6ª Edición

Comunicaciones y Redes de Computadores

Prentice Hall

William Stallings

Contenido

Prólogo

OBJETIVOS

Este libro intenta dar una visión unificada del amplio campo que abarcan las comunicaciones y redes de computadores. La organización del libro refleja un intento de estructurar este vasto campo en partes comprensibles, y de construir, poco a poco, una visión panorámica de su estado actual. El libro destaca principios básicos y temas de importancia fundamental que conciernen a la tecnología de este área; además, proporciona una discusión detallada de temas de vanguardia.

Para unificar la discusión se utilizan los siguientes criterios básicos:

- **Principios:** a pesar de que el alcance de este libro es muy amplio, hay varios principios básicos que aparecen repentinamente como temas y que unifican el campo. Por ejemplo, multiplexación, control de flujo y control de errores. El libro destaca estos principios y contrasta su aplicación en áreas específicas de la tecnología.
- **Enfoques de diseño:** el libro examina distintos enfoques alternativos para satisfacer especificaciones concretas de comunicaciones.
- **Normalizaciones:** las normalizaciones han llegado a asumir un papel en el campo importante y creciente, e incluso dominante. Para entender el estado actual de la tecnología, y su futura dirección, se requiere una discusión amplia de las normalizaciones relacionadas con el campo.

ESTRUCTURA DEL LIBRO

El libro está estructurado en cinco partes:

I. **Introducción:** incluye una introducción al abanico de los distintos temas abordados en el libro. Además, esta parte incluye una discusión sobre protocolos OSI y el conjunto de protocolos TCP/IP.

II. **Comunicaciones de datos:** esta parte se refiere principalmente al intercambio de datos entre dos dispositivos directamente conectados. Dentro de esta situación restrictiva, se examinan los aspectos clave de la transmisión, interfaces, control de enlace y multiplexación.

III. **Redes de área amplia:** esta parte examina los mecanismos internos y la tecnología que se han desarrollado para admitir voz, datos y comunicaciones multimedia en redes que cubren grandes distancias. Se examinan las tecnologías tradicionales de conmutación de paquetes y conmutación de circuitos, así como la más reciente de ATM. Un capítulo independiente se dedica a los temas de control de congestión.

IV. **Redes de área local:** esta parte explora las tecnologías y arquitecturas que se han desarrollado para interconexión de redes en distancias más cortas. Se analizan los medios de transmisión, las topologías y protocolos de control de acceso al medio, que son los ingredientes clave del diseño LAN, y se estudian sistemas específicos LAN normalizados.

V. **Protocolos de red:** esta parte explora tanto los principios arquitectónicos como los mecanismos requeridos para el intercambio de datos entre computadores, estaciones de trabajo, servidores y otros sistemas de procesamiento de datos. Gran parte del material de esta sección se refiere al conjunto de protocolos TCP/IP.

Además el libro incluye un extenso glosario, una lista de los acrónimos más frecuentemente usados, y una bibliografía. Cada capítulo incluye problemas y sugerencias de lecturas complementarias.

El libro va dirigido a una audiencia tanto académica como profesional. Para los profesionales interesados en este campo, el libro sirve como obra de referencia básica y es adecuado para auto-estudio. Como libro de texto, puede usarse para un curso de uno o dos semestres. Abarca el material descrito en el curso de «Redes de Comunicaciones entre Computadores» del «Computing Curricula 1991» definido conjuntamente por la ACM y la IEEE. Los capítulos y partes del libro son suficientemente modulares para proporcionar gran flexibilidad en la estructuración de cursos. A continuación se dan algunas sugerencias para diseñar un curso:

- **Fundamentos de comunicaciones de datos:** parte I (introducción) y II (comunicación de datos), y capítulos 9 al 11 (conmutación de circuitos, conmutación de paquetes, y ATM).
- **Redes de comunicaciones:** si el estudiante tiene conocimientos básicos de comunicación de datos, este curso podría abarcar: Parte I (introducción), Parte III (WAN), y Parte IV (LAN).
- **Redes de computadores:** si el estudiante dispone de conocimientos básicos de comunicaciones de datos, entonces este curso podría incluir: Parte I (introducción), Capítulos 6 y 7 (interfases de comunicaciones de datos y control de enlace de datos), y la Parte V (protocolos).

Además es posible un curso más profundo, abarcando la totalidad del libro salvo ciertos capítulos que no son esenciales en una primera lectura. Los capítulos que podrían ser esenciales son: Capítulo 3 (transmisión de datos) y Capítulo 4 (medios de transmisión), caso de que el alumno tenga un conocimiento básico previo de estos temas; Capítulo 8 (multiplexación); Capítulo 9 (conmutación de circuitos); Capítulo 12 (control de congestión); Capítulo 16 (interconexión de redes); y Capítulo 18 (seguridad en redes).

SERVICIOS INTERNET PARA PROFESORES Y ESTUDIANTES

Hay un sitio Web para este libro que proporciona ayuda para estudiantes y profesores. El sitio incluye enlaces a otros lugares relevantes, transparencias con las figuras del libro, e información para suscribirse a una lista de correo internet sobre información de este libro. La dirección Web de la página es: http://www.williamstallings.com/DCC6e.html; para más detalles ver la sección «Página Web para comunicaciones y redes de computadores» que precede a este Prólogo. También se ha configurado una lista de distribución internet para que los profesores que usen este libro puedan intercambiar información sugerencias y preguntas entre ellos y con el autor. Tan pronto como se encuentren errores tipográficos o de otro tipo se incluirá una fe de erratas del libro en http://www.williamstallings.com.

PROYECTOS PARA LA ENSEÑANZA DE COMUNICACIONES Y REDES DE COMPUTADORES

Para muchos profesores, un componente importante de un curso de comunicaciones y redes de computadores es un proyecto o conjuntos de proyectos con los que el estudiante vaya adquiriendo experiencia práctica para reforzar los conceptos del texto. Este libro proporciona un grado incomparable de apoyo ya que incluye una sección de proyectos en el curso. El manual del profesor no sólo incluye una guía de cómo asignar y estructurar los proyectos, sino también un conjunto de proyectos propuestos que abarcan un amplio rango de la materia de este texto, entre los que se encuentran proyectos de investigación, proyectos de simulación, proyectos de modelado analítico y asignación de informes de recopilación bibliográfica. Para más detalles puede verse el Apéndice C.

NOVEDADES EN LA SEXTA EDICIÓN

La sexta edición ve la luz del día casi 15 años después de la publicación de la primera edición. Han sucedido numerosas cosas durante estos años. Además, el ritmo de los cambios, si cabe, se está incrementando. En esta nueva edición he tratado de captar estas innovaciones manteniendo a la vez una visión amplia y comprensible del campo completo. Para realizar este proceso de revisión, la quinta edición fue ampliamente revisada por diversos profesores que imparten esta materia. El resultado es que en muchos lugares la narrativa ha sido clarificada y ajustada, y las ilustraciones han sido mejoradas. También se han añadido diversos problemas probados en la realidad.

Además de estas mejoras que perfeccionan la pedagogía y el uso cómodo del libro, se han introducido otros cambios relevantes a lo largo del mismo. Se han revisado todos los capítulos, se han incluido otros nuevos, y se ha mejorado la organización global del libro. Los cambios más notables son los siguientes:

- **xDSL:** el término xDSL hace referencia a una familia de tecnologías de línea de abonados digitales que proporciona alta velocidad de acceso a ISDN y a otras redes de área amplia a través de cables de par trenzado entre la red y los abonados domésticos o empresariales. El libro da una visión global de xDSL haciendo énfasis en la tecnología Línea de Abonado Digital Asimétrica (ADSL).
- **Ethernet Gigabit:** la discusión sobre Ethernet de 100 Mbps ha sido actualizada, habiéndose añadido una introducción a Ethernet Gigabit.
- **Servicio de velocidad de transmisión disponible (ABR, Available Bit Rate) y mecanismos asociados:** ABR es una incorporación reciente a la ofertas de redes ATM. Proporciona un soporte mejorado para el tráfico de datos basado en IP.
- **Control de congestión:** en esta edición se incluye un capítulo dedicado específicamente a este tópico. Esta presentación unificada clarifica los conceptos involucrados. El capítulo incluye un análisis ampliado de las técnicas ATM para gestión de tráfico y control de congestión.
- **Multidestino IP:** se dedica una nueva sección a este tópico.
- **Servicios Integrados y Diferenciados. RSVP:** desde la publicación de la quinta edición ha habido mejoras sustanciales en Internet con objeto de admitir una gran variedad de tráfico multimedia y sensible al tiempo. Un nuevo capítulo abarca el estudio de servicios integrados, servicios diferenciados, y otras cuestiones relacionadas a la calidad del servicio (QoS, Quality of Service), y el importante protocolo de reserva RSVP (Reservation Protocol).
- **Control de Congestión TCP:** este tema continúa siendo un área activa de investigación. El libro incluye una nueva sección examinando este tópico.

Además, a través del libro, la mayoría de los tópicos ha sido actualizado para reflejar los desarrollos en normalizaciones y tecnología que han tenido lugar desde la publicación de la quinta edición.

CONTROL DE CALIDAD

Se ha realizado un gran esfuerzo para asegurar un alto nivel de calidad en la producción del libro. Se han dedicado más tiempo y más recursos de los habituales en las revisiones del manuscrito original y de las pruebas de imprenta, tanto por el autor como por el editor. Además se han reclutado diversos voluntarios de la comunidad profesional, cada uno de los cuales se ha responsabilizado de la lectura cuidadosa de un capítulo con objeto de corregir los posibles errores técnicos y tipográficos. Cada capítulo ha sido mejorado con dos de estas revisiones. Muchas gracias a Mel Adams, Navin Kumar Agarwal, Ferdinand N. Ahlberg, David Airlie, Tom Allebrandi, Maurice Baker, Rob Blais, Art Boughan, Frank Byrum, George Cherian, Christian Cseh, Dr. Mickael Fontaine, Charles Freund, Bob Furtaw, Andrew Gallo, Gary Gapinski, Sundar Kessler, Steven Kilby, John Kristoff, David Lucantoni, Kenneth Ma, Eddie Maendel, Richard Masoner, Mark McCutcheon, John McHarry, Mittal Monanim, Dr. John Naylon, Robert Olsson, Mike Patterson, Mahbubur Rashid, Jeffrey Rhodes, Monika Riffle, Peter Russell, Ahmet Sekercioglu, Rayaz Siddiqu, Dick Smith, Dave Stern, Omeh Tickoo, Scott Valcourt, Dominick Vanacore, Eko Wibowo, Craig Wiesner y Jeffrey Wright.

Finalmente, Arthur Werbner revisó y verificó todos los problemas planteados y sus soluciones.

AGRADECIMIENTOS

Esta nueva edición se ha beneficiado de la revisión de una serie de personas que han aportado generosamente su tiempo y conocimientos. Robert H.Greenfield (Villanova University) cumplió sobradamente su cometido suministrando numerosos y detallados comentarios sobre cuestiones técnicas y pedagógicas. Otros comentarios muy útiles han procedido de Thomas Milham (Devry Institute of Technology), Gregory B. Brewster (DePaul University), Marc Delvaux (GlobeSpan Semiconductors), Robert E. Morris (Devry Institute of Technology) y Matt Mutka (Michigan State University).

Prólogo a la edición en español

El estudio de la estructura y arquitectura de computadores se incluye en diversos currícula de ingeniería y ciencias. No abundan los buenos textos, como el presente, que cubran los programas correspondientes de forma amplia y rigurosa.

La elaboración de un texto de las características indicadas (al igual que sucede con otros libros de ingeniería) es de gran complejidad dado que el autor debe realizar un laborioso trabajo de generalización de las diversas técnicas utilizadas en computadores concretos, y no sólo debe limitarse a recopilar información detallada sobre ellas. El texto debe presentar al lector abstracciones de equipos reales, de forma que le capaciten no sólo a entender los computadores actuales sino también los futuros, cuando éstos vean la luz. Este concepto es especialmente relevante en un área tan cambiante y en explosión como es la de los computadores. Considero que ésta es una de las principales cualidades del libro de Stallings, donde se da mayor relevancia a los conceptos que a la información (siempre en evolución). En casi todos los capítulos el autor utiliza este enfoque: primero presenta los conceptos clave, y luego los aplica a procesadores concretos. En la presente edición utiliza fundamentalmente las familias de procesadores Pentium y PowerPC, que prácticamente cubren la mayor parte de las tendencias de diseño de los computadores actuales (CISC y RISC, respectivamente), sin que por ello olvide describir ideas relevantes introducidas o usadas en otros procesadores (UltrSparc II, MIPS R10000, IA64, etc.).

También es destacable, como corresponde a un buen libro de ingeniería, la búsqueda que en todo momento hace el autor del análisis de prestaciones, y la presentación (dentro de este contexto) de técnicas específicas (fundamentalmente paralelismo) para equilibrar las prestaciones de los distintos elementos que pueden integrar un computador.

En la presente edición, además de las innovaciones indicadas, se ha efectuado una revisión completa de todo el material del libro, pudiendo destacar la actualización, o nueva introducción, de contenidos tales como memoria óptica, diseño superescalar, repertorio de instrucciones multimedia, ejecución anticipada y carga especulativa, sistemas SMP, clusters, y sistemas NUMA. El libro es complementado con una página Web (http://www.shore.net/~ws/COA5e.html)que contiene abundante ayuda tanto para los lectores como para los profesores de la materia.

Esta edición del libro en español contiene además, como valor añadido, un apéndice (Apéndice C), que no aparece en la versión original en inglés, que trata de completar más aún el texto con procesadores o técnicas de última hora. Este apéndice será actualizado conforme se vayan realizando reimpresiones del presente libro, sin necesidad de esperar a ediciones nuevas.

