campo de datos de la trama recibida.

Error. Definido en varios lugares de la norma 802.3 como una transmisión de al menos 20.000 a 50.000 tiempos de bit de duración. Sin embargo, la mayoría de las herramientas de diagnóstico informan de un error siempre que en una transmisión una trama excede el tamaño máximo legal (mucho menor que 20.000 a 50.000 tiempos de bit).

Ethernet a 10 GB. Creada con tecnología Ethernet y empleada en la mayoría de redes LAN actuales, Ethernet a 10 GB se describe como la tecnología que ofrece una mayor eficacia y un menor coste para el movimiento de datos en las conexiones *backbone* entre redes, además de proporcionar una tecnología consistente extremo a extremo. Ethernet a 10 GB puede ofrecer velocidades superiores a los 10 Gbps.

Ethernet. Especificación LAN inventada por Xerox Corporation y desarrollada por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD, funcionan con varios tipos de cable a 10, 100 y 1000 Mbps. Ethernet es parecida a las normas de las series IEEE 802.3.

Fast Ethernet. Cualquiera de las especificaciones para Ethernet a 100 Mbps. Fast Ethernet ofrece un incremento de velocidad 10 veces mayor que la especificación 10BASE-T, además de preservar cualidades como el formato de trama, los mecanismos MAC y el MTU. Estas similitudes permiten la utilización de las aplicaciones 10BASE-T y las herramientas de administración de redes en redes Fast Ethernet. Fast Ethernet se basa en una extensión de la especificación IEEE 802.3.

FDDI (Interfaz de datos distribuidos por fibra, *Fiber Distributed Data Interface*). Norma LAN definida por la 3T9.5 del Instintito nacional americano de normalización (ANSI), que especifica una red de paso de testigo a 100 Mbps utilizando cable de fibra óptica con una distancia de transmisión superior a 2 Km. La FDDI utiliza una arquitectura de anillo doble para proporcionar redundancia.

Ghost. Fluke Networks acuñó este nuevo término para darle nombre a la energía (ruido) que se detecta en un cable y que parece ser una trama, pero que no lleva un SFD válido. Para calificarla como *ghost*, esta "trama" debe tener por los menos 72 octetos de longitud (preámbulo incluido); en caso contrario, se clasifica como colisión remota.

Gigabit Ethernet. Norma para Ethernet de alta velocidad, aprobada por el comité de normalización IEEE 802.3z en 1996.

IEEE (Instituto de ingenieros eléctricos y electrónicos, *Institute of Electrical and Electronic Engineers)*. Organización profesional entre cuyas actividades se incluyen el desarrollo de normas para las redes y las comunicaciones. Las normas IEEE para las redes LAN son las predominantes actualmente.

IEEE 802.2. Protocolo IEEE LAN que especifica una implementación de la subcapa LLC de la capa de enlace de datos. La IEEE 802.2 administra los errores, el entramado, el control del flujo y la interfaz de servicio de la capa de red (capa 3).

IEEE 802.3. Protocolo IEEE LAN que especifica una implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. La IEEE 802.3 utiliza el acceso CSMA/CD a distintas velocidades en varios medios físicos. Las extensiones de la norma IEEE 802.3 especifican las implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10BASE2, 10BASE5, 10BASE-F,

y 10BROAD36. Las variaciones físicas para Fast Ethernet incluyen 100BASE-TX y BASE-FX.

Información final. Información de control añadida a los datos cuando se encapsulan para su transmisión por la red.

LLC (Control de enlace lógico, *Logical Link Control*). La mayor de las dos subcapas de la capa de enlace de datos que define el IEEE. La subcapa LLC administra el control de errores, el control del flujo, el entramado y el direccionamiento de la subcapa MAC. El protocolo LLC más común es el IEEE 802.2, que incluye variantes sin conexión y orientadas a la conexión.

MAC (Control de acceso al medio, *Media Access Control*). La más inferior de las dos subcapas de la capa de enlace de datos que define el IEEE. La subcapa MAC manipula el acceso a los medios compartidos, como, por ejemplo, si se utiliza el paso de un testigo o la contención. Véase también **LLC**.

MTU (Unidad de transmisión máxima, *Maximun Transmission Unit*). Tamaño máximo del paquete en bytes, que puede manipular una interfaz en particular.

OUI (identificador único de organización, *organizationally unique identifier*). Tres octetos asignados por el IEEE en un bloque de direcciones LAN de 48 bytes.

Retardo de propagación. Tiempo que se necesita para que los datos viajen por la red desde su origen hasta su destino final.

Retardo. El retardo de transmisión aumenta cuando se produce una colisión.

Segmento. Sección de red limitada por puentes, *routers* o *switches*.

Semidúplex. Capacidad para transmitir datos sólo en una dirección en cada momento entre una estación emisora y una estación receptora.

Sin conexión. Datos transferidos sin la existencia de un circuito virtual.

SNMP (Protocolo simple de administración de redes, *Simple Network Management Protocol*). Protocolo de administración de redes que se emplea casi exclusivamente en las redes TCP/IP. SNMP proporciona un significado a los dispositivos de monitorización y control de redes, y administra las configuraciones, la recolección de estadísticas, el rendimiento y la seguridad.

Token Ring. LAN de paso de testigo (*token*) desarrollada y soportada por IBM. Token Ring funciona a 4 ó 16 Mbps sobre una topología en anillo.

Trama larga. Trama mayor que el tamaño máximo legal y que se tiene en cuenta si la trama fue etiquetada.

Unidireccional. Capacidad de transmitir sólo en una dirección entre una estación emisora y una estación receptora. La televisión es un ejemplo de tecnología unidireccional.

Ponga a prueba sus conocimientos

Complete todas las preguntas de repaso para comprobar sus conocimientos sobre los temas y conceptos de este capítulo. Las respuestas las encontrará en el Apéndice C.

1. ¿Cuál de las siguientes no es una subcapa reconocida por el IEEE?
   A. Control de acceso al medio.
   B. Control de enlace de datos.
   C. Control de enlace lógico.
   D. Ninguna de las anteriores.
2. ¿Con qué capas del Modelo de referencia OSI están relacionadas las subcapas reconocidas por el IEEE?
   A. 2 y 3
   B. 1 y 2
   C. 3 y 4
   D. 1 y 3
3. El LLC, como subcapa, participa en el proceso de.
   A. Encriptación.
   B. Encapsulación.
   C. Entramado.
   D. Todas las anteriores.
4. Los primeros seis números hexadecimales de una dirección MAC representan .....?
   A. Número de serie de la interfaz.
   B. Identificador único de organización.
   C. Identificador único de interfaz.
   D. Ninguna de las anteriores.
5. Las direcciones MAC tienen una longitud de _____ bits.
   A. 12
   B. 24
   C. 48
   D. 64
6. ¿Cuál es el nombre del método de acceso utilizado en Ethernet para explicar su funcionamiento?
   A. TCP/IP
   B. CSMA/CD
   C. CMDA/CS
   D. CSMA/CA
7. ¿Dónde reside la dirección MAC?
   A. Transceptor
   B. BIOS de la computadora
   C. NIC

D. CMOS

8. ¿Cuál de las siguientes sentencias describe mejor la comunicación entre dos dispositivos de una LAN?

   A. El dispositivo de origen encapsula los datos en una trama con la dirección MAC del dispositivo de destino y después la transmite. Todos los dispositivos de la LAN la ven, pero los que tengan una dirección que no coincida ignoran la trama.