Deseo destacar el esmerado trabajo de los traductores y la profesionalidad de Andrés Otero, editor de la edición en español.

Alberto Prieto
Coordinador de la traducción
Granada, 1 de mayo de 2000

PARTE I

VISIÓN GENERAL

CUESTIONES DE LA PARTE I

El objetivo de la Parte I del texto es proporcionar los conocimientos básicos, a la vez que especificar el contexto en el que se desarrollará el resto del libro. En este capítulo se presentan un espectro amplio de cuestiones relacionadas con el campo de las redes y la transmisión de datos, así como los conceptos fundamentales relacionados con los protocolos y sus arquitecturas.

ESQUEMA DE LA PARTE I

CAPÍTULO 1. INTRODUCCIÓN

El Capítulo 1 proporciona una visión general del libro, en el que se consideran todos los temas que se estudiarán posteriormente. Esencialmente, en el libro se estudian cuatro aspectos: las comunicaciones de datos a través del enlace de transmisión; las redes de área amplia; las redes de área local; y los protocolos y la arquitectura TCP/IP. El Capítulo 1 es una introducción a todos estos conceptos, y a la vez se proporciona información sobre las organizaciones clave que especifican los estándares.

CAPÍTULO 2. PROTOCOLOS Y ARQUITECTURA

El Capítulo 2 es una extensión de la Sección 1.4, abordando los protocolos y sus arquitecturas. Este capítulo se puede leer inmediatamente tras el Capítulo 1, o bien se puede posponer hasta antes del comienzo de las Partes III, IV o V.

El capítulo trata las características fundamentales de los protocolos. Posteriormente se estudian las dos arquitecturas más importantes: el modelo de interconexión de sistemas abiertos (OSI, Open System Interconnection) y el modelo TCP/IP. Aunque el modelo OSI se utiliza con frecuencia como referente para introducir los conceptos en este campo, la familia de protocolos TCP/IP es con diferencia la base de la mayoría de los productos comerciales, esta es la razón que justifica su consideración en la Parte V del presente texto.

CAPÍTULO 1

Introducción

- El objetivo de este libro es amplio y abarca tres grandes áreas: comunicaciones, redes y protocolos.
- El estudio de las comunicaciones aborda la transmisión de señales de forma tal que sea eficaz y segura. Entre otros aspectos, se estudiarán la transmisión y codificación de señales, los medios de transmisión, las interfaces, el control del enlace de datos y la multiplexación.
- En el estudio de las redes se abordará tanto la tecnología como los aspectos relacionados con las arquitecturas de redes de comunicación utilizadas para la interconexión de dispositivos. Esta materia se divide normalmente en redes de área local (LAN) y redes de área amplia (WAN).
- Respecto a los protocolos de comunicación, se abordan tanto las arquitecturas como un análisis individualizado de los mismos para cada una de las capas de la arquitectura.

En torno a los años 70 y 80 se produjo una sinergia entre los campos de los computadores y las comunicaciones que ha desencadenado un cambio drástico en las tecnologías, productos y en las propias empresas que desde entonces, se dedican simultáneamente a los sectores de los computadores y de las comunicaciones. Aunque las consecuencias de esta combinación revolucionaria están todavía por determinar, no es arriesgado decir que la revolución ha ocurrido y que ninguna investigación dentro del campo de la transmisión de la información debería realizarse sin esta perspectiva.

La revolución antes mencionada ha producido los siguientes hechos significativos:

- No hay grandes diferencias entre el procesamiento de datos (los computadores) y las comunicaciones de datos (la transmisión y los sistemas de conmutación).
- No hay diferencias fundamentales entre la transmisión de datos, de voz o de vídeo.
- Las fronteras entre computadores monoprocesador o multiprocesador; así como entre redes de área local, metropolitanas y de área amplia son cada vez más difusas.

Un efecto de esta tendencia ha sido el solapamiento creciente que se puede observar entre las industrias de las comunicaciones y de los computadores, desde la fabricación de componentes hasta la integración de sistemas. Otro resultado es el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos e información. Las organizaciones de normalización, tanto técnicas como tecnológicas, tienden hacia un sistema único y público que integre todas las comunicaciones y haga que virtualmente todos los datos y fuentes de información sean fácil y uniformemente accesibles a escala mundial.

El objetivo fundamental de este libro es proporcionar una visión unificada del vasto campo de las comunicaciones de datos y los computadores. La organización del libro refleja un intento de dividir esta extensa materia en partes coherentes, proporcionando a la vez, una visión de su estado actual. Este capítulo introductorio comienza presentando un modelo general para las comunicaciones. Posteriormente, se presentan de forma sucinta cada una de las cuatro partes principales de este texto. Termina describiendo el papel decisivo que juegan los estándares.

1.1. UN MODELO PARA LAS COMUNICACIONES

Comenzaremos nuestro estudio considerando el modelo sencillo de sistema de comunicación, mostrado en la Figura 1.1a, en la que se propone un diagrama de bloques.

El objetivo principal de todo sistema de comunicaciones es intercambiar información entre dos entidades. La Figura 1.1b muestra un ejemplo particular de comunicación entre una estación de trabajo y un servidor a través de una red telefónica pública. Otro posible ejemplo consiste en el intercambio de seña-

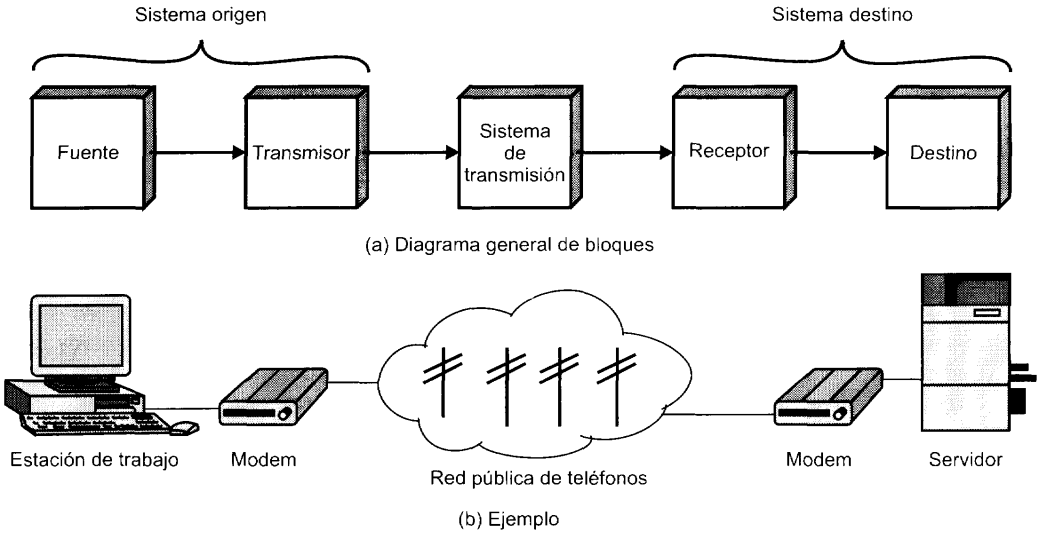


Figura 1.1. Modelo simplificado para las comunicaciones.

les de voz entre dos teléfonos a través de la misma red anterior. Los elementos clave en este modelo son los siguientes:

- **La fuente**. Este dispositivo genera los datos a transmitir: por ejemplo teléfonos o computadores personales.
- **El transmisor**. Normalmente los datos generados por la fuente no se transmiten directamente tal y como son generados. Al contrario, el transmisor transforma y codifica la información, generando señales electromagnéticas susceptibles de ser transmitidas a través de algún sistema de transmisión. Por ejemplo, un modem convierte las cadenas de bits generadas por un computador personal y las transforma en señales analógicas que pueden ser transmitidas a través de la red telefónica.
- **El sistema de transmisión**, que puede ser desde una sencilla línea de transmisión hasta una compleja red que conecte a la fuente con el destino.
- **El receptor**, que acepta la señal proveniente del sistema de transmisión y la transforma de tal manera que pueda ser manejada por el dispositivo destino. Por ejemplo, un modem captará la señal analógica de la red o línea de transmisión y la convertirá en una cadena de bits.
- **El destino**, que toma los datos del receptor.

Aunque el modelo presentado pueda parecer aparentemente sencillo, en realidad implica una gran complejidad. Para hacerse una idea de la magnitud de ella, la Tabla 1.1 lista algunas de las tareas claves que se deben realizar en un sistema de comunicaciones. Esta relación es en un sentido un tanto arbitraria

Tabla 1.1. Tareas en los sistemas de comunicación.

Utilización del sistema de transmisión	Direccionamiento
Implementación de la interfaz	Encaminamiento
Generación de la señal	Recuperación
Sincronización	Formato de mensajes
Gestión del intercambio	Seguridad
Detección y corrección de errores	Gestión de red
Control de flujo	

ya que se podría añadir elementos, mezclar ítems, etc.; es más, algunos elementos representan tareas que se realizan en diferentes «niveles» del sistema.

El primer ítem **«utilización del sistema de transmisión»** se refiere a la necesidad de hacer un uso eficaz de los recursos utilizados en la transmisión, los cuales típicamente se suelen compartir entre una serie de dispositivos de comunicación. La capacidad total del medio de transmisión se reparte entre los distintos usuarios haciendo uso de técnicas denominadas de multiplexación. Además puede que se necesiten técnicas de control de congestión para garantizar que el sistema no se sature por una demanda excesiva de servicios de transmisión.

Para que un dispositivo pueda transmitir información tendrá que hacerlo a través de la **interfaz** con el medio de transmisión. Todas las técnicas de transmisión presentadas en este libro dependen en última instancia de la utilización de señales electromagnéticas que se transmitirán a través del medio. De tal manera que, una vez que la interfaz está establecida, se necesitará la **generación de la señal**. Las características de la señal, tales como, la forma y la intensidad, deben ser tales que permitan: 1) ser propagada a través del medio de transmisión y 2) ser interpretada en el receptor como datos.

Las señales se deben generar no sólo considerando que deben cumplir los requisitos del sistema de transmisión y del receptor, sino que deben permitir alguna forma de **sincronizar** el receptor y el emisor. El receptor debe ser capaz de determinar cuándo comienza y cuándo acaba la señal recibida. Igualmente, deberá conocer la duración de cada elemento de señal.

Además de las cuestiones básicas referentes a la naturaleza y temporización de las señales, se necesitará verificar un conjunto de requisitos que se pueden englobar bajo el término **gestión del intercambio**. Si se necesita intercambiar datos durante un período de tiempo, las dos partes deben cooperar. Por ejemplo, para los dos elementos que intervienen en una conversación telefónica (emisor y receptor), uno de ellos deberá marcar el número del otro, dando lugar a una serie de señales que harán que el otro teléfono suene. En este ejemplo el receptor establecerá la llamada descolgando el auricular. En los dispositivos para el procesamiento de datos, se necesitarán ciertas convenciones además del simple hecho de establecer la conexión. Por ejemplo se deberá establecer si ambos dispositivos pueden transmitir simultáneamente o deben hacerlo por turnos, se deberá decidir la cantidad y el formato de los datos que se transmiten cada vez, y se debe especificar qué hacer en caso de que se den ciertas contingencias, como por ejemplo la detección de un error.

Los dos ítems siguientes (Tabla 1.1) deberían considerarse dentro de la gestión del intercambio, pero debido a su importancia, se consideran por separado. En todos los sistemas de comunicación es posible que aparezcan errores; es decir, la señal transmitida se distorsiona de alguna manera antes de alcanzar su destino. Por tanto, en circunstancias donde no se puedan tolerar errores, se necesitarán procedimientos para la **detección y corrección de errores**. Así por ejemplo, en sistemas para el procesamiento de datos, si se transfiere un fichero desde un computador a otro, no sería aceptable que el contenido del fichero se modificara accidentalmente. Para evitar que la fuente no sature al destino transmitiendo datos más rápidamente de lo que el receptor pueda procesar y absorber, se necesitan una serie de procedimientos denominados **control de flujo**.

Conceptos relacionados pero distintos a los anteriores son el **direccionamiento** y el **encaminamiento**. Cuando cierto recurso se comparte por más de dos dispositivos, el sistema fuente deberá de alguna manera indicar a dicho recurso compartido la identidad del destino. El sistema de transmisión deberá garantizar que ese destino, y sólo ése, reciba los datos. Es más, el sistema de transmisión puede ser una red en la que exista la posibilidad de más de un camino para alcanzar al destino; en este caso se necesitará, por tanto, la elección de una de entre las posibles rutas.

La **recuperación** es un concepto distinto a la corrección de errores. En ciertas situaciones en las que el intercambio de información, por ejemplo una transacción de una base de datos o la transferencia de un fichero, se vea interrumpida por algún fallo, se necesitará un mecanismo de **recuperación**. El objetivo será pues, o bien ser capaz de continuar transmitiendo desde donde se produjo la interrupción, o al menos recuperar el estado donde se encontraban los sistemas involucrados antes de comenzar el intercambio.

El **formato de mensajes** está relacionado con el acuerdo que debe existir entre las dos partes respecto al formato de los datos intercambiados, como por ejemplo el código binario usado para representar los caracteres.

Además, frecuentemente es necesario dotar al sistema de algunas medidas de **seguridad**. El emisor debe asegurarse de que sólo el destino deseado reciba los datos. Igualmente, el receptor querrá estar seguro de que los datos recibidos no se han alterado en la transmisión y que dichos datos realmente provienen del supuesto emisor.

Por último, todo el sistema de comunicación es lo suficientemente complejo como para ser diseñado y utilizado sin más, es decir, se necesita la habilidad de un gestor de red que configure el sistema, monitorice su estado, reaccione ante fallos y sobrecargas, y planifique con acierto los crecimientos futuros.