   B. El origen encapsula los datos y coloca una dirección MAC de destino en la trama. Después coloca la trama en la LAN, donde sólo el dispositivo con la dirección coincidente puede comprobar el campo de dirección.

   C. El dispositivo de destino encapsula los datos en una trama con la dirección MAC del dispositivo de origen y lo coloca en la LAN. El dispositivo cuya dirección coincida elimina la trama.

   D. Cada dispositivo de la LAN recibe la trama y la pasa a la computadora, donde el software decide si la mantiene o la descarta.

9. ¿Qué funciones se asocian con el entramado?

   A. Identifica qué computadoras se están comunicando con otras.

   B. Señala cuándo empieza o termina la comunicación entre computadoras individuales.

   C. Señala las tramas corruptas.

   D. Todas las anteriores.

10. ¿Cómo detecta una computadora de una red LAN un error en una trama?

   A. Envía una copia de la trama de vuelta al emisor para su verificación.

   B. Comprueba la dirección de destino para verificar que la trama ha sido realmente proyectada por ella.

   C. Compara un FCS en la trama con el que la computadora calcula a partir del contenido de la trama.

   D. Calcula una suma de comprobación a partir de los datos de la trama y la devuelve al origen para su verificación.

11. ¿A qué hace referencia el control de acceso al medio?

   A. Al estado en que una NIC ha capturado el medio de red y está preparado para transmitir.

   B. Las normas que gobiernan la captura del medio y su liberación.

   C. Los protocolos que determinan qué computadora en un entorno de medios compartidos tiene permitida la transmisión de datos.

   D. Una secuencia formal de bytes que se ha transmitido.

12. ¿Qué describe mejor a una red CSMA/CD?

   A. Una transmisión de nodos atraviesa toda la red y es recibida y examinada por cualquier nodo.

B. Señales que se envían directamente a la dirección de destino si el origen conoce las direcciones MAC e IP.

C. La transmisión de un nodo va hasta el *router* más cercano, que lo envía directamente hasta el destino.

D. Las señales siempre se envían en modo de difusión.

13. ¿Cuándo se producen las colisiones en Ethernet o en una LAN EEE 802.3?

A. Cuando un nodo coloca un paquete en una red sin informar a los otros nodos

B. Cuando dos estaciones escuchan en espera de tráfico, no oyen nada, y transmiten a la vez.

C. Cuando dos nodos de red envían paquetes a un nodo que ya no efectúa la difusión.

D. Cuando se detecta una fluctuación de fase y el tráfico se desorganiza durante la transmisión normal.

14. ¿Cuál es una importante función de la capa de enlace de datos de la capa 2?

A. Control de enlace lógico.

B. Direccionamiento.

C. Control de acceso al medio.

D. Todas las anteriores.

15. ¿Cuál de los siguientes es un tipo de error de trama en Ethernet?

A. Colisión local.

B. Colisión remota.

C. Colisión atrasada.

D. Todos los anteriores.

16. ¿Qué protocolo es no determinista?

A. Token Ring

B. CSMA/CD

C. IPX

D. RIP

17. ¿Cuál de las siguientes definiciones es cierta acerca de un protocolo MAC determinista?

A. Define las colisiones y especifica qué hacer con ellas.

B. Permite que el *hub* decida el número de usuarios activos en cada momento.

C. Permite que los *hosts* "hagan turnos" para el envío de datos.

D. Permite a los administradores de redes la utilización del "bastón que habla" para controlar el acceso a los medios de cualquier usuario que se considere "problemático".

18. ¿Cómo se llama el área de red en la que se crean y chocan los paquetes de datos?

A. Dominio de colisión.

B. Dominio de red.
C. Dominio de difusión.
D. Segmento de red.

19. ¿Qué describe mejor la difusión?
A. El envío de una trama a muchas estaciones al mismo tiempo.
B. El envío de una trama a todos los *routers* para actualizar simultáneamente sus tablas de enrutamiento.
C. El envío de una trama a todos los *routers* al mismo tiempo.
D. El envío de una trama a todos los *hubs* y puentes al mismo tiempo.

20. El empleo de repetidores _____ el dominio de colisión.
A. Reduce.
B. No tiene efecto en.
C. Extiende.
D. Ninguna de las anteriores.

21. El proceso de usar dispositivos de red complejos, como puentes, *switches* y *routers*, para dividir los dominios de colisión se conoce como
A. Seccionamiento.
B. Segmentación.
C. Reducción del dominio de colisión.
D. Ninguna de las anteriores.

Objetivos

Una vez completado este capítulo, estará en condiciones de:

- Comprender la evolución de la tecnología Ethernet.
- Comprender el método MAC, el formato de trama y el proceso de transmisión de las tecnologías Ethernet.
- Comprender el medio específico y la codificación usada en cada tecnología Ethernet.
- Comprender los *pinouts* y el cableado típicos de cada tecnología Ethernet.
- Comprender las consideraciones básicas acerca de la arquitectura de cada tecnología Ethernet.
- Definir la microsegmentación.
- Describir el puente a la capa 2.
- Describir cómo opera un *switch* de una LAN.
- Describir la transmisión *dúplex*.
- Identificar los métodos de conmutación más comunes: de almacenamiento y envío (*Store-and-Forward)*, por método de corte (*cut-through)* y de liberación de fragmentos (*fragment-free*).
- Describir las funciones y características del STP (Protocolo de árbol de extensión *Spanning Tree Protocol*).
- Describir cómo trabaja el STP.
- Describir los distintos estados de los puertos STP.

CAPÍTULO 6

Tecnologías Ethernet y conmutación Ethernet

Ethernet, junto con sus protocolos asociados IEEE 802.3, es una de las normas de red importantes del mundo. Debido al gran éxito de la Ethernet original y a lo silencioso diseño, ha evolucionado a lo largo del tiempo. Esta evolución fue la respuesta al desarrollo de las modernas LAN, y desde luego dicha evolución continuará para dar cabida a futuras demandas de las capacidades de la red.

En el capítulo anterior vimos tanto la historia de Ethernet como la de sus normas asociadas. También aprendimos que el término *Ethernet* hace referencia a toda la familia de tecnologías Ethernet. En este capítulo nos centraremos con más detalle en dichas tecnologías.

Además, este capítulo presenta las técnicas de *bridging* y conmutación de la capa 2. Estas son técnicas que disminuyen la congestión en las LAN reduciendo el tráfico y aumentando el ancho de banda.

Por último, este capítulo estudia el STP, muestra cómo funciona este protocolo y explica el estado de los puertos de los *switch* STP.

Consulte los capítulos e-Lab Activities, Videos y PhotoZooms asociados que encontrará en el CD-ROM que incluye este libro. Los elementos de dicho CD-ROM están diseñados para complementar el material y reforzar los conceptos introducidos en este capítulo.

Ethernet a 10 Mbps y a 100 Mbps

Esta sección trata las especificaciones de las más importantes variantes de Ethernet. El objetivo no es memorizar todas las características de cada uno de los tipos Ethernet, sino asimilar un sentido general acerca de lo que es común en todos los modelos de Ethernet y cuáles son los puntos fuertes y débiles de las Ethernet comerciales más comunes.

La popularidad de Ethernet comenzó con el grueso cable coaxial 10Base5. Sin embargo, el cable *Thicknet* tuvo unas indeseables propiedades de instalación. 10Base2 utilizó Thinnet (cable coaxial más delgado que era más sencillo de instalar y terminar; la distancia disminuyó de 500 a 185 metros). Esta tendencia hacia la sencillez de instalación y la reducción de costes dio un gran paso hacia delante con la introducción del 10BaseT basado en UTP. Sin embargo, la distancia que una señal sin repetir podía recorrer disminuyó hasta 100 metros, lo que obligó a la introducción de repetidores y, más adelante, repetido-

res multipuerto (*hubs*). El concepto de repetidor permitió las redes 10BaseT de más de 500 metros. Como los grupos de trabajo crecieron en tamaño y las aplicaciones en complejidad, el ancho de banda compartido del *hub* se convirtió en un factor limitador. La introducción de los *switches* Ethernet 10BaseT solventó el problema de las limitaciones de longitud y ancho de banda (los enlaces estación-*switch* se transformaron entonces en punto-a-punto).

La potencia, versatilidad y bajo coste de 10BaseT coincidió con una explosión en el número de usuarios de red, el de usuarios Internet (lo que, a su vez, incrementó el tráfico de la propia red) y de la complejidad de las aplicaciones. La solicitud de anchos de banda mayores se tradujo en la aparición de Fast Ethernet. La versión con cable de cobre de Fast Ethernet que se comercializó con éxito fue 100BaseTX, y se desarrollaron muchas características para permitir la interoperabilidad entre sistemas 10BaseT (por ejemplo, la emergencia de las interfaces 10/100). Para competir con la tecnología *backbone*/LAN de FDDI, se desarrolló 100BaseFX basado en fibra. Todas estas variantes de Ethernet mantuvieron una serie de conceptos invariables: el direccionamiento MAC, el formato de trama y el método CSMA/CD MAC.

Versiones de Ethernet de 10 Mbps

La Figura 6.1 muestra un subconjunto de las implementaciones de la capa física que se puede desplegar para soportar Ethernet. Las implementaciones **10Base5**, **10Base2** y **10BaseT** de Ethernet están consideradas como implementaciones heredadas y están explicadas en las secciones siguientes.

Subcapa de control de enlace lógico										
Control de acceso al medio 802.3										
Subcapa de señalización física	10Base5 (500 m) 50 Ohm Coaxial N-Style	10Base2 (185 m) 50 Ohm Coaxial BNC	10BaseT (100 m) 100 Ohm UTP RJ45	10Base-TX (100 m) 100 Ohm UTP RJ45	100Base-FX (228_412 m) Fibra MM SC	1000Base-T (100 m) 100 Ohm UTP RJ45	1000BASE-SX (220-550 m) Fibra MM SC	1000BASE-LX (550-5000 m) Fibra MM SC	10BASE-(Various) Fibra MM o Sm SC
Medio físico										

Figura 6.1. Tipos de Ethernet.

A través de todas las versiones de Ethernet, cuatro han sido las cosas que han permanecido invariables:

- Los parámetros de temporización.
- El formato de la trama.

- El proceso de transmisión.
- Una regla de diseño básica.

Una vez que aprenda los que estas tres históricamente importantes versiones tienen en común, estudiaremos cada una con más detalle.

10Base5, 10Base2 y 10BaseT comparten los mismos parámetros de temporización, tal y como puede verse en la Tabla 6.1. Observe que el tiempo de bit a 10 Mbps = 100 nanosegundos = 0.1 microsegundo = 1 diezmillonésima de segundo.

Tabla 6.1. Parámetros de una operación Ethernet a 10 Mbps.

Parámetro	Valor
Tiempo de bit	100 nanosegundos
Tiempo de ranura	512 tiempos de bit
Espacio ente tramas	96 bits*
Límite de intento de colisión	16
Límite de retardo de colisión	10
Tamaño de congestión de colisión	32 bits
Tamaño máximo de la trama sin etiquetar	1518 octetos
Tamaño mínimo de la trama	512 bits (64 octetos)

*El valor mostrado es el espacio oficial entre tramas.

El formato de la trama es común a 10Base5, 10Base2 y 10BaseT. La Figura 6.2 muestra una trama Ethernet tal y como se ve en la subcapa MAC.

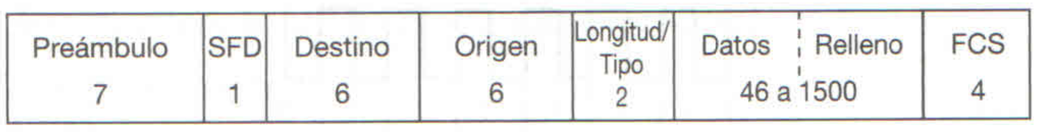

Figura 6.2. Trama Ethernet.

El proceso de transmisión Ethernet es idéntico hasta la parte inferior de la capa física OSI. Ya que la trama pasa desde la subcapa MAC a la capa física, son muchos los procesos que tienen lugar antes de que los bits sean colocados en el medio desde la capa física. Uno de dichos procesos, que es particularmente importante a este nivel, es la señal SQE (Error de calidad de señal, *Signal Quality Error*). Esta señal es habitual en cualquier tecnología de red que pueda ver. En la capa física, la red está "viva", no sólo con los datos del usuario, sino también con otra serie de comunicaciones que aseguran un correcto funcionamiento de la red. SQE siempre se utiliza en conexiones semidúplex; no es necesaria, aunque si está permitida, en operaciones dúplex. SQE está activa en los siguientes casos:

- Dentro de los 4 a 8 microsegundos que siguen a una transmisión normal para indicar que la trama de ida fue transmitida satisfactoriamente.
- Siempre que existe una colisión en el medio.

- Siempre que aparezca una señal inapropiada en el medio. Entre otras, las señales inapropiadas pueden incluir la detección de ruidos o los reflejos provocados por un cable en mal estado (existen condiciones distintas dependiendo del medio).
- Siempre que una transmisión se ha interrumpido debido al ruido, es decir, ha transmitido más allá de lo permitido.

Todas las formas de Ethernet a 10 Mbps recuperan octetos recibidos desde la subcapa MAC y llevan a cabo un proceso llamado **codificación en línea**. La codificación en línea describe la forma en la que los bits son marcados en el hilo. Las **codificaciones** más sencillas, como NRZ (código sin retorno a cero, ***nonreturn to zero***) en donde un bit 1 es 5 voltios [V] y el 0 es 0V, suelen tener temporizaciones y características eléctricas poco adecuadas. Por tanto, los códigos de línea han sido proyectados para tener propiedades de transmisión adecuadas y ajustadas a cada medio. La codificación en línea utilizada en los sistemas a 10 Mbps recibe el nombre de **codificación Manchester**. La Figura 6.3 muestra un ejemplo de este tipo de codificación. El eje "y" es el voltaje, mientras que el "x" representa el tiempo.

Nota

En la codificación NRZ, las señales se mantienen en niveles de voltaje constantes, sin transiciones de señal durante el intervalo de un bit (no hay retorno al nivel de 0V).