Como se ha visto, de la aproximación simplista de partida hemos formulado una lista más extensa y elaborada de tareas involucradas en todo el proceso de la comunicación. A lo largo de este libro esta lista se estudiará en profundidad, describiendo todo el conjunto de tareas y actividades que pueden englobarse genéricamente bajo los términos comunicación de datos y redes de computadores.

1.2. COMUNICACIONES DE DATOS

Además de los dos primeros capítulos considerados en la primera parte, el libro se ha estructurado en cuatro partes adicionales. La segunda parte aborda fundamentalmente los temas relacionados con las funciones de comunicación, centrándose en la transmisión de señales de una forma segura y eficiente. Intencionadamente dicha segunda parte se ha titulado «Comunicaciones de Datos», aunque con ese término se alude a algunos, o incluso a todos, los tópicos de las restantes partes (de la III a la V).

Para explicar todos los conceptos abordados en la segunda parte, la Figura 1.2 muestra una perspectiva novedosa del modelo tradicional para las comunicaciones de la Figura 1.1a. Dicha figura se explica a continuación, paso a paso, con la ayuda de un ejemplo: la aplicación de correo electrónico.

Suponiendo que tanto el dispositivo de entrada como el transmisor están en un computador personal. Y que por ejemplo, el usuario de dicho PC desea enviar el mensaje m a otro. El usuario activa la aplicación de correo en el PC y compone el mensaje con el teclado (dispositivo de entrada). La cadena de caracteres se almacenará temporalmente en la memoria principal como una secuencia de bits (g). El computador se conecta a algún medio de transmisión, por ejemplo una red local o una línea telefónica, a través de un dispositivo de E/S (transmisor), como por ejemplo el «transceiver» a una red local o modem. Los datos de entrada se transfieren al transmisor como una secuencia de niveles de tensión [$g(t)$] que representan los bits en algún tipo de bus de comunicaciones o cable. El transmisor se conecta direc-

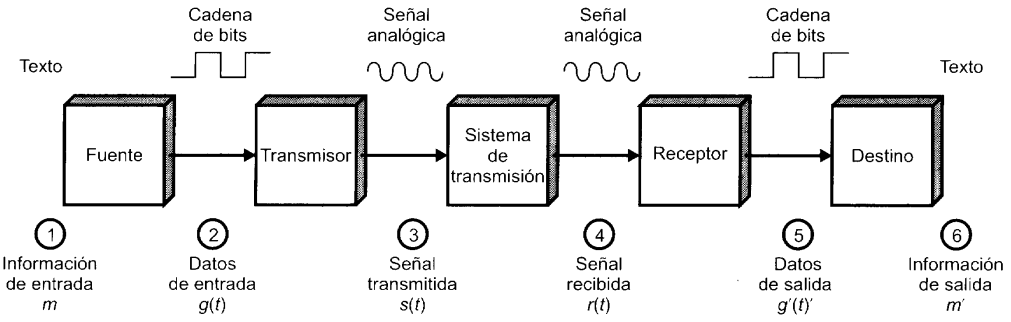


Figura 1.2. Modelo simplificado para las comunicaciones de datos.

tamente al medio y convierte la cadena [$g(t)$] en la señal a transmitir [$s(t)$]; posteriormente en el Capítulo 5 se describirán las distintas alternativas para esta conversión.

Al transmitir $s(t)$ a través del medio, antes de llegar al receptor, aparecerán una serie de dificultades que se estudiarán en el Capítulo 3. Por lo tanto, la señal recibida $r(t)$ puede diferir de alguna manera de la transmitida $s(t)$. El receptor intentará estimar la señal original $s(t)$, a partir de la señal $r(t)$ y de su conocimiento acerca del medio, obteniendo una secuencia de bits $g'(t)$. Estos bits se envían al computador de salida, donde se almacenan temporalmente en memoria como un bloque de bits (g'). En muchos casos, el destino intentará determinar si ha ocurrido un error, y en su caso, cooperar con el origen para eventualmente conseguir el bloque de datos completo y sin errores. Los datos, finalmente se presentan al usuario a través del dispositivo de salida, que por ejemplo puede ser la impresora o la pantalla de su terminal. El mensaje recibido por el usuario (m') será normalmente una copia exacta del mensaje original (m).

Consideremos ahora una conversación telefónica. En este caso, la entrada al teléfono es un mensaje (m) consistente en unas ondas sonoras. Dichas ondas se convierten en el teléfono en señales eléctricas de la misma frecuencia. Estas señales se transmiten sin modificación a través de la línea telefónica. Por tanto, la señal de entrada $g(t)$ y la señal transmitida $s(t)$ son idénticas. La señal $s(t)$ sufrirá algún tipo de distorsión a través del medio, de tal manera que $r(t)$ no será idéntica a $s(t)$.

No obstante, la señal $r(t)$ se convierte recuperando una onda sonora, sin aplicar ningún tipo de corrección o mejora de la calidad. Por lo tanto, m' no es una réplica exacta de m. Sin embargo, el mensaje sonoro recibido es normalmente comprensible por el receptor.

En la discusión aquí realizada, no se han considerado otros aspectos fundamentales en las comunicaciones de datos, como lo son las técnicas de control del enlace, necesarias para regular el flujo de información, o como la detección y corrección de errores; tampoco se han considerado las técnicas de multiplexación, necesarias para conseguir una utilización eficaz del medio de transmisión. Todos estos aspectos se estudian en la Parte II.

1.3. COMUNICACIÓN DE DATOS A TRAVÉS DE REDES

A veces no es práctico que dos dispositivos de comunicaciones se conecten directamente mediante un enlace punto a punto. Esto es debido a alguna (o a las dos) de las siguientes circunstancias:

- Los dispositivos están muy alejados. En este caso no estaría justificado, por ejemplo, utilizar un enlace dedicado entre cada dos dispositivos, que puedan estar separados por miles de kilómetros.
- Hay un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes. Un ejemplo de esta necesidad es la red telefónica mundial, o el conjunto de computadores pertenecientes a una compañía. Salvo el caso de que el número de dispositivos sea pequeño, no es práctico utilizar un enlace entre cada dos.

La solución a este problema es conectar cada dispositivo a una red de comunicación. La Figura 1.3 relaciona este concepto dentro del modelo de comunicaciones de la Figura 1.1a y a la vez sugiere dos grandes categorías en las que se clasifican tradicionalmente las redes: redes de área amplia (WAN, Wide Area Networks) y redes de área local (LAN, Local Area Networks). Recientemente, las diferencias entre estas dos categorías son cada vez más difusas, tanto en términos tecnológicos como de posibles aplicaciones; no obstante, es una forma natural y didáctica de organizar su estudio, por lo que aquí se adoptará dicha clasificación.

REDES DE ÁREA AMPLIA

Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una

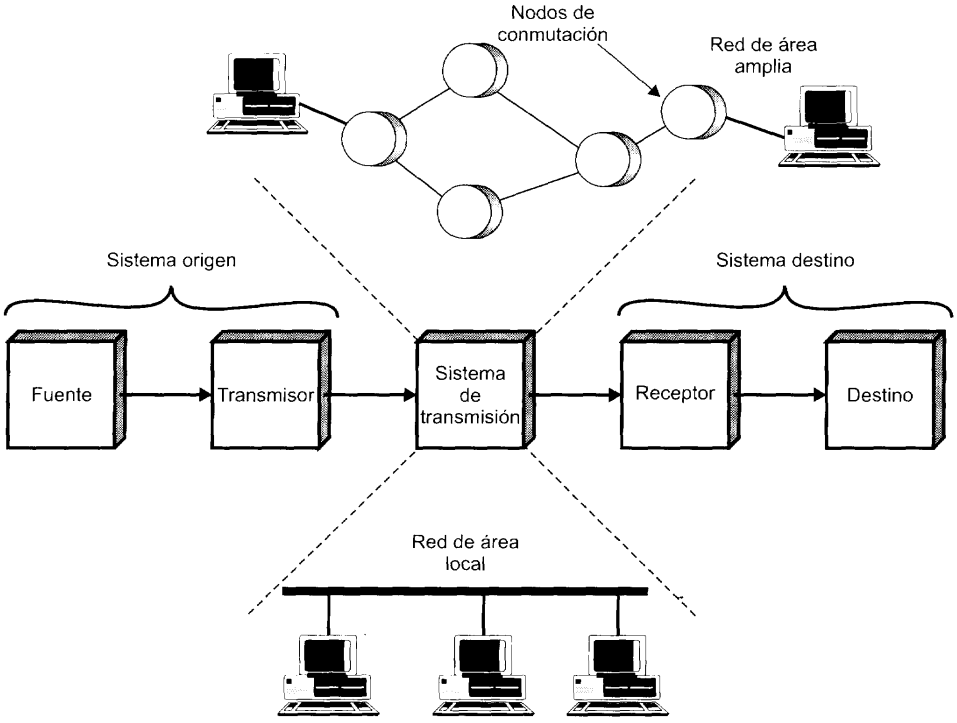


Figura 1.3. Modelos simplificados de redes.

serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo a los situados en los contornos) no les concierne el contenido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Tradicionalmente, las WAN se han implementando usando una de las dos tecnologías siguientes: conmutación de circuitos y conmutación de paquetes. Aunque últimamente, se está empleando como solución la técnica de retransmisión de tramas («frame relay»), así como las redes ATM.

Conmutación de circuitos

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red telefónica.

Conmutación de paquetes

Un enfoque diferente al anterior es el adoptado en redes de conmutación de paquetes. En este caso, no es necesario hacer una reserva a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y la

destino. En cada nodo, el paquete se recibe completamente, se almacena durante un intervalo breve y posteriormente se transmite al siguiente nodo. Las redes de conmutación de paquetes se usan fundamentalmente para comunicaciones terminal-computador y computador-computador.

Retransmisión de tramas (Frame Relay)

La conmutación de paquetes se desarrolló en la época en la que los servicios de transmisión a larga distancia sufrían una tasa de error relativamente elevada, comparada con los servicios de los que se dispone actualmente. Por tanto, para compensar esos errores relativamente frecuentes, en los esquemas de conmutación de paquetes se realiza un esfuerzo considerable, que se traduce en añadir información redundante en cada paquete, así como la realización de un procesamiento extra, tanto en el destino final como en los nodos intermedios de conmutación, necesario para detectar los errores y en su caso, corregirlos.

Ahora bien, con los modernos sistemas de comunicaciones de alta velocidad, este esfuerzo adicional es innecesario y contraproducente. Es innecesario ya que la tasa de errores se ha reducido drásticamente y los escasos errores que aparecen se pueden tratar en el sistema final mediante dispositivos que operan por encima del nivel de la lógica dedicada a la conmutación de paquetes. A su vez es contraproducente ya que los bits redundantes significan un desperdicio de parte de la capacidad proporcionada por la red.

La retransmisión de tramas («frame relay») se ha desarrollado teniendo presente las mayores velocidades de transmisión que actualmente se disponen, así como de las bajas tasas de error. Mientras que las redes originales de conmutación de paquetes se diseñaron para ofrecer una velocidad de transmisión al usuario final de 64 kbps, las redes «frame relay» están diseñadas para operar eficazmente a velocidades de transmisión de usuario de 2 Mbps. La clave para conseguir estas velocidades reside en eliminar la mayor parte de la información redundante y el procesamiento asociado para el control de errores.

ATM

El Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode), a veces denominado como modo de retransmisión de celdas («cell relay»), es la culminación de todos los desarrollos en conmutación de circuitos y conmutación de paquetes realizados durante los últimos 25 años.

ATM se puede interpretar como una evolución de la retransmisión de tramas («frame relay»). La diferencia más obvia entre «frame relay» y ATM es que «frame relay» usa paquetes de longitud variable, llamados «tramas», y ATM usa paquetes de longitud fija denominadas «celdas». Al igual que en «frame relay», ATM introduce poca información adicional para el control de errores, confiando en la inherente robustez del medio de transmisión así como en la lógica adicional localizada en el sistema destino para detectar y corregir errores. Al utilizar paquetes de longitud fija, el esfuerzo adicional de procesamiento se reduce incluso todavía más aquí que en «frame relay». El resultado es que ATM se ha diseñado para trabajar a velocidades de transmisión del orden de 10 a 100 Mbps, e incluso del orden de Gbps.

ATM se puede considerar a su vez como una evolución de la conmutación de circuitos. En la conmutación de circuitos, se dispone solamente de circuitos a velocidad fija de transmisión entre los sistemas finales. ATM permite la definición de múltiples canales virtuales con velocidades de transmisión que se definen dinámicamente en el instante en que el canal virtual se crea. Mediante la utilización de celdas de tamaño fijo, ATM es tan eficaz que puede ofrecer un canal a velocidad de transmisión constante aunque esté usando una técnica de conmutación de paquetes. Por lo tanto, ATM es una ampliación de la conmutación de circuitos en la que se ofrecen varios canales, en los que la velocidad de transmisión para cada canal se fija dinámicamente según las necesidades.

RDSI y RDSI de banda ancha

La sinergia y evolución entre las comunicaciones y las tecnologías de la computación, junto con la creciente demanda de servicios eficaces de captación, procesamiento y diseminación de la información,

está desembocando en el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos. Una consecuencia significativa de esta tendencia ha sido el desarrollo de la Red Digital de Servicios Integrados (RDSI).

La RDSI se ha diseñado para sustituir a las redes públicas de telecomunicaciones existentes, proporcionando una gran variedad de servicios. La RDSI se define mediante la estandarización de las interfaces de usuario, y se ha implementado como un conjunto de conmutadores digitales y enlaces que proporcionan una gran variedad de tipos de tráfico, a la vez que servicios de valor añadido. En la práctica, se trata de múltiples redes, implementadas dentro de los límites nacionales, pero desde el punto de vista del usuario se considera como una única red mundial, uniformemente accesible.