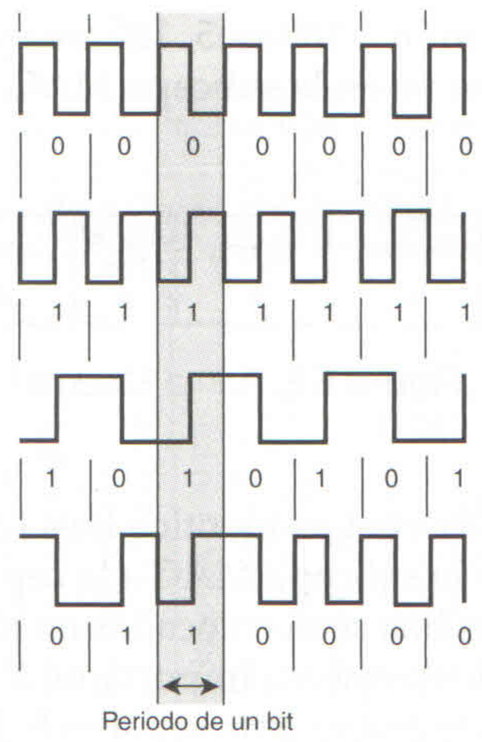

Figura 6.3. Ejemplos de codificación Manchester.

La **codificación Manchester** se basa en la dirección de la transición de contorno en la mitad de la ventana de temporización para determinar el valor binario para cada periodo de bit. En el ejemplo de codificación mostrado en la Figura 6.3, una de estas ventanas se encuentra resaltada verticalmente a través de los cuatro ejemplos en forma de onda.

onda superior tiene un borde de caída en la mitad de la ventana de temporización, lo que se interpreta como un 0 binario.

El resultado es que en el centro de la ventana de temporización de la segunda onda, existe un límite elevado, lo que se interpreta como un 1 binario.

En el tercer ejemplo de onda, en lugar de una secuencia repetida del mismo bit, existe una secuencia binaria alternativa. En los dos primeros ejemplos, la señal debe transitar antes entre cada periodo de bit para que pueda tener la misma dirección de transición en la mitad de la ventana de temporización. Con datos binarios alternativos, no es necesario volver al nivel de voltaje previo en preparación para el siguiente límite en el centro de la ventana de temporización. En su lugar, cada vez que existe una separación larga entre un límite y otro, puede estar seguro de que ambos límites representan el centro de una de estas ventanas. El cuarto ejemplo de onda son datos aleatorios que le permiten verificar que siempre que exista una separación importante entre dos transiciones, ambos límites están en el centro de la ventana de temporización y representan el valor binario para dicha ventana.

Las Ethernet heredadas a 10 Mbps tienen otras características de arquitectura comunes. Todas estas versiones están referenciadas como **Ethernet compartidas** porque comparten un dominio de colisión común. Esto no sólo está permitido, sino que es normal que una red Ethernet pueda contener diversos tipos de medios (por ejemplo, 10Base5, 10Base2, 10BaseT, etc.). La norma va más allá de esta forma para asegurar que la interoperabilidad sea mantenida. Sin embargo, cuando se implementa una red con mezcla de medios, es importante prestar especial atención al diseño de la estructura global. Resulta muy sencillo violar los límites máximos de retardo en el momento en el que la red crece y se hace más compleja. Los límites de temporización están basados en parámetros como éstos:

- Longitud del cable y su retardo de propagación.
- Retardo de los repetidores.
- Retardo de los transceptores (incluyendo NICs, *hubs* y *switches*).
- Merma del hueco entre tramas.
- Retardos dentro de la estación.

Actividad de laboratorio

Decodificación de la forma de onda

El propósito de esta práctica es integrar los conocimientos acerca de los medios de la red, las capas OSI 1, 2 y 3 y Ethernet, decodificando una onda digital de una trama Ethernet.

Regla 5-4-3

La Ethernet a 10 Mbps opera dentro de los límites de temporización ofrecidos por una serie de no más de cinco segmentos separados por no más de cuatro repetidores. Es decir, no se pueden conectar más de cuatro repetidores en serie entre dos estaciones distantes. Las implementaciones coaxiales tienen un requerimiento más y es que no puede haber más de tres segmentos poblados entre dos estaciones diferentes. Los otros dos segmentos

coaxiales permitidos son utilizados para extender el diámetro del dominio de colisión y reciben el nombre de segmentos de enlace. La característica principal de uno de estos segmentos es que tiene exactamente dos dispositivos conectados. Todos los enlaces de par *trenzado, como 10BaseT,* coinciden en la definición de segmento de enlace.10Base5.

La Ethernet original (10Base5; año 1980) transmitía 10 Mbps a través de un único y grueso cable coaxial, de hay su nombre de *Thicknet*. 10Base5 es importante por razones históricas: fue el primer medio usado por Ethernet. 10Base5 formaba parte de la norma 802.3 original, y todavía puede encontrarse como parte de las instalaciones heredadas. Ésta no es una elección adecuada para las redes nuevas porque su principal beneficio, la longitud, puede alcanzarse de otras maneras. Aun cuando los sistemas 10Base5 son baratos y no requieren de configuración (no son necesarios *hubs* para ampliar la longitud del sistema), los componentes básicos como las NICs son muy difíciles de encontrar, y la tecnología es muy sensible a las reflexiones en el cable. Además, los sistemas 10Base5 son muy dependientes del cable a lo largo de todo el dominio de colisión y esto supone un importante punto de fricción.

La temporización, el formato de la trama y el proceso de transmisión fueron descritos anteriormente en el Capítulo 5, y son comunes a todas las redes Ethernet a 10 Mbps heredadas.

10Base5 utiliza señales con codificación Manchester en cable coaxial grueso. La Figura 6.4 es un ejemplo de una señal 10Base5, que es transmitida entre, aproximadamente, 0V y –1V. 10Base5 podría estar inactiva potencialmente (0V) durante días si ninguna estación desea transmitir. Y, además, es asíncrona.

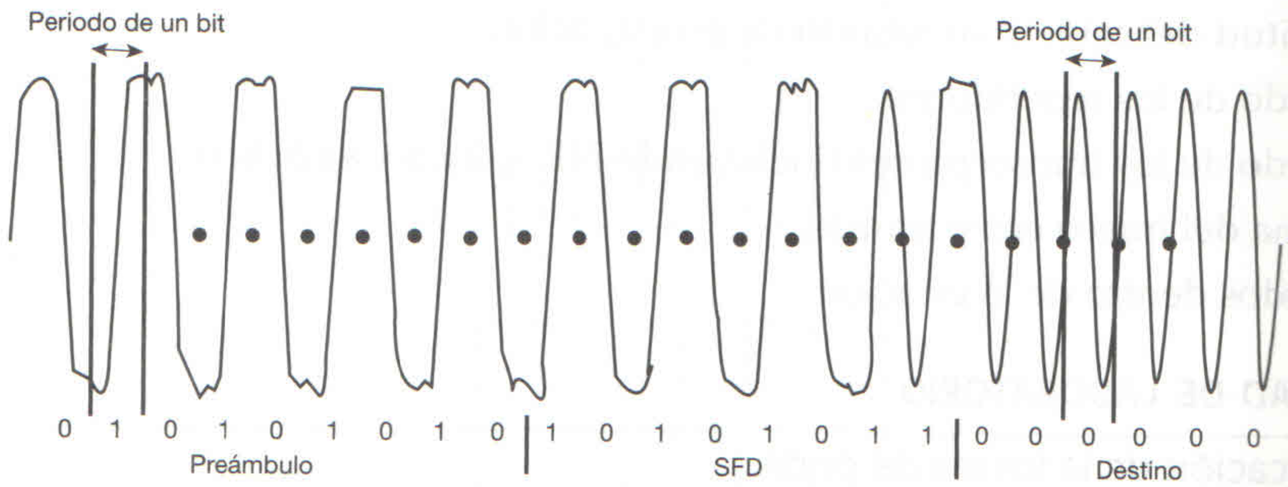

Figura 6.4. Señal 10Base5 decodificada.

En la Figura 6.4, se han añadido marcas de temporización para ayudarle a reconocer las ventanas de temporización desde las que se decodifica el dato binario. El eje "y" representa el voltaje mientras que el "x" es el tiempo. El voltaje se ha medido entre el conductor central y la cubierta externa del cable coaxial.

Un cable coaxial 10Base5 **grueso** (véase la Figura 6.5) dispone de un sólido conductor central, una mínima velocidad nominal de propagación (NVP, *Nominal Velocity of Propagation*) de 0,77c y 50 ohmios de impedancia; utiliza conexiones de estilo N para abonados. Cada uno de los cinco máximos segmentos de un coaxial grueso puede superar los 50

metros de longitud (1640 pies) y cada estación se conecta a un transceptor del cable a través de un cable AUI (Interfaz de conexión a unidad, *Attachment Unit Interface*), que puede superar los 50 metros (164 pies). El cable es largo, pesado y difícil de instalar, pero las limitaciones de distancia fueron favorables; esto prolongó su uso en ciertas aplicaciones.

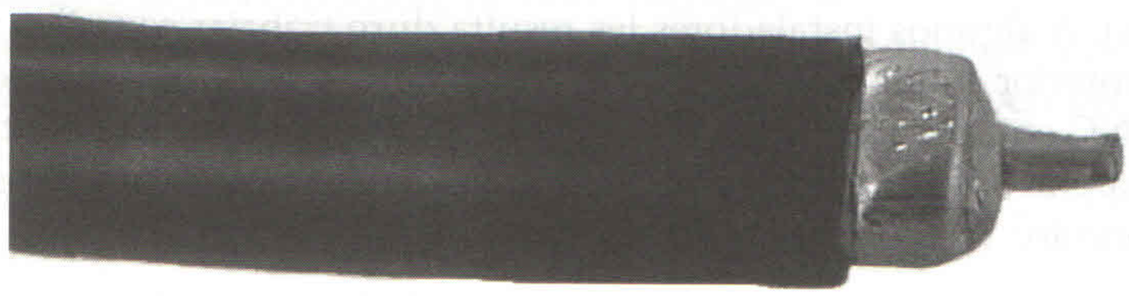

Figura 6.5. Cable 10Base5 *Thicknet*.

Otras especificaciones o limitaciones del cable 10Base5 son las siguientes:

- Sólo puede transmitir una estación cada vez (o podrá ocurrir una colisión).
- 10Base5 **sólo** puede funcionar en modo semidúplex, sujeto a las reglas CSMA/CD.
- Más de 100 estaciones, incluyendo los repetidores, pueden existir en cualquier segmento 10Base5 individual.

10Base2

10Base2 (originalmente, 802.3a-1985) fue presentado en 1985 porque su cable coaxial de menor tamaño, peso más ligero y mayor flexibilidad hacía la instalación mucho más sencilla que 10Base5. Debido al uso de un cable más delgado, 10Base2 suele recibir el nombre de *Thinnet*. 10Base2 aun permanece en redes heredadas. Aunque en la actualidad éstos son motivos menores para la instalación de una red 10Base2, su bajo coste y la no necesidad de hubs la hacen atractiva en ciertas situaciones. Esencialmente, 10Base2 no requiere configuración, aun cuando la obtención de NICs es extremadamente complicada. Al igual que ocurre con los sistemas 10Base5, los 10Base2 son muy dependientes del cable a lo largo de todo el dominio de colisión, lo que supone un importante punto de problemas.

La temporización, el formato de la trama y el proceso de transmisión fueron descritos anteriormente en el Capítulo 5 y son comunes a todas las redes Ethernet a 10 Mbps heredadas.

10Base2 utiliza señales con codificación Manchester en cable coaxial fino. Una señal 10Base2 se transmite entre, aproximadamente, 0V y –1V (el eje "y" es el voltaje y el "x" es el tiempo). El voltaje es medido entre el conductor central y la cubierta externa del cable coaxial.). 10Base2 podría estar inactiva potencialmente (0V) durante días si ninguna estación desea transmitir. Y, además, es asíncrona.

Las computadoras de la LAN fueron unidas como las cuentas de un collar por una serie de largos cables coaxiales sin división. Dichos cables fueron conectados mediante BNC (Conectores navales británicos, *British Naval Connectors*) a un conector en forma de T en la

NIC, tal y como puede verse en la Figura 6.6. Este único cable coaxial fue el bus compartido por la red. La estaciones de trabajo podían ser movidas y conectadas de nuevo de forma sencilla, además de permitirse la adición de nuevas estaciones a la LAN. Por otro lado, 10Base2 usó el mismo protocolo dúplex Ethernet original.

Un cable coaxial 10Base2 **fino**, tal y como se muestra en la Figura 6.8, tiene un conductor central trenzado (asegúrese de especificar esta característica cuando se compren cables nuevos). A algunos instaladores les resulta duro trabajar con ellos y utilizan cables coaxiales de interior sólido). Tiene una NVP de 0,65c, 50 ohmios de impedancia y utiliza conexiones BNC en forma de T. Cada uno de los cinco máximos segmentos de un coaxial fino puede superar los 185 metros de longitud (600 pies) y cada estación se conecta directamente al conector BNC T en el cable.

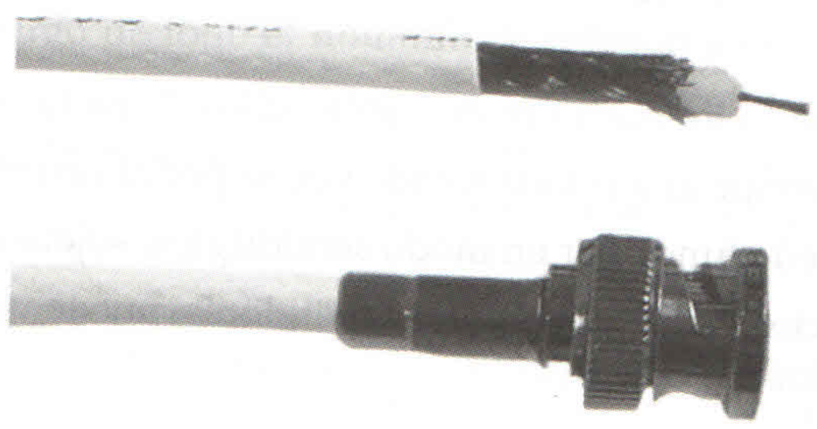

Figura 6.6. Thinnet y conector BNC.

10BaseT

10BaseT (originalmente, 802.3i-1990) sustituyó el cable de cobre UTP más barato y sencillo de instalar por cable coaxial. Dicho cable conectaba un dispositivo de conexión central, un *hub* o un *switch*, que contenía el bus compartido. El tipo de cable usado en 10BaseT, las distancias que dicho cable podía alcanzar desde el *hub* y la forma en que el UTP fue instalado, interconectado y analizado fueron estandarizados en un "sistema de cableado estructurado", lo que con el tiempo se extendió a la topología en estrella o en estrella extendida. 10BaseT fue originalmente un protocolo semidúplex, aunque más tarde adquirió características dúplex. La explosión de la popularidad de Ethernet en los 90 (cuando pasó a dominar la tecnología LAN) hizo que 10BaseT funcionara con UTP de categoría (Cat) 5. Para refrescar su memoria en cuanto a topologías y medios de red, consulte los Capítulos 2 y 3.