A pesar de que la RDSI tiene todavía que conseguir la cobertura mundial para la que fue diseñada, está ya en su segunda generación. La primera generación, a veces denominada como **RDSI de banda estrecha**, se basa en el uso de canales de 64 kbps como unidad básica de conmutación, presentando una clara orientación hacia la conmutación de circuitos. Técnicamente hablando, la principal contribución de la RDSI de banda estrecha ha sido el «frame relay». La segunda generación, denominada **RDSI de banda ancha**, proporciona velocidades de transmisión muy elevadas (cientos de Mbps) y tiene una clara orientación hacia la conmutación de paquetes. La contribución técnica principal de la RDSI de banda ancha ha sido el modo de transferencia asíncrono (ATM), también denominado retransmisión de celdas «cell relay».

REDES DE ÁREA LOCAL

Al igual que las redes de área amplia, una red de área local es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos. No obstante, hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

1. La cobertura de una LAN es pequeña, típicamente un edificio o como mucho un conjunto de edificios próximos. Como se verá más adelante, esta diferencia en cuanto a la cobertura geográfica, condicionará la solución técnica finalmente adoptada.
2. Es común que la LAN sea propiedad de la misma entidad que es propietaria de los dispositivos conectados a la red. En WAN, esto no es tan corriente, o al menos una fracción significativa de recursos de la red son ajenos. Esto tiene dos implicaciones. La primera es que se debe cuidar mucho la elección de la LAN, ya que evidentemente, lleva acarreado una inversión substancial de capital (comparado con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto en la adquisición como en el mantenimiento. Segunda, la responsabilidad de la gestión de la red local recae solamente en el usuario.
3. Las velocidades de transmisión internas en una LAN son mucho mayores.

Tradicionalmente, en LAN se utiliza la difusión en lugar de utilizar técnicas de conmutación. En una red de difusión, no hay nodos intermedios. En cada estación hay un transmisor/receptor que se comunica con las otras estaciones a través de un medio compartido. Una transmisión desde cualquier estación se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el medio es compartido, una y sólo una estación en cada instante de tiempo podrá transmitir el paquete.

Más recientemente, la conmutación también se está utilizando en LAN, fundamentalmente en LAN tipo Ethernet. Otros dos ejemplos de especial relevancia son las LAN ATM, en las que se usa una red ATM como una red de área local, así como los Canales de Fibra. Estas LAN se estudiarán, junto con las basadas en difusión, en la Parte IV de este texto.

1.4. PROTOCOLOS Y ARQUITECTURA DE PROTOCOLOS

Cuando se realiza un intercambio de datos entre computadores, terminales y/o otros dispositivos de procesamiento, las cuestiones a estudiar son muchas más que las mencionadas en las Secciones 1.2 y 1.3.

Considérese, por ejemplo, la transferencia de un fichero entre dos computadores. En este caso, debe haber un camino entre los dos computadores, directo o a través de un red de comunicación, pero además, típicamente se requiere la realización de las siguientes tareas adicionales:

1. El sistema fuente de información debe activar el camino directo de datos, o bien debe proporcionar a la red de comunicación la identificación del sistema destino deseado.
2. El sistema fuente debe asegurarse de que el destino está preparado para recibir datos.
3. La aplicación de transferencia de fichero en el origen debe asegurarse de que el programa gestor en el destino está preparado para aceptar y almacenar el fichero para el usuario determinado.
4. Si los formatos de los dos ficheros son incompatibles entre ambos sistemas, uno de los dos deberá realizar una operación de adecuación.

Al intercambio de información entre computadores con el propósito de cooperar se le denomina *comunicación entre computadores*. De igual manera, al conjunto de computadores que se interconectan a través de una red de comunicaciones, se les denomina *red de computadores*. Estos términos se extienden igualmente a cuando alguna de las partes es un terminal, ya que el grado de cooperación en este caso es similar.

En el estudio de las comunicaciones entre computadores y las redes de computadores, son especialmente relevantes los dos conceptos siguientes:

- Los protocolos.
- Las arquitecturas para comunicaciones entre computadores.

Para la comunicación entre dos entidades situadas en sistemas diferentes es necesario la definición y utilización de un protocolo. Nótese que los términos «entidad» y «sistema» se están usando en un sentido muy general. Ejemplos de entidades son: los programas de aplicación de los usuarios, las utilidades para transferencia de ficheros, los sistemas de gestión de bases de datos, así como los gestores de correo electrónico y terminales. Ejemplos de sistemas son: los computadores, los terminales y los sensores remotos. Nótese que en algunos casos la entidad y el sistema en el que se ubica son coincidentes (por ejemplo los terminales). En general, una entidad es cualquier cosa capaz de enviar y recibir información, y un sistema es un objeto físico que contiene a una o más entidades. Para que dos entidades se comuniquen con éxito, se requiere que «hablen el mismo idioma». Qué se comunica, cómo se comunica, y cuándo se comunica debe seguir una serie de convenciones mutuamente aceptadas por las entidades involucradas. Este conjunto de convenios se denominan protocolos, que se pueden definir como el conjunto de reglas que gobiernan el intercambio de datos entre dos entidades. Los puntos clave que definen o caracterizan a un protocolo son:

- **La sintaxis:** incluye aspectos tales como el formato de los datos y los niveles de señal.
- **La semántica:** incluye información de control para la coordinación y el manejo de errores.
- **La temporización:** incluye la sintonización de velocidades y secuenciación.

Tras haber introducido el concepto de protocolo, se está en disposición de definir el concepto de arquitectura para las comunicaciones entre computadores. Es claro que debe haber un grado alto de cooperación entre los computadores. En lugar de implementar toda la lógica para llevar a cabo la comunicación en un único módulo, dicha tarea se divide en subtareas, cada una de las cuales se realiza por separado. A modo de ejemplo, la Figura 1.4 muestra cómo empleando tres módulos, se podría implementar una aplicación de transferencia de fichero. Las tareas 3 y 4 de la lista anterior se podrían realizar por el módulo de transferencia de ficheros. Los dos módulos en ambos sistemas intercambian ficheros y órdenes. Sin embargo, en vez de exigir que el módulo de transferencia se encargue de los detalles con los que se realiza el envío de datos y órdenes, dichos módulos delegan en los módulos de servicio de comunicaciones. Éste se encargará de asegurar que el intercambio de órdenes y datos se realice fiablemente. Entre otras cosas, este módulo realizará la tarea 2. Por lo que a partir de este momento, la naturaleza del intercambio entre los sistemas será independiente de la naturaleza de la red que los interconecta. Por lo

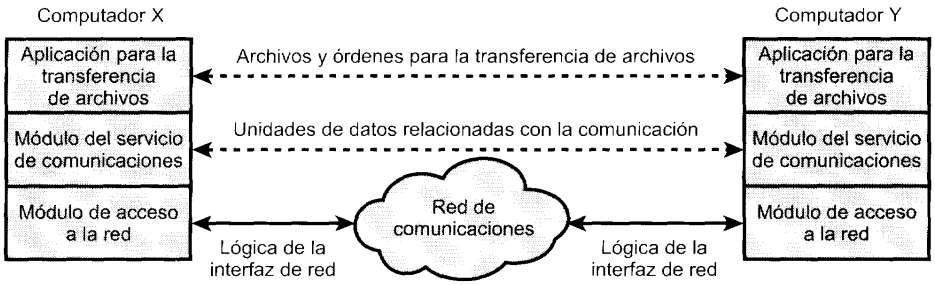


Figura 1.4. Una arquitectura simplificada para la transferencia de archivos.

tanto, en vez de implementar la interfaz de red en el módulo de servicio de comunicaciones, tiene sentido prever un módulo adicional de acceso a la red que lleve a cabo la tarea 1.

Resumiendo, de los tres módulos de la Figura 1.4, el módulo de transferencia de fichero contiene toda la lógica que es exclusiva de la aplicación para la transferencia de ficheros, tal como la transmisión de una palabra clave, órdenes de fichero, y registros del fichero. Se necesita que esta información se transmita de una forma segura. Sin embargo, esta necesidad de seguridad es compartida por otro tipo de aplicaciones (por ejemplo, el correo electrónico y la transferencia de documentos). Por tanto, estos requerimientos se localizan en el módulo separado de servicio de comunicaciones de tal forma que puedan ser utilizados por otras aplicaciones. El módulo de servicio de comunicaciones trata de asegurar que los dos computadores estén activos y preparados para la transferencia de datos, así como de seguir la pista de los datos que se intercambian, garantizando su envío. No obstante, estas tareas son independientes del tipo de red que se esté usando. Por tanto, la lógica encargada de tratar con la red se considera en un módulo separado. De esta forma, si se modifica la red que se esté usando, sólo se verá afectado el módulo de acceso a la red.

Así, en vez de disponer de un solo módulo que realice todas las tareas involucradas en la comunicación, se considera una estructura consistente en un conjunto de módulos que realizarán todas las funciones. Esta estructura se denomina arquitectura de protocolos. A continuación, dentro de esta sección se generalizará el ejemplo precedente para presentar una arquitectura de protocolos sencilla, considerando posteriormente ejemplos más realistas y complejos, como son TCP/IP y OSI.

UN MODELO DE TRES CAPAS

En términos muy generales, se puede afirmar que las comunicaciones involucran a tres agentes: aplicaciones, computadores y redes. Un ejemplo de aplicación es la transferencia de ficheros. Este tipo de aplicaciones se ejecutan frecuentemente en computadores que procesan múltiples aplicaciones simultáneamente. Los computadores se conectan a redes, y los datos a intercambiar se transfieren por la red de un computador a otro. Por tanto, la transferencia de datos desde una aplicación a otra implica en primer lugar la obtención de los mismos y posteriormente hacerlos llegar a la aplicación correspondiente en el computador remoto.

Por todo lo dicho, parece natural organizar la tarea en tres capas independientes:

- Capa de acceso a la red.
- Capa de transporte.
- Capa de aplicación.

La **capa de acceso a la red** está relacionada con el intercambio de datos entre el computador y la red a la que está conectado. El computador emisor debe proporcionar a la red la dirección del destino, de tal forma que la red pueda encaminar los datos al destino apropiado. El computador emisor necesitará hacer uso de algunos de los servicios proporcionados por la red, como, por ejemplo, la gestión de

prioridades. Las características del software de esta capa dependerán del tipo de red que se use. Así, se han desarrollado diferentes estándares para conmutación de circuitos, conmutación de paquetes, redes de área local y otros. De esta manera, se pretende separar las funciones que tienen que ver con el acceso a la red en una capa independiente. Haciendo esto, el resto del software de comunicaciones que esté por encima de la capa de acceso a la red no tendrá que ocuparse de las características específicas de la red que se use. El mismo software de las capas superiores funcionará adecuado e independientemente del tipo de red particular a la que el computador esté conectado.

Independientemente de la naturaleza de las aplicaciones que estén intercambiando datos, es un requisito habitual que los datos se intercambien de una manera segura. Esto es, sería deseable estar seguros de que todos los datos llegan a la aplicación destino y además llegan en el mismo orden en que fueron enviados. Como se verá, los mecanismos que proporcionan dicha seguridad son independientes de la naturaleza de las aplicaciones. Por tanto, tiene sentido concentrar todos estos procedimientos en una capa común que se comparta por todas las aplicaciones, denominada **capa de transporte**.

Finalmente, la **capa de aplicación** contiene la lógica necesaria para admitir varias aplicaciones de usuario. Para cada tipo distinto de aplicación, como por ejemplo la transferencia de ficheros, se necesita un módulo independiente y con características bien diferenciadas.

Las Figuras 1.5 y 1.6 ilustran esta arquitectura sencilla. En la Figura 1.5 se muestran tres computadores conectados a una red. Cada computador contiene software en las capas de acceso a la red, de transporte y de aplicación para una o más aplicaciones. Para una comunicación con éxito, cada entidad deberá tener una dirección única. En realidad se necesitan dos niveles de direccionamiento. Cada computador en la red debe tener una dirección de red; esto permite a la red proporcionar los datos al computador apropiado. A su vez, cada aplicación en el computador debe tener una dirección que sea única dentro del propio computador, esto permitirá a la capa de transporte proporcionar los datos a la aplicación apropiada. Las anteriores direcciones son denominadas puntos de acceso al servicio (SAP, Service Access Point), nótese que cada aplicación accede individualmente a los servicios proporcionados por la capa de transporte.

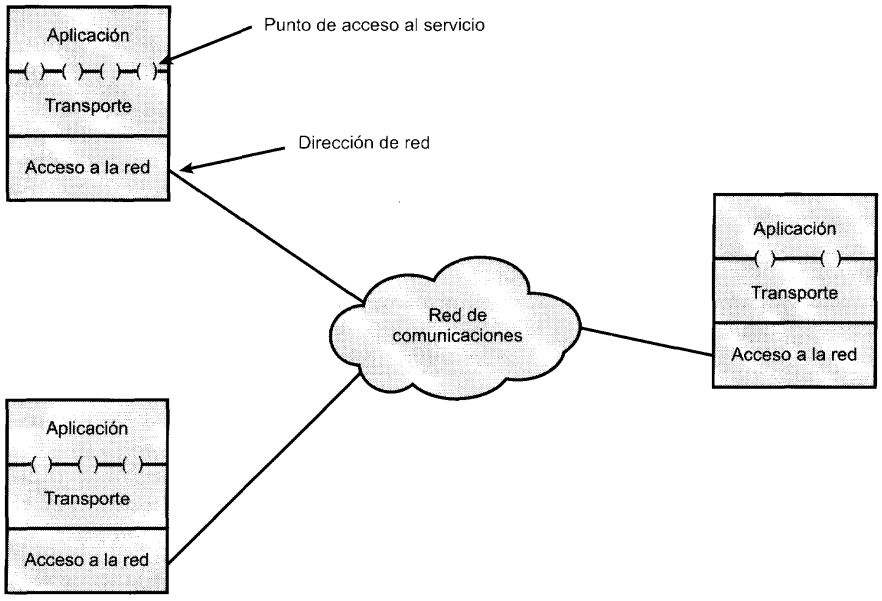


Figura 1.5. Redes y arquitecturas de protocolos.