La temporización, el formato de la trama y el proceso de transmisión fueron descritos anteriormente y son comunes a todas las redes Ethernet a 10 Mbps heredadas.

10BaseT utiliza señales con codificación Manchester sobre categoría 3 UTP (ahora 5 o superior).

Ethernet a 10 Mbps es asíncrona, y el cable suele estar completamente inactivo (sin) durante largos periodos de tiempo entre diferentes transmisiones. Los enlaces 10BaseT in-

...en un **pulso de enlace** cada 125 milisegundos (ocho veces por segundo), aunque puedan estar totalmente inactivas. Las redes 10BaseT están "vivas" mediante estos pulsos de enlace.

Un cable 10BaseT (UTP) de par trenzado sin apantallar tiene un poderoso conductor por cada hilo de 90 metros de longitud horizontal, con un diámetro que oscila entre 0,4 y 0,6 milímetros (de 26 a 22 AWG [Calibre de hilo americano, *American Wire Gauge*]). Los 10 metros de latiguillo permitidos utilizan un cable trenzado de dimensiones similares por temas de durabilidad, porque se espera que experimente dobleces repetidas. El cable UTP adecuado tiene un NVP mínimo de 0,585c, 100 ohmios de impedancia y utiliza conectores modulares RJ-45 de ocho pines tal y como se especifica en el ISO/IEC 8877. La longitud del cable entre una estación y un *hub* oscila entre 0 y 100 metros (de 0 a 328 pies), aunque la longitud máxima exacta viene determinada por el retardo en la propagación a través del segmento de enlace (cualquier longitud que no exceda de 1000 nanosegundos de retraso es aceptable). Habitualmente, un hilo UTP de 0,5 milímetros de diámetro (24 AWG) cumplirá las necesidades a 100 metros.

Aunque el cable de categoría 3 es adecuado para su uso en redes 10BaseT, es muy recomendable que cualquier instalación de un nuevo cable se haga con categoría 5e o, incluso, con mejores materiales. Utilice los cuatro pares y use la disposición de pines del cable T568A o T568B. Con este tipo de instalación, debería ser posible tratar con diferentes protocolos de acceso al medio (incluyendo 1000BaseT) sobre el mismo cable sin cambiar la instalación eléctrica.

La Tabla 6.2 muestra la distribución de pines para una conexión 10BaseT. Observe que existen dos rutas diferentes para transmitir/recibir (aun cuando sólo existe un cable coaxial).

Tabla 6.2. Configuración de pines de un cable 10BaseT.

Número de pin	Señal
	TD+ (Transmisión de datos, señal diferencial va a positivo)
	TD– (Transmisión de datos, señal diferencial va a negativo)
	RD+ (Recepción de datos, señal diferencial va a positivo)
	Sin utilizar
	Sin utilizar
	RD+ (Recepción de datos, señal diferencial va a negativo)
	Sin utilizar
	Sin utilizar

La Figura 6.7 muestra las conexiones físicas y conceptuales establecidas entre dos estaciones. Es necesario un cable cruzado de modo que Tx en el dispositivo A envíe las señales a Rx en el B. Observe que existen dos conexiones punto-a-punto (de TxA hacia RxB y de TxB hacia RxA).

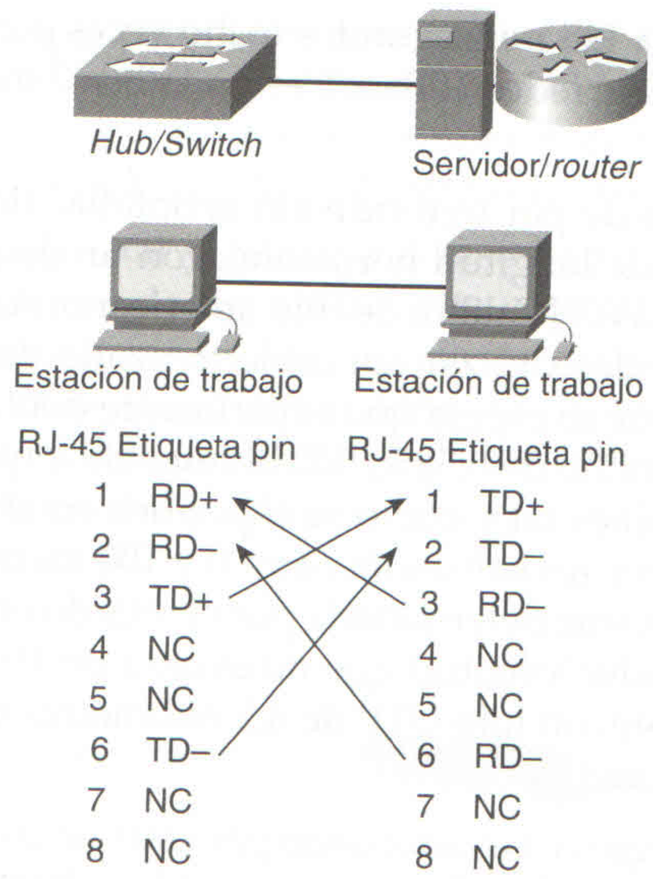

Figura 6.7. 10BaseT de estación a estación.

La Figura 6.8 muestra la conexión entre estaciones y repetidores, *hubs* o *switches*. También podría usar la misma conexión entre un *router* y un *hub* o un *switch*. Se usa un cable recto. Observe que el interior del *hub* es una topología en bus, lo que es un dominio de colisión. Cuando se conecta una estación a un *switch* a través de un cable recto, todos los enlaces individuales son punto-a-punto. La estructura de la circuitería del *switch* permite un ancho de banda completo simultáneo entre pares de puertos sin colisiones.

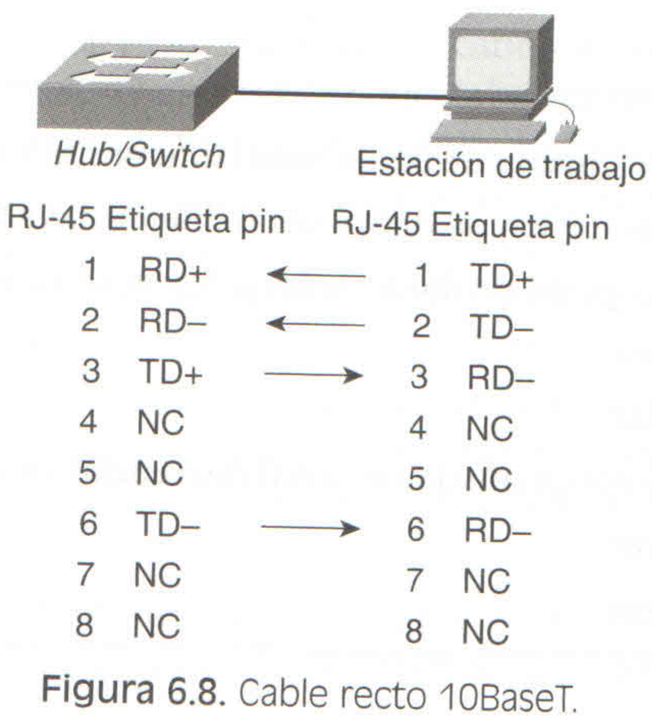

Figura 6.8. Cable recto 10BaseT.