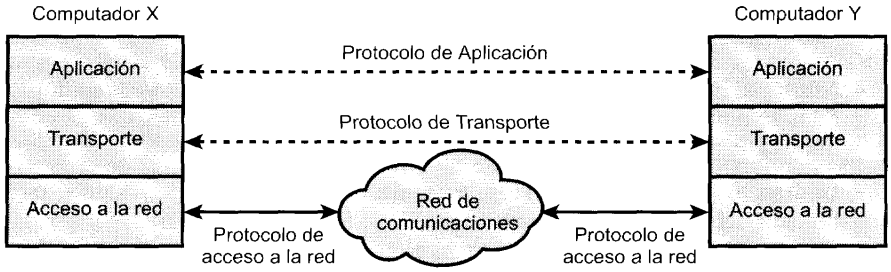


Figura 1.6. Protocolos en una arquitectura simplificada.

La Figura 1.6 muestra cómo se comunican, mediante un protocolo, los módulos en el mismo nivel de computadores diferentes. Veamos su funcionamiento. Supóngase que una aplicación, asociada al SAP 1 en el computador X, quiere transmitir un mensaje a otra aplicación, asociada al SAP 2 del computador Y. La aplicación en X pasa el mensaje a la capa de transporte con la instrucción de que lo envíe al SAP 2 de Y. La capa de transporte pasa el mensaje a la capa de acceso a la red, la cual proporciona las instrucciones necesarias a la red para que envíe el mensaje a Y. Debe observarse que la red no necesita conocer la dirección del punto de acceso al servicio en el destino. Todo lo que necesita conocer es que los datos estén dirigidos al computador Y.

Para controlar esta operación, se debe transmitir información de control junto a los datos del usuario, como así se muestra en la Figura 1.7. Supongamos que la aplicación emisora genera un bloque de datos y se lo pasa a la capa de transporte. Esta última puede fraccionar el bloque en unidades más pequeñas para hacerlas más manejables. A cada una de estas pequeñas unidades la capa de transporte añadirá una cabecera, que contendrá información de control según el protocolo. La unión de los datos generados por la capa superior junto con la información de control de la capa actual se denomina unidad de datos del protocolo (PDU, Protocol Data Unit); en este caso, se denominará como PDU de transporte. La cabecera en cada PDU de transporte contiene información de control que se usará por el mismo protocolo de transporte en el computador Y. La información que se debe almacenar en la cabecera es por ejemplo:

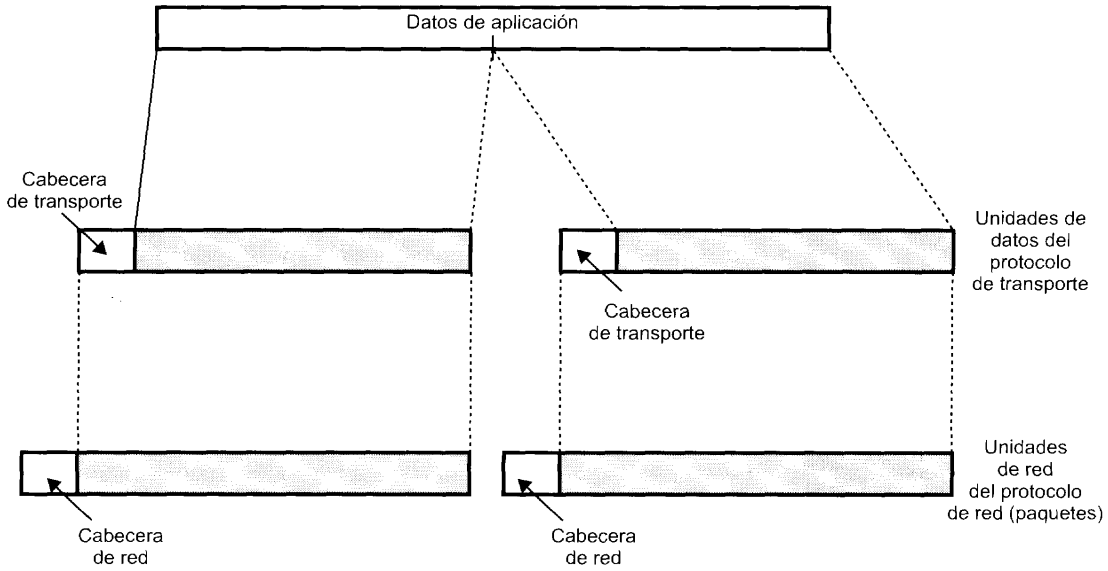


Figura 1.7. Unidades de datos de los protocolos.

- **SAP destino:** cuando la capa de transporte destino reciba la PDU de transporte, deberá saber para quién van destinados los datos.
- **Número de secuencia:** ya que el protocolo de transporte está enviando una secuencia de PDU, éstas se numerarán secuencialmente para que si llegan desordenadas, la entidad de transporte destino sea capaz de ordenarlas.
- **Código de detección de error:** la entidad de transporte emisora debe incluir un código que es función del contenido del resto de la PDU. El protocolo de transporte receptor realiza el mismo cálculo y compara los resultados con el código recibido. Si hay discrepancia se concluirá que ha habido un error en la transmisión, y en ese caso el receptor, podrá descartar la PDU y adoptar las acciones oportunas para su corrección.

El siguiente paso en la capa de transporte es pasar cada una de las PDU a la capa de red, con la instrucción de que sea transmitida al computador destino. Para satisfacer este requerimiento, el protocolo de acceso a la red debe pasar los datos a la red con una solicitud de transmisión. Como anteriormente, esta operación requiere el uso de información de control. En este caso, el protocolo de acceso a la red añade la cabecera de acceso a la red a los datos provenientes de la capa de transporte, creando así la PDU de acceso a la red. A modo de ejemplo, la cabecera debe contener la siguiente información:

- **La dirección del computador destino:** la red debe conocer a quién (qué computador de la red) debe entregar los datos.
- **Solicitud de recursos:** el protocolo de acceso a la red puede pedir a la red que realice algunas funciones, como por ejemplo gestionar prioridades.

En la Figura 1.8 se conjugan todos estos conceptos, mostrando la interacción entre los módulos para transferir un bloque de datos. Supongamos que el módulo de transferencia de ficheros en el computador X está transfiriendo registro a registro al computador Y. Cada registro se pasa al módulo de la capa de transporte. Se puede describir esta acción como si se tratase de una orden o una llamada a un procedimiento. Posibles argumentos de este procedimiento serán la dirección del destino, el SAP destino y el registro del fichero. La capa de transporte añade el punto de acceso al servicio e información de control adicional, que se agregará al registro para formar la PDU de transporte. Ésta se pasa a la capa inferior de acceso a la red mediante la llamada a otro procedimiento. En este caso, los argumentos para esta llamada serán la dirección del computador destino y la unidad de datos del protocolo de transporte. La

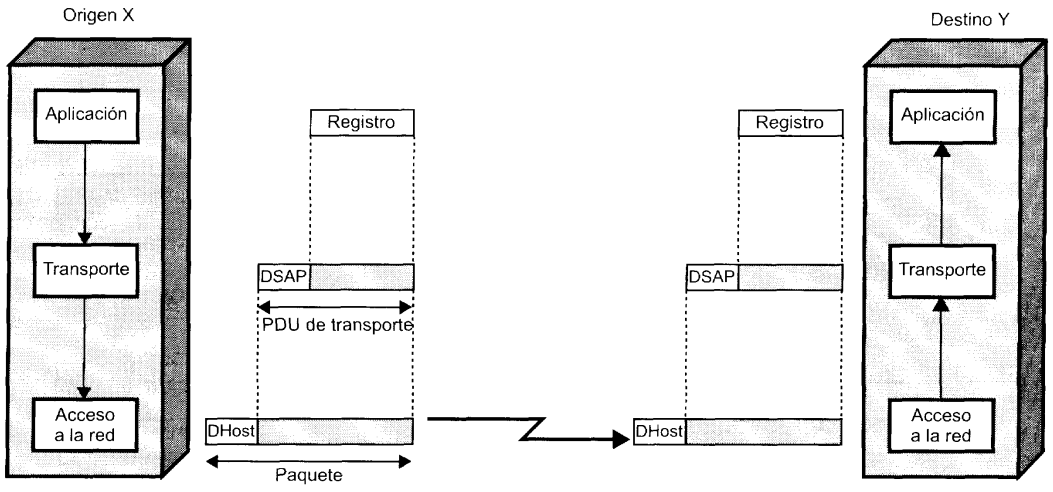


Figura 1.8. Funcionamiento de una arquitectura de protocolos.

capa de acceso a la red usará esta información para construir la PDU de red. La PDU de transporte es el campo de datos de la PDU de red, y su cabecera contendrá información relativa a las direcciones origen y destino. Nótese que la cabecera de transporte no es «visible» al nivel de acceso a la red; en otras palabras, a dicho nivel no le concierne el contenido concreto de la PDU de transporte.

La red acepta la PDU de transporte de X y la transmite a Y. El módulo de acceso a la red en Y recibe la PDU, elimina la cabecera y pasa la PDU de transporte adjunta al módulo de la capa de transporte de Y. La capa de transporte examina la cabecera de la unidad de datos del protocolo de transporte y en función del campo en la cabecera que contenga el SAP, entregará el registro correspondiente a la aplicación pertinente, en este caso al módulo de transferencia de ficheros de Y.

LA ARQUITECTURA DE PROTOCOLOS TCP/IP

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo de referencia de OSI. TCP/IP es la arquitectura más adoptada para la interconexión de sistemas, mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación. En esta sección, se incluye un breve resumen de las dos arquitecturas, aunque posteriormente se desarrollarán con más detalle en el Capítulo 2.

TCP/IP es resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes ARPANET, financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, Defense Advanced Research Projects Agency), y se denomina globalmente como la familia de protocolos TCP/IP. Esta familia consiste en un extensa colección de protocolos que se han erigido como estándares de Internet.

Al contrario que en OSI, no hay un modelo oficial de referencia TCP/IP. No obstante, basándose en los protocolos estándar que se han desarrollado, todas las tareas involucradas en la comunicación se puede organizar en cinco capas relativamente independientes:

- Capa de aplicación.
- Capa origen-destino o de transporte.
- Capa internet.
- Capa de acceso a la red.
- Capa física.

La **capa física** define la interfaz física entre el dispositivo de transmisión de datos (por ejemplo, la estación de trabajo o el computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos, y cuestiones afines.

La **capa de acceso a la red** es responsable del intercambio de datos entre el sistema final y la red a la cual se está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que la red pueda encaminar los datos hasta el destino apropiado. El emisor puede requerir ciertos servicios, como por ejemplo solicitar una determinada prioridad, que pueden ser proporcionados por el nivel de red. El software en particular que se use en esta capa dependerá del tipo de red que se disponga; se han desarrollado diversos estándares para conmutación de circuitos, conmutación de paquetes (por ejemplo, X.25), redes de área local (por ejemplo, Ethernet), entre otros.

La capa de acceso a la red está relacionada con el acceso y encaminamiento de los datos a través de la red. En situaciones en las que los dos dispositivos estén conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. Ésta es la función de la **capa Internet**. El protocolo internet (IP, Internet Protocol) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los «routers» intermedios. Un «router» es un dispositivo con capacidad

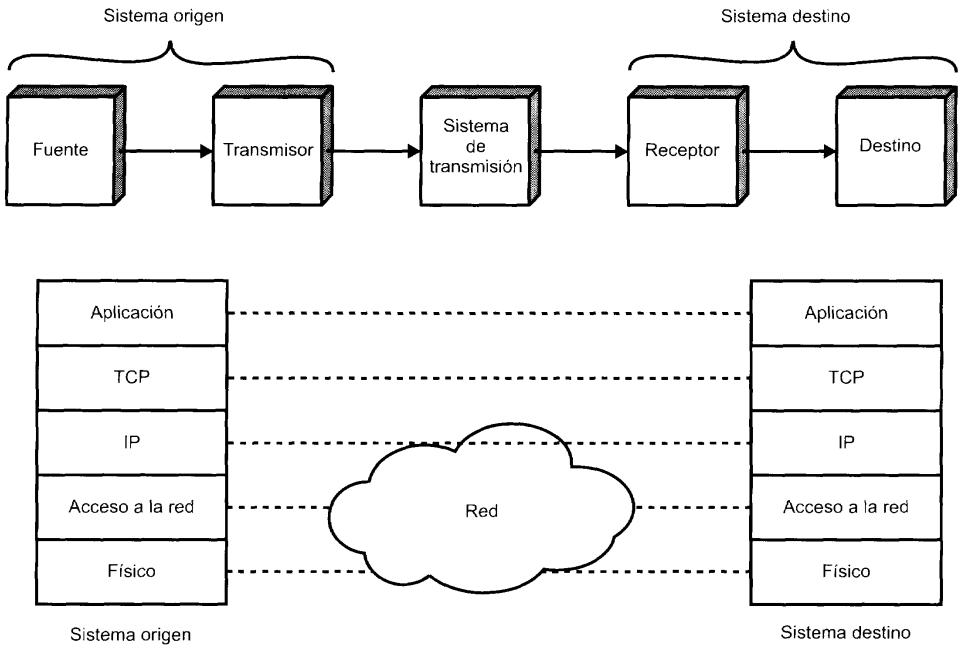


Figura 1.9. Modelo de arquitectura de protocolo.

de procesamiento que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la ruta adecuada para alcanzar al destino.

Independientemente de la naturaleza de las aplicaciones que están intercambiando datos, es usual requerir que los datos se intercambien de forma segura. Esto es, sería deseable asegurar que todos los datos llegan a la aplicación destino y en el mismo orden en el que fueron enviados. Los procedimientos que garantizan una transmisión segura están localizados en la **capa origen-destino**, o **capa de transporte**. El protocolo TCP (Transmission Control Protocol) es el más utilizado para proporcionar esta funcionalidad.

Finalmente, la **capa de aplicación** contiene la lógica necesaria para posibilitar las distintas aplicaciones de usuario. Para cada tipo particular de aplicación, como por ejemplo la transferencia de ficheros, se necesitará un módulo bien diferenciado.

La Figura 1.9 muestra como se implementan los protocolos TCP/IP en los sistemas finales, a la vez que relaciona la arquitectura con el modelo para las comunicaciones de la Figura 1.1a. Nótese que las capas física y de acceso a la red proporcionan la interacción entre el sistema final y la red, mientras que las capas de aplicación y transporte albergan los protocolos denominados «extremo a extremo», ya que facilitan la interacción entre los dos sistemas finales. La capa internet tiene algo de las dos aproximaciones anteriores. En esta capa, los sistemas origen y destino proporcionan a la red la información necesaria para realizar el encaminamiento, pero a la vez, deben proporcionar algunas funciones adicionales de intercambio entre los dos sistemas finales; estos aspectos se desarrollarán posteriormente en los Capítulos 15 y 16.

EL MODELO OSI

El modelo de OSI (Open Systems Interconection) se desarrolló por la Organización Internacional de Estandarización ISO (International Organization for Standarization) como una arquitectura para comuni-

caciones entre computadores, con el objetivo de ser el marco de referencia en el desarrollo de protocolos estándares. OSI considera siete capas:

- Aplicación.
- Presentación.
- Sesión.
- Transporte.
- Red.
- Enlace de datos.
- Física.

En la Figura 1.10 se muestra el modelo OSI y se definen brevemente las funciones que se realizan en cada capa. La intención del modelo OSI es que los protocolos se desarrollen de forma tal que realicen las funciones de cada una de las capas.

Figura 1.10. Las capas de OSI.

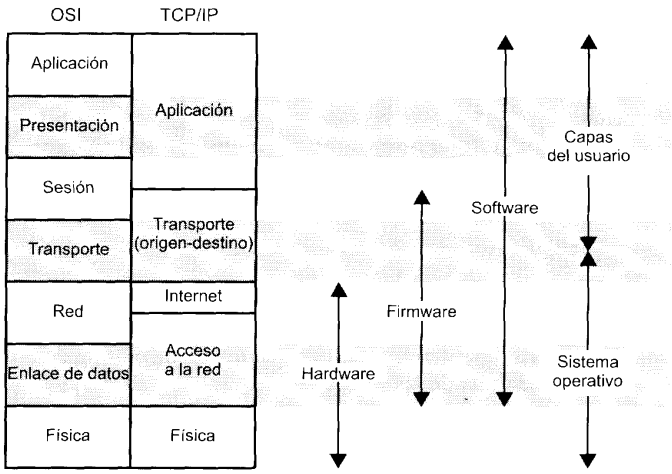


Figura 1.11. Una comparación entre las arquitecturas de protocolo TCP/IP y OSI.

Los diseñadores de OSI consideraron que este modelo y los protocolos asociados llegarían a dominar las comunicaciones entre computadores, reemplazando eventualmente las implementaciones particulares de protocolos, así como a modelos rivales tales como TCP/IP. Sin embargo, esto no ha sido así. Aunque se han desarrollado muchos protocolos de utilidad dentro del contexto de OSI, el modelo de las siete capas en su conjunto no ha prosperado. Por el contrario, la arquitectura TCP/IP se ha erigido como dominante. Por tanto, en este libro se pondrá mayor énfasis en TCP/IP.

La Figura 1.11 muestra las capas de las arquitecturas OSI y TCP/IP, indicando la posible correspondencia en términos de funcionalidad entre ambas. La misma figura sugiere a su vez formas de implementar las diferentes capas.

1.5. NORMALIZACIONES

En la industria de las comunicaciones desde hace tiempo se ha aceptado que los estándares son necesarios para definir las características físicas, mecánicas y de procedimiento de los equipos de comunicación. En el pasado, este punto de vista no ha sido compartido por la industria de los computadores. Mientras que los productores de equipos de comunicación reconocían que sus equipos deberían en general interconectarse y comunicarse con equipos desarrollados por terceros, los fabricantes de computadores han tratado de monopolizar a sus clientes. La proliferación de diferentes computadores y la generalización del procesamiento distribuido ha desencadenado una situación insostenible. Computadores de diferentes fabricantes deben comunicarse con otros, y dada la evolución actual en la normalización de protocolos, los clientes no admitirán la necesidad de software para la conversión de protocolos de uso específico. Como consecuencia, los estándares en la actualidad están imponiéndose en todas las áreas tecnológicas consideradas en este libro.

A lo largo del texto se describirán los estándares más importantes que están en uso o en desarrollo para los diversos aspectos involucrados en las comunicación entre computadores. En el apéndice de este capítulo se mencionan las organizaciones más significativas implicadas en el desarrollo de los estándares.

Hay una serie de ventajas y desventajas en el proceso de estandarización. A continuación se citan las más relevantes. Las principales ventajas son:

- Un estándar asegura un gran mercado. Esto estimula la producción masiva y, en algunos casos, el uso de integración a gran escala (LSI) o integración a muy gran escala (VLSI), reduciéndose así los costos.
- Un estándar permite que los productos de diferentes fabricantes se comuniquen, dotando al comprador de mayor flexibilidad en la selección y uso de los equipos.

Las principales desventajas son:

- Los estándares tienden a congelar la tecnología. Mientras que un estándar se desarrolla, se revisa y se adopta, se habrán desarrollado otras técnicas más eficaces.
- Hay muchos estándares para la misma función. Este problema en realidad no es atribuible a los estándares en sí, sino a la manera en que se hacen las cosas. Afortunadamente, recientemente las diversas organizaciones para el establecimiento de estándares han comenzado a cooperar más estrechamente. No obstante, todavía hay áreas donde coexisten varios estándares en conflicto.

APÉNDICE 1A. ORGANIZACIONES DE NORMALIZACIÓN

A lo largo de este libro, se describen los estándares más importantes relacionados con las comunicaciones y los computadores. Se consideran tanto aquellos que en la actualidad están en uso, como los que están en fase de desarrollo. Para la promoción o desarrollo de estos estándares han participado decisivamente varias organizaciones. Este apéndice presenta una breve descripción de las organizaciones más importantes de normalización:

- IEFT.
- ISO.
- UIT-T.
- El Forum ATM.

NORMALIZACIONES EN INTERNET Y EL IETF

Muchos de los protocolos que constituyen la serie TCP/IP se han estandarizado o están en fase de estandarización. Mediante acuerdos universales, una organización denominada la Sociedad Internet (Internet Society) es responsable del desarrollo y la publicación de estos estándares. La Sociedad Internet es una organización de profesionales que supervisa a una serie de gabinetes y grupos de trabajo involucrados en el desarrollo y normalización de Internet.

En esta sección se proporciona una breve descripción del procedimiento que siguen los estándares de la familia TCP/IP en su fase de desarrollo.

Las Organizaciones de Internet y la publicación de RFC

La Sociedad Internet es el comité coordinador para el diseño, ingeniería y gestión de Internet. Entre otras cuestiones, se encarga del propio funcionamiento de Internet, así como de la normalización de los protocolos usados por los sistemas finales. Dentro de la Sociedad Internet hay tres organizaciones responsables tanto del desarrollo de los estándares como de su publicación:

- **El comité para la arquitectura en Internet (IAB, Internet Architecure Board):** responsable de definir toda la arquitectura de Internet, proporciona las directrices y las líneas de actuación del IETF.
- **El comité para la ingeniería en Internet (IEFT, Internet Engineering Task Force):** responsable del desarrollo e ingeniería de los protocolos.

- **El comité para la investigación en Internet (IRTF, Internet Research Task Force):** responsable de la gestión de las actividades del IETF, así como del proceso de normalización.

Todo el trabajo necesario para la especificación de las normas y de los protocolos se lleva a cabo mediante grupos de trabajo. La pertenencia a cada uno de los grupos de trabajo es voluntaria, siendo característico el hecho de que cualquier interesado puede participar en los distintos grupos. Durante el desarrollo de una especificación, el grupo de trabajo hará un borrador del documento final denominado Borrador Internet (Internet Draft), el cual se publicará y estará disponible «on-line» en el directorio del IETF. El documento permanecerá como «Internet Draft» como mucho hasta seis meses, durante este periodo todas las partes interesadas podrán revisarlo y comentarlo. A la vez durante ese periodo, el IESG puede aprobar que el borrador se publique como RFC (Request For Comment). Si el borrador no pasa al estado de RFC durante los seis meses mencionados, será eliminado del directorio. El grupo de trabajo puede posteriormente publicar versiones revisadas del borrador.

El IEFT, tras su aprobación por parte del IESG, es el responsable de la publicación de los RFC. Los RFC son las notas de trabajo para la comunidad que desarrolla e investiga en Internet. El contenido de estos documentos puede ser cualquier cosa relacionada con las comunicaciones entre computadores, es decir, desde un informe sobre una reunión hasta la especificación de un estándar.

El proceso de normalización

La decisión definitiva de cuál de los RFC se erige como estándar se toma en el IESG, oídas las recomendaciones del IETF. Para convertirse una especificación en un estándar debe verificar los criterios siguientes:

- Ser estable y bien conocida.
- Ser adecuada técnicamente.
- Haber sido experimentada suficientemente demostrando su interoperatividad entre varias implementaciones independientes.
- Tener una aceptación pública.
- Ser considerada útil por Internet, parcialmente o en su totalidad.

Las diferencia esencial entre estos criterios y los que se utilizan en los estándares internacionales del ISO y la ITU-T reside en el énfasis que aquí se pone en los aspectos relacionados con el funcionamiento real y la experimentación.

En la Figura 1.12 se muestra la sucesión de pasos, denominados *«Standars Track»*, que debe seguir una especificación hasta llegar a ser aceptada como estándar, este proceso se ha definido en el RFC 2026[1]. En todo el proceso, los pasos sucesivos requieren una necesidad creciente de consenso y verificación. En cada paso, el IEFT debe establecer unas recomendaciones o directrices para el desarrollo del protocolo, que deben ser ratificadas por el IESG. El proceso comienza a partir de que el IESG aprueba la publicación del borrador o «Internet Draft» como un RFC en estado de norma o Estándar Propuesto.

Las cajas blancas en el diagrama mencionado representan situaciones temporales, que deberían implicar el mínimo intervalo posible de tiempo. Sin embargo, un determinado documento debe permanecer en el estado de estándar propuesto durante seis meses como mínimo y como borrador estándar durante al menos cuatro, esto es para permitir así un periodo suficiente de revisión y remisión de comentarios. Las cajas de color gris representan situaciones a más largo plazo, que pueden durar varios años.

Para pasar a la situación de borrador, cada especificación debe experimentarse sobre al menos dos realizaciones independientes, comprobándose su interoperatividad.

Tras obtener la suficiente experiencia, la especificación puede ser elevada a la categoría de estándar Internet. Llegados a este punto, se le asigna un número de estándar (STD), así como un número de RFC.

---

[1] Los RFC que se citen a lo largo del libro se listan en el Apéndice B.

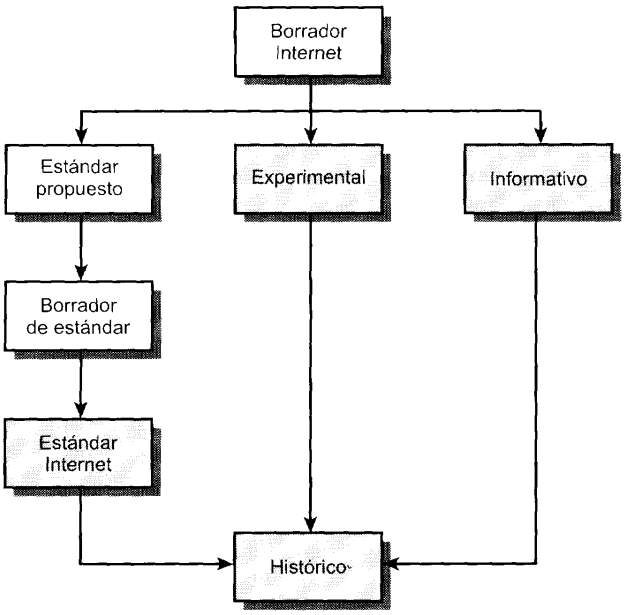


Figura 1.12. Publicación de RFC en Internet.

Por último, cuando un protocolo se vuelve obsoleto, se pasa a la condición de histórico.

El proceso de normalización en documentos no estándar

Cualquier protocolo o especificación que no se considere estar preparada para ser normalizada se puede publicar como un RFC experimental. Tras la realización de trabajos adicionales, la especificación puede ser remitida para su reconsideración. Si la especificación es lo suficientemente estable, ha resuelto problemas planteados en el diseño, se suponga bien comprendida, ha recibido suficientes revisiones y críticas, y parezca que despierta el suficiente interés en la comunidad, entonces el RFC se considerará estar en el estado de Estándar Propuesto.

Por último, para informar a la comunidad de Internet se publica una Especificación Informativa.