Debido a que las conexiones estación-estación, *switch-switch* y estación-*switch* son enlaces punto-a-punto, disponen de dos canales físicos de comunicación separados

pares de hilos UTP separados. En este caso, las colisiones no son eventos físicos, sino el resultado de la decisión de no permitir simultáneamente Tx y Rx. Por tanto, semidúplex (objeto de la imposición administrativa de CSMA/CD) o dúplex (no ocurren colisiones físicas) es una elección de configuración. La mayoría de las veces, estas conexiones funcionan en modo dúplex, lo que no sólo elimina las colisiones sino que también dobla el rendimiento de la conexión. Cuando fue presentado por primera vez, la norma IEEE correspondiente tenía el título 802.3x-1997 Full-Duplex. Sin embargo, las conexiones estación-*hub* implican a la topología en bus del interior de este último, un dominio físico de colisión. Por tanto, esta conexión **sólo** puede ejecutarse en modo semidúplex y está sujeta al CSMA/CD debido a la naturaleza física de la estructura.

10BaseT porta 10 Mbps de tráfico en modo semidúplex; sin embargo, 10BaseT en modo dúplex puede llegar a intercambiar 20 Mbps (aunque, de nuevo, parte de dicho tráfico se debe al consumo de recursos, no a los datos del usuario). Este concepto crecerá en importancia a medida que vaya creciendo también la velocidad de los enlaces Ethernet.

Arquitectura 10BaseT

Los enlaces 10BaseT suelen consistir en una conexión entre una estación y un *hub* o switch. Los *hubs* deben concebirse como repetidores multipuerto y se cuentan hacia el límite de los repetidores situados entre estaciones distantes. Los *switches* pueden definirse como puentes multipuerto y son la causa de la limitación a 100 metros, aunque no hay límite en el número de estos elementos entre estaciones distantes.

Aunque los *hubs* pueden ser enlazados en serie (lo que a veces recibe el nombre de cadena enlazada, o cascada), es mejor evitar esta situación siempre que sea posible para no violar el límite del retardo máximo entre estaciones distantes. El tamaño físico de una red 10BaseT está sujeta a las mismas reglas que las 10Base5 y 10Base2 en cuanto al número de repetidores. Cuando son necesarios varios *hubs*, es mejor conectarlos en orden jerárquico para crear una estructura de árbol en lugar de una cadena. Además, el rendimiento puede ser mejorado cuantos menos repetidores separen las estaciones. Los *hubs* "apilables", o concentradores con planos traseros comunes que soportan tarjetas adaptadoras multipuerto, permiten la conexión de un gran número de estaciones a un dispositivo que cuenta como un único *hub* (repetidor). Los *switches* de cadena enlazada son una mejor elección pero están sujetos a restricciones.

Todas las distancias entre estaciones son aceptables, aunque en una dirección, la arquitectura es su límite. El aspecto más importante a considerar es cómo reducir al máximo el retardo entre estaciones distantes (independientemente de la arquitectura y los tipos de medios involucrados). Un retardo mínimo ofrece un rendimiento mucho más adecuado. Considere las siguientes arquitecturas:

- En la Figura 6.9 hay cinco segmentos y cuatro repetidores desde la Estación 1 a cualquier otra estación. En las conexiones 10BaseT no se aplica el máximo de tres segmentos con estaciones porque no existe ninguna otra en el mismo cable. Cada conexión está descrita como un segmento de conexión.

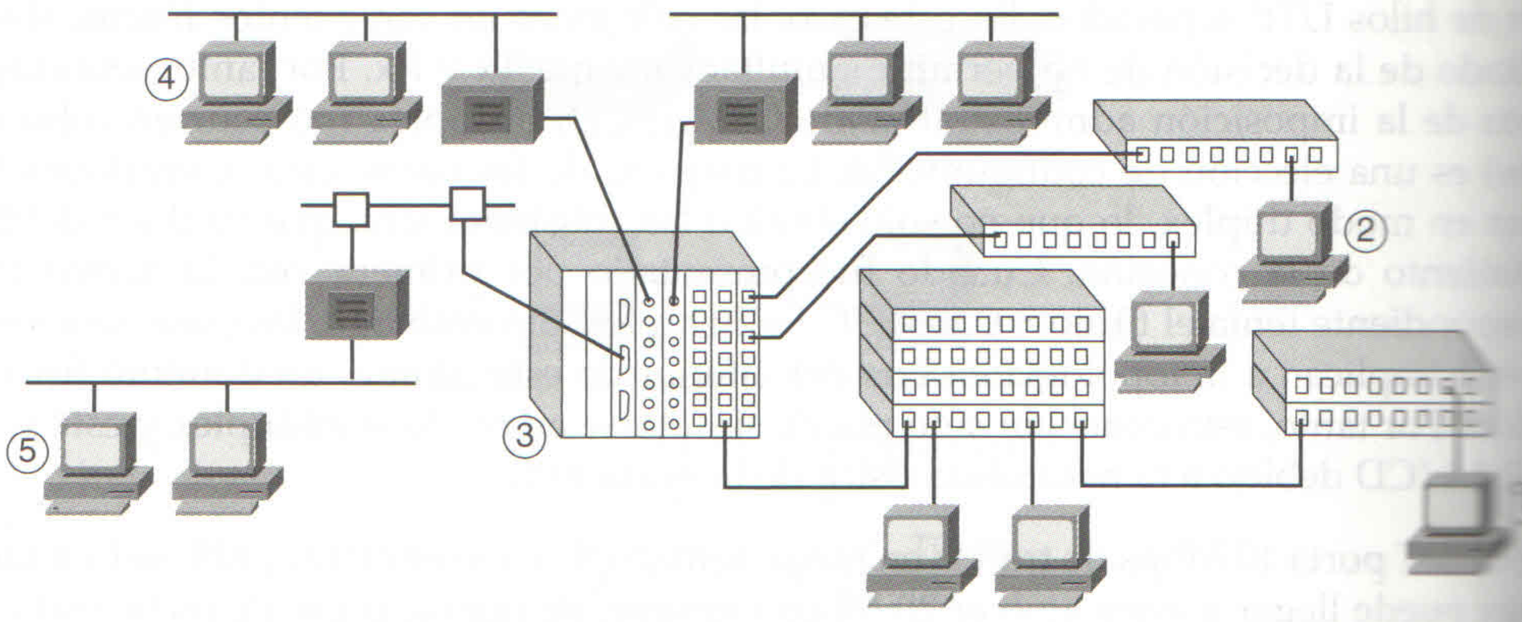

Figura 6.9. Ejemplo 1 de arquitectura mixta a 10 Mbps.

- En la Figura 6.10, desde una estación (excepto desde la 1) a cualquier otra, la ruta sólo tiene tres repetidores. Debido a que estas rutas alternativas incluyen enlaces 10Base5 y 10Base2, es necesario aplicar los otros requerimientos (como el de disponer de sólo tres segmentos con estaciones).