LA ORGANIZACIÓN INTERNACIONAL PARA LA NORMALIZACIÓN (ISO)

La ISO[2] (International Organization for Standardization) es una agencia internacional para el desarrollo de normalizaciones que abarcan un amplio abanico de materias. Es una organización sin ánimo de lucro, de voluntariado, cuyos miembros son organismos de estandarización de las naciones participantes además de una serie de organizaciones observadoras sin voto. Aunque ISO no es gubernamental, más del 70 % de los miembros son instituciones gubernamentales. La mayoría de los miembros restantes tienen relaciones muy estrechas con las administraciones públicas de los respectivos países. Por ejemplo, el miembro estadounidense es el organismo denominado «American National Standards Institute» (ANSI).

ISO se fundó en 1946 y desde entonces ha especificado más de 12.000 normalizaciones en una gran cantidad de áreas de diversa índole. Su objetivo es promocionar el desarrollo de normalizaciones y de actividades relacionadas para facilitar el intercambio internacional de bienes y servicios, así como desa-

[2] ISO no es en realidad el acrónimo (en su caso debería ser literalmente IOS), sino una palabra derivada de la griega *isos*, que significa igual.

rrollar la cooperación en la esfera intelectual, científica, tecnológica y económica. ISO ha definido estándares para todo, desde el paso de los tornillos hasta cuestiones de energía solar. Un área importante dentro del campo de las normalizaciones se encarga de la arquitectura de comunicaciones para la interconexión de sistemas abiertos (OSI, Open Systems Interconnection), así como de la definición de estándares para cada una de las capas de la arquitectura OSI.

En lo referente a los temas estudiados en este texto, los estándares OSI se han desarrollado en realidad como un esfuerzo conjunto con otras organizaciones, como es la IEC (International Electrotechnical Commission). La IEC se encarga principalmente de la normalización en ingeniería eléctrica y electrónica. En el área de las tecnologías de la información, ambas organizaciones se solapan, aunque la IEC pone más énfasis en los aspectos hardware, mientras que ISO lo hace en software. En 1987, los dos grupos formaron el JTC (Joint Technical Committee). Este comité ha tenido la responsabilidad del desarrollo de documentos en el área de las tecnologías de la información que han sido adoptados por ISO (y por el IEC).

El desarrollo de un estándar ISO en particular, desde que empieza como una propuesta hasta que se formaliza como un estándar oficial, sigue un proceso que se puede describir en seis pasos o fases. El objetivo es que el resultado final sea aceptado por el mayor número posible de países. A continuación se describen brevemente las fases:

1. **Fase de proposición:** se asigna un tema al comité técnico apropiado, y dentro de ese comité, al grupo de trabajo adecuado.
2. **Fase de preparación:** el grupo de trabajo prepara un borrador de trabajo. Durante esta fase es probable que se consideren sucesivos borradores hasta que el grupo de trabajo esté convencido de que ha desarrollado la mejor solución técnica al problema abordado. En esta fase, el borrado se envía al comité jerárquicamente superior al grupo de trabajo para entrar en la fase de consenso.
3. **Fase en el comité:** tan pronto como el comité apruebe el primer borrador, se registra en la Secretaría Central de la ISO. Se hace circular entre los miembros interesados para su consideración, emisión de comentarios técnicos y su posterior votación. Puede que en esta fase se consideren sucesivos borradores hasta que se alcance el consenso en lo referente al contenido técnico. Cuando hay un acuerdo suficiente, el texto está preparado para ser remitido como documento DIS (Draft International Standard).
4. **Fase de indagación:** la Secretaría Central de la ISO hace circular el DIS entre todos los miembros del ISO para su votación y formulación de comentarios durante un periodo de cinco meses. El documento se aprobará para su consideración como FDIS («Final Draft International Standard») siempre y cuando se consiga una mayoría de las dos terceras partes y no más de un cuarto del número total de votos sean negativos. Si no se consigue la aprobación, el texto se devuelve al grupo de trabajo proponente para su nueva reelaboración, para posteriormente hacerlo circular de nuevo como documento DIS y repetir el proceso.
5. **Fase de aprobación:** el documento FDIS se distribuye entre todos los estamentos del ISO por parte de la Secretaría Central para una votación final (Sí/No) durante un periodo de dos meses. Si se reciben comentarios técnicos durante ese periodo, no serán considerados durante esta fase, pero serán registrados para su posterior consideración en una revisión futura del Estándar Internacional. El texto se aprobará como Estándar Internacional si obtiene una mayoría de las dos terceras partes y no más de un cuarto del número total de votos sean negativos. Si no consigue su aprobación, el estándar es devuelto al grupo de trabajo original para su reconsideración, teniendo en cuenta las razones técnicas argumentadas por parte de los votantes negativos.
6. **Fase de publicación:** una vez que el documento FDIS se haya aprobado, se introducirán sólo cambios mínimos en el texto definitivo. El texto final será remitido a la Secretaría Central de la ISO, la cual publicará el documento en su estado de Estándar Internacional.

El proceso de definición de un estándar ISO puede ser lento. Ciertamente, sería deseable que la definición de estándares fuera tan rápida como los detalles técnicos lo permitieran, pero ISO debe asegurarse de que el estándar recibe una aceptación suficiente.

EL SECTOR DE NORMALIZACIÓN DE LA UIT PARA LAS TELECOMUNICACIONES

El sector de estandarización UIT para las Telecomunicaciones (UIT-T) es un órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que es a su vez una agencia especializada de la Organización de las Naciones Unidas. Por tanto los miembros del UIT-T son gobiernos. La representación de USA reside en el Departamento de Estado. El objeto de la UIT-T es «estudiar y definir recomendaciones de cuestiones técnicas, tecnológicas, de operación y tarificación para así normalizar las telecomunicaciones a escala mundial». Su objetivo central es la estandarización, tanto como sea necesario, de técnicas y de modos de operación en telecomunicaciones para llevar a cabo una compatibilidad extremo a extremo en las conexiones internacionales de telecomunicación, independientemente de los países origen y destino.

La UIT-T fue creada el 1 de marzo de 1993 como consecuencia del proceso de reforma dentro de la UIT. Este organismo sustituye al Comité Consultivo Internacional de Telefonía y Telégrafos (CCITT), que en esencia tenía los mismos estatutos y objetivos que el nuevo UIT-T.

La UIT-T se ha organizado en 14 grupos de estudio que establecen las recomendaciones:

2. Funcionamiento de la red y servicios.

3. Tarificación y cuestiones económicas.

4. Red para la gestión de las telecomunicaciones y mantenimiento de la red.

5. Protección contra interacciones electromagnéticas.

6. Equipamiento externo.

7. Redes de datos y comunicaciones de sistemas abiertos.

8. Características de los sistemas telemáticos.

9. Transmisión de televisión y sonido.

10. Lenguajes y cuestiones generales de software para sistemas de telecomunicación.

11. Requerimientos de señalización y protocolos.

12. Prestaciones de redes y terminales en la transmisión extremo a extremo.

13. Aspectos generales de la red.

15. Redes de transporte, sistemas y equipos.

16. Equipos y sistemas de transmisión.

El trabajo dentro de la UIT-T se organiza en ciclos de cuatro años, coincidiendo con la frecuencia con la que se organiza una conferencia mundial (o reunión plenaria) para la Estandarización de las Telecomunicaciones. El programa de trabajo para los siguientes cuatro años se determina en la asamblea, en forma de cuestiones, planteadas por los distintos grupos de estudio, basándose en los requerimientos de los miembros pertenecientes a los mencionados grupos de estudio. En la conferencia se fijan las cuestiones, se revisan los objetivos de los grupos de estudio, se crean o disuelven los grupos de acuerdo con las necesidades, y se les asignan las cuestiones mencionadas.

En función de las cuestiones asignadas, cada grupo de estudio prepara borradores de las recomendaciones. Un borrador de recomendación puede ser considerado en la siguiente reunión, de periodicidad cuatrianual, para su aprobación. Sin embargo, cada vez más frecuentemente las recomendaciones están siendo aprobadas tan pronto como estén listas, sin necesidad de esperar al final del periodo de cuatro años. Este procedimiento acelerado se está adoptando desde el periodo de estudio que finalizó en 1988.

Por tanto, 1988 fue la última vez en la que se publicaron simultáneamente un gran número de documentos a modo de recomendación.

EL FORUM ATM

La UIT-T es responsable, de entre otras áreas, del desarrollo de estándares para la RDSI de banda ancha (RDSI-B), que está basada en la tecnología ATM. El Forum ATM juega igualmente un papel crucial en el desarrollo de los estándares ATM. En la UIT-T y en los miembros participantes provenientes de los distintos países, el proceso de la elaboración de normas se caracteriza por un mecanismo de consenso, entre gobiernos, usuarios, y representantes del sector industrial. Este proceso puede ser dilatado en el tiempo. Aunque la UIT-T ha extremado sus esfuerzos, los retardos en la elaboración de las normas son particularmente significativos el área de la RDSI-B, en la que la tecnología dominante es el modo de transferencia asíncrono (ATM «Asynchronous transfer mode»), caracterizada por su rápida y cambiante evolución. Debido, pues, al gran interés que ha despertado la tecnología ATM, se creó el Forum ATM con el objetivo de acelerar el procedimiento elaboración de normas para ATM. El Forum ATM es una organización internacional sin ánimo de lucro, constituida por 600 miembros de distintas compañías. Los usuarios finales también tienen su representación en el Forum.

El Forum ATM ha recibido una mayor atención y nivel de vinculación por parte de los fabricantes de computadores que la propia UIT-T. Debido a que el Forum trabaja sobre una política de mayorías en lugar de la estrategia del consenso, ha sido capaz de adaptarse rápidamente para definir algunos de los detalles necesarios para la implementación de ATM. Este esfuerzo, ha redundado en un beneficio para el esfuerzo normalizador de la UIT-T.

APÉNDICE 1B. RECURSOS EN INTERNET

Hay una serie de recursos disponibles en Internet y en la Web para complementar a este texto, que pueden ayudar al lector para estar al día respecto a los desarrollos llevados a cabo en este contexto.

PÁGINAS WEB PARA ESTE LIBRO

Se ha diseñado una página Web especial para complementar a este libro, está disponible en http://www.williamstallings.com. Una descripción detallada de este sitio puede verse en la sección «Páginas Web para este libro» antes del Prefacio.

Tan pronto como se detecten erratas tipográficas así como toda clase de errores, se publicarán en http://www.williamstallings.com. El fichero se actualizará cuando se necesite. Por favor, comuniquen cualquier tipo de error detectado al autor ws@shore.net. En el mismo sitio se pueden encontrar listas de erratas para otros libros del autor, así como información y ofertas para la adquisición de otros libros escritos por el autor.

OTROS SITIOS WEB

Hay una cantidad enorme de sitios Web con información relacionada con los temas tratados en el libro. En los capítulos siguientes, se pueden encontrar referencias de sitios Web específicos, en cada una de las secciones «Lecturas Recomendadas». Debido a la tendencia que tienen las URL de cambiar frecuentemente, no han sido incluidas en este libro. Todos los sitios Web citados a lo largo del libro pueden ser explorados a través de los correspondientes enlaces que se han habilitado en la página Web del libro.

Las siguientes páginas Web son de interés general y están relacionadas con las comunicaciones y redes de computadores:

- **El mundo de las redes:** información y enlaces a recursos sobre comunicaciones de datos y redes.
- **IETF:** mantiene archivos relacionados con Internet y sobre las actividades de la IETF. Incluye una biblioteca de RFC y de borradores indexada por palabras clave, así como otros muchos documentos relacionados con Internet y protocolos asociados.
- **Fabricantes:** enlaces a páginas Web de más de 1.000 fabricantes de hardware y software, así como un directorio telefónico de miles de empresas de computadores y redes.
- **Bibliografías sobre computación:** una colección de cientos de bibliografías con cientos de miles de referencias.
- **La sociedad «IEEE Communications»:** una buena forma de estar informado sobre conferencias publicaciones, etc.
- **Grupo «ACM Special Group on Communications (SIGCOMM)»:** una buena forma de estar informado sobre congresos, publicaciones, etc.
- **Unión Internacional de Telecomunicaciones:** contiene una lista de recomendaciones de la UIT-T, más información para la obtención de documentos de la UIT-T, impresos o en CD-ROM.
- **Organización Internacional para la Estandarización (OSI):** contiene una lista de normas ISO, más información sobre como obtener documentos impresos o en CD-ROM.

GRUPOS DE NOTICIAS USENET

Se ha establecido una serie de grupos de noticias USENET, sobre aspectos relacionados con la comunicación de datos y las redes. Como en casi todos los otros grupos USENET, en estos grupos hay una gran relación ruido-señal, a pesar de esto, periódicamente vale la pena comprobar si algo se ajusta a sus necesidades. He aquí una muestra:

- comp.dcom.lan, comp.dcom.lans.misc: debate sobre LAN en general.
- comp.std.wireless: debate sobre redes inalámbricas, incluyendo, entre otras, redes de área local inalámbricas.
- comp.security.misc: seguridad en computadores y encriptación.
- comp.dcom.cell-relay: sobre ATM y LAN ATM.
- comp.dcom.frame-relay: sobre redes «frame relay».
- comp.dcom.net-management: debate sobre aplicaciones de gestión de red, protocolos y estándares.
- comp.protocolo.tcp-ip: sobre la familia TCP/IP.

CAPÍTULO 2

Protocolos y arquitectura

- Una arquitectura de protocolos es una estructura de capas hardware y software que facilita el intercambio de datos entre sistemas, y proporciona aplicaciones distribuidas como por ejemplo el correo electrónico y la transferencia de ficheros.
- En cada capa de la arquitectura se implementan uno o varios protocolos. Cada protocolo proporciona un conjunto de reglas que regulan el intercambio de datos entre los sistemas.
- Las tareas típicas que realiza un protocolo son entre otras: encapsulamiento, segmentación, ensamblado, control de la conexión, transmisión ordenada, control del flujo, control de errores, direccionamiento y multiplexación.
- La arquitectura que más se usa es la familia de protocolos TCP/IP, en la que se definen las siguientes capas: física, acceso a la red, internet, transporte y aplicación.

El objetivo de este capítulo es servir de visión general y proporcionar los conocimientos básicos para abordar con éxito el resto de capítulos del texto. En este capítulo se muestra cómo los temas considerados de la Parte II a la V se enmarcan dentro de la transmisión de datos y de las redes de computadores. Este capítulo se puede leer aquí, es decir en su lugar natural, o bien al principio de las Partes III, IV o V[1].

El capítulo comienza presentando el concepto de protocolo de comunicación. Se demuestra que los protocolos son fundamentales en todas las comunicaciones de datos. A continuación, para describir e implementar sistemáticamente las comunicaciones, el problema se plantea en términos de capas, las cuales contendrán protocolos. Esta misma aproximación es la que se adoptó en el ya famoso modelo de interconexión de sistemas abiertos (OSI, Open Systems Interconnection).

Aunque el modelo OSI es considerado universalmente como el modelo de referencia hay otro modelo, denominado arquitectura de protocolos TCP/IP que definitivamente ha ganado la batalla comercial. La mayor parte de los protocolos que se describen en la Parte V pertenecen a la familia TCP/IP. A lo largo de este capítulo se presentará un resumen de los más significativos.

2.1. PROTOCOLOS

Comenzaremos nuestro estudio dando una visión general de las características principales de los protocolos. Antes de proseguir, el lector debería repasar los conceptos asociados a los protocolos definidos en el Capítulo 1.

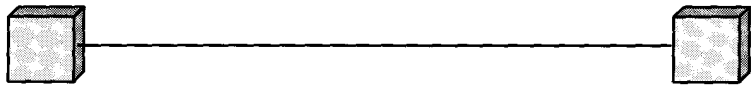
CARACTERÍSTICAS

Los protocolos se caracterizan fundamentalmente por ser:

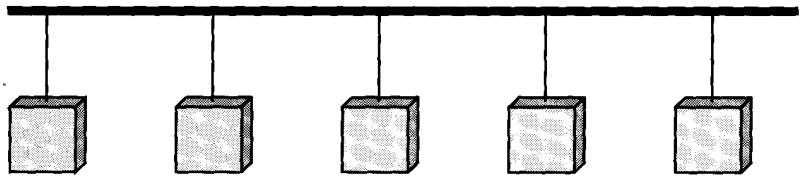
- Directos/indirectos.
- Monolíticos/estructurados.
- Simétricos/asimétricos.
- Estándares/no estándares.

[1] Puede ser útil para el lector hacer una lectura preliminar del mismo y posteriormente reconsiderarlo en profundidad antes del comienzo de la Parte V.

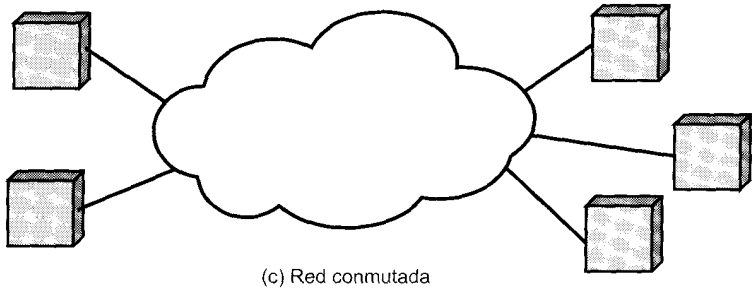
La comunicación entre dos entidades puede ser **directa** o **indirecta**. En este sentido, en la Figura 2.1 se describen algunas situaciones posibles. Si los dos sistemas que se van a comunicar comparten una línea punto a punto, las entidades de estos sistemas se podrán comunicar directamente; es decir, los datos y la información de control pasarán directamente entre las entidades sin la intervención de un agente activo. Esta misma idea es aplicable a configuraciones multipunto, aunque en este caso las entidades deberán solucionar el problema del control del acceso, complicando así el protocolo. Si los sistemas se conectan a través de una red conmutada no se podrá aplicar un protocolo directo. El posible intercambio de datos entre dos entidades dependerá a su vez del buen funcionamiento de otras entidades. Un caso algo más complejo será cuando las dos entidades no compartan la misma red conmutada, aunque eso sí deberán estar conectadas a través de dos o más redes. A un conjunto de este tipo de redes interconectadas se les denomina Internet.



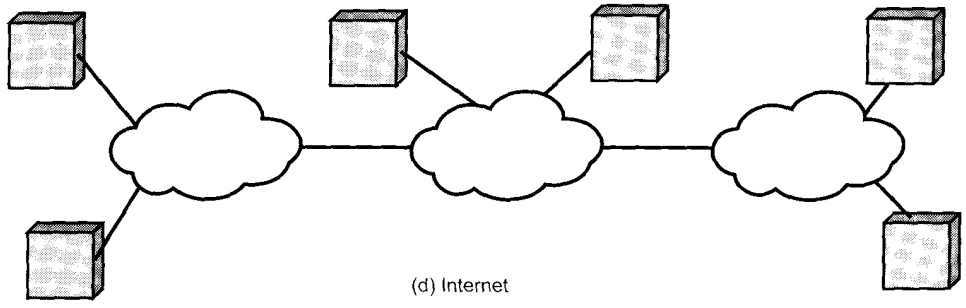
(a) Punto a punto



(b) Red de difusión multipunto



(c) Red conmutada



(d) Internet

Figura 2.1. Tipos de conexión en un sistema de comunicación.

Otra característica de los protocolos es su carácter **monolítico** o **estructurado**. Conforme el lector se vaya adentrando en el libro irá comprendiendo que la tarea de la comunicación entre sistemas remotos es lo suficientemente compleja como para abordarla y concebirla monolíticamente como un todo. Por ejemplo, supóngase una aplicación de correo electrónico ejecutándose en dos computadores conectados mediante un enlace síncrono HDLC. Para ser estrictamente monolítica, la aplicación debería contener toda la lógica del HDLC. Si la conexión se llevara a cabo a través de una red de conmutación de paquetes, en este caso la aplicación necesitaría igualmente incluir la lógica del HDLC (o algún protocolo equivalente) para conectarse a la red. Además del software anterior, la aplicación debería incluir: el software para dividir los mensajes a transmitir en unidades del tamaño de un paquete, el software para solicitar un circuito virtual, etc. La aplicación necesitaría incluir software para la sincronización temporal, es decir, los mensajes se deben enviar sólo en el caso de que el sistema y la entidad destino estén activas y preparadas para recibir. Esta sincronización necesitará de lógica adicional que debe incluirse en la aplicación. Es más, como se irá viendo más adelante, la lista de problemas a resolver es todavía mayor. En la aproximación monolítica, una modificación en cualquiera de los detalles implicaría que toda la aplicación debería modificarse, con el riesgo de introducir errores difíciles de localizar.

Como alternativa se puede optar por una técnica de diseño e implementación estructurada. En lugar de un único protocolo, en este caso habrá un conjunto de protocolos organizados con una estructura por capas o jerárquica. Las funciones básicas se implementarán en las entidades de los niveles inferiores, las cuales proporcionarán servicios a las entidades de los niveles superiores. Por ejemplo, la aplicación de correo electrónico podría utilizar los servicios del módulo (o entidad) HDLC cuando le hiciera falta. Nótese que esto introduce una nueva forma de dependencia: al intercambiar datos las entidades de los niveles superiores dependerán de las entidades de los niveles inferiores.

Cuando se opta por un diseño estructurado, a todo el conjunto de hardware y software que se utiliza para la implementación de las funciones de comunicación se denomina arquitectura. Tras esta sección, el resto del capítulo se dedica a este concepto.

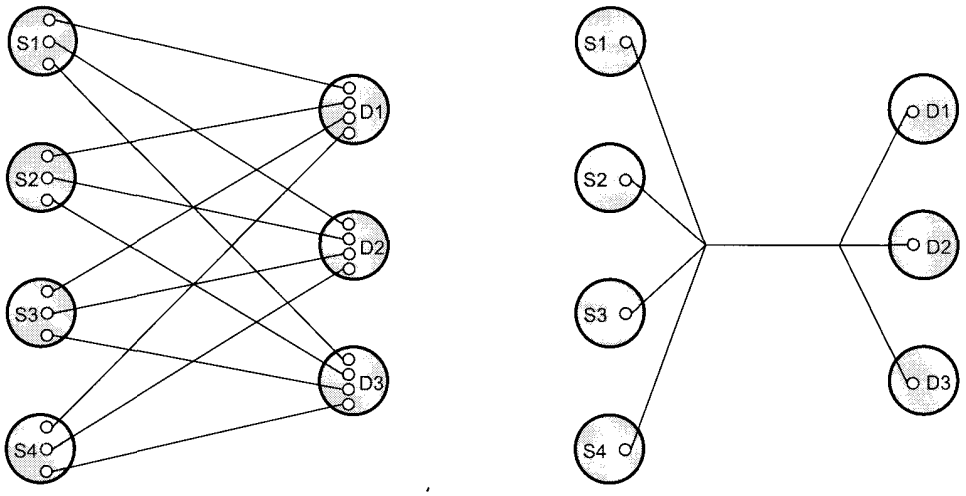
Un protocolo puede ser **simétrico** o **asimétrico**. La mayoría de los protocolos que se van a estudiar serán simétricos. Es decir, involucran a entidades pares. En ciertas situaciones la simetría vendrá impuesta por la naturaleza del intercambio (por ejemplo, un proceso «cliente» y un «servidor»), o por la necesidad expresa de reducir la complejidad de las entidades o de los sistemas. Un ejemplo de esta necesidad puede ser el modo de respuesta normal del HDLC. Normalmente, este modo implica que un computador sondea una serie de terminales. La lógica en el extremo del terminal es muy sencilla.

Por último, un protocolo puede ser **estándar** o **no estándar**. Un protocolo no estándar es aquel que se diseña y se implementa para una comunicación particular, o al menos para un computador con un modelo particular. Supóngase que se comunican K tipos diferentes de fuentes con L tipos de receptores de información, si no hubiera estándares se necesitarían $K \times L$ protocolos diferentes, además de $2 \times K \times L$ implementaciones diferentes (Figura 2.2a). Si todos los sistemas compartieran un protocolo común, se necesitarían tan sólo $K + L$ implementaciones (Figura 2.2b). El uso creciente de sistemas de procesamiento distribuido junto con la tendencia decreciente por parte de los clientes a depender de un único fabricante, han forzado a que los fabricantes implementen protocolos que obedezcan a estándares bien establecidos.

FUNCIONES

Antes de retomar la discusión sobre las arquitecturas de comunicación así como sobre las distintas capas de protocolos, se va a estudiar un conjunto reducido de funciones que constituyen la base de todos los protocolos. No todos los protocolos proporcionan estas funciones, ya que ello implicaría una duplicación innecesaria de las mismas. No obstante, hay algunas funciones que se repiten en algunos protocolos situados en distintos niveles.

El análisis que se va a realizar es necesariamente abstracto, ya que se va a proporcionar una revisión genérica de las características y funciones de los protocolos de comunicación. El concepto de protocolo



(a) Sin estándares: 12 protocolos; 24 implementaciones de protocolos

(b) Con estándares: 1 protocolo; 7 implementaciones

Figura 2.2. Uso de protocolos estandarizados.

es muy importante para la mayoría de las cuestiones que se abordan en este texto, y conforme el lector vaya adentrándose en el mismo, podrá encontrar ejemplos de todas las funciones que a continuación se van a comentar.

Las funciones de un protocolo se pueden agrupar en:

- Encapsulamiento.
- Segmentación y ensamblado.
- Control de la conexión.
- Entrega en orden.
- Control del flujo.
- Control de errores.
- Direccionamiento.
- Multiplexación.
- Servicios de transmisión.

Encapsulamiento

Cada PDU no sólo contiene datos, sino que además debe incluir información de control. De hecho algunas PDU contienen información de control exclusivamente. La información de control se puede clasificar en las siguientes categorías:

- **Dirección:** en la PDU se debe indicar la dirección del emisor y/o del receptor.
- **Código para la detección de errores:** para la detección de errores en la trama se debe incluir alguna secuencia de comprobación.

- **Control del protocolo:** en la PDU se incluye información adicional para llevar a cabo las funciones *del protocolo que se mencionan a continuación.*

Se denomina encapsulamiento al hecho de añadir a los datos información de control. Los datos se aceptan o generan por una entidad, y se encapsulan en la PDU junto con la información de control (véase Figuras 1.7 y 1.8).

Segmentación y ensamblado[2]

El protocolo es el encargado del intercambio de cadenas de datos entre dos entidades. Normalmente, la transferencia se realiza mediante una secuencia de bloques de datos de tamaño limitado. En el nivel de aplicación, la unidad lógica de datos a transmitir se denomina mensaje. Tanto si la entidad de aplicación envía los datos agrupados en mensajes o si se trata si los envía como cadena continua, los protocolos de los niveles inferiores pueden necesitar partir los datos en bloques más pequeños. Este procedimiento se denomina segmentación. Denominaremos unidad de datos del protocolo (PDU, Protocol Data Unit) al bloque de datos a intercambiar entre dos entidades.

Hay una serie de razones, dependientes del contexto, que justifican la segmentación. Entre otras están:

- La red de comunicaciones puede que sólo acepte bloques de datos de un tamaño limitado. Por ejemplo, en una red ATM el tamaño de los bloques está limitado a 53 octetos, por el contrario Ethernet impone un tamaño máximo de 1.526 octetos.
- Los mecanismos