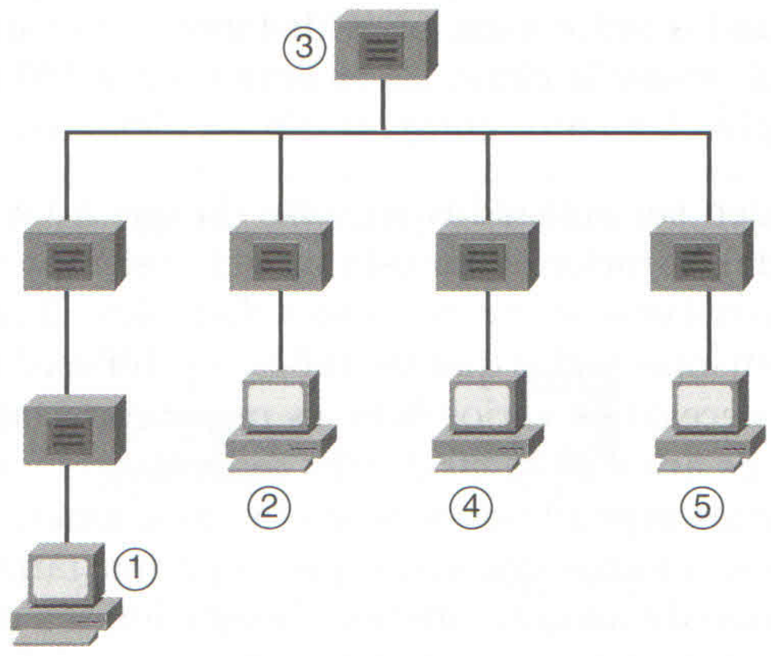

Figura 6.10. Ejemplo 2 de arquitectura mixta a 10 Mbps.

Los enlaces 10BaseT pueden tener distancias por encima de 100 metros sin repetidor. Puede parecer una distancia muy larga, pero suele utilizarse como forma rápida de cablear un edificio. Los *hubs* pueden resolver este asunto de la distancia, aunque sólo pueden encadenarse cuatro repetidores debido a las necesidades de temporización. La rápida introducción de *switches* ha hecho menos importante esta limitación de distancia. Supongamos que las estaciones estén localizadas dentro de los 100 metros que las separan de un *switch*. La dicha distancia de 100 metros comienza a partir de ese *switch*, el cual podría conectarse a su vez con otro a 100 metros y así sucesivamente. Debido a que la mayoría de las Ethernet 10BaseT modernas están conmutadas, esos son los límites prácticos entre dispositivos de

…logías en anillo, estrella y estrella extendida están permitidas. El problema se centra …nces en la topología lógica y en el flujo de datos, no en la temporización o en las limi…nes de distancia.

La Tabla 6.3 muestra las características de los enlaces 10BaseT.

…a 6.3. Características de los enlaces 10BaseT.

…nexión	Segmento máximo
…ación a estación, estación a *switch*, …a *switch*	100 metros, sin limitaciones en la cadena enlazada.
…ación a *hub*	100 metros, pero sujeta a la regla de cuatro repetidores.

…siones Ethernet a 100 Mbps

…thernet a 100 Mbps, también conocida como Fast Ethernet (en comparación con la …net original a 10 Mbps), era una serie de tecnologías. Las dos tecnologías que se hicie…más importantes comercialmente hablando son **100BaseTX** (basada en cobre UTP) y …BaseFX (basada en fibra óptica multimodo). Esta sección examina primero las similitu…entre ambas tecnologías para después centrarse en sus diferencias.

…Tres son las cosas que comparten 100BaseTX y 100BaseFX:

- Los parámetros de temporización.
- El formato de la trama.
- Las partes del proceso de transmisión.

La Tabla 6.4 muestra los parámetros de una operación Ethernet a 100 Mbps.

…a 6.4. Parámetros de una operación Ethernet a 100 Mbps.

…metro	Valor
…po de bit	10 nanosegundos
…po de ranura	512 tiempos de bit
…ente tramas	96 bits
…o de intento de colisión	16
…o de retardo de colisión	10
…o de congestión de colisión	32 bits
…o máximo de la trama sin etiquetar	1518 octetos
…o mínimo de la trama	512 bits (64 octetos)

100BaseTX y 100BaseFX comparten los mismos parámetros de temporización. Observe que 1 tiempo de bit en una Ethernet a 1000 Mbps es 10 nanosegundos = 0,01 microsegundos = 1 100 millonésima parte de un segundo.

El formato de la trama a 100 Mbps es el mismo que el de la trama a 10 Mbps. A diferencia de Ethernet a 10 Mbps, en que el proceso era el mismo para todas las tecnologías hasta que la señal era aplicada al medio.

Fast Ethernet implementa un importante incremento de la velocidad. Debido a ello son necesarios una serie de requerimientos extra. Los bits enviados tienen una duración más corta pero la operación ocurre con más frecuencia. Esto implica que la temporización debe ser más cuidadosa, y que las transmisiones requieran frecuencias cercanas a los límites del ancho de banda del medio y se vuelvan especialmente sensibles a los ruidos. Para solucionar todos estos inconvenientes en la sincronización, ancho de banda y **SNR** (**Tasa de señal-ruido**, ***Signal-to-Noise Ratio***), la Ethernet a 100 Mbps utiliza dos pasos diferentes para la codificación. La idea básica es usar códigos (que pueden ser diseñados para cumplir ciertas propiedades) para representar los datos del usuario de forma que resulten eficientes a la hora de transmitir, incluyendo sincronización, uso óptimo del ancho de banda y características SNR mejoradas. La primera parte de la codificación utiliza una técnica llamada 4 bits (4B/5B) mientras que la segunda es la codificación específica propia del cobre o la fibra.

Las dos versiones de Ethernet a 100 Mbps tratadas en este libro, 100BaseTX y 100BaseFX, codifican *nibbles* (agrupaciones de 4 bits) desde las partes superiores de la capa MAC. Los patrones de 4 bits son convertidos en símbolos de 5 bits y éstos, a su vez, en información de control (como trama de inicio, trama de finalización o condiciones inherentes a si el medio está inactivo). La trama a transmitir está compuesta por símbolos de control y símbolos de datos (grupos de códigos de datos). De nuevo se hace necesaria esta complejidad para alcanzar el incremento de la velocidad de estas redes.

Tras la codificación 4B/5B, los bits (en forma de grupos de códigos) aun deben ser situados en el medio (es decir, deben ser codificados para la línea). La conversión de los bits implica que ahora se deban transmitir 125 Mbps en lugar 100 Mbps durante el mismo intervalo de tiempo. Esto supone una serie de requerimientos más estrictos en el medio, transmisores y receptores utilizados. Por ejemplo, el cable debe ser comprobado a frecuencias más altas para garantizar unas características de transmisión adecuadas. Cada vez que no haya datos para transmitir, los grupos correspondientes a "código de inactividad" se siguen enviando para rellenar los periodos vacíos y mantener la sincronización. En este punto, la ruta que sigue el dato difiere según se esté usando cobre (100BaseTX) o fibra (100BaseFX) como medio.

100BaseTX

La necesidad de redes más rápidas llevó a la aparición de 100BaseT Fast Ethernet y una norma de autonegociación en 1995 (originalmente 802.3u-1995). 100BaseT incrementa la tasa de bit de Ethernet a 100 Mbps. 100BaseTX fue la versión UTP de categoría 5 de 100BaseT que tuvo éxito comercial. Pronto, los *hubs* y *switches* 10/100 permitían transmisiones Ethernet a la tasa original de 10 Mbps para compartir la red con tramas enviadas a 100 Mbps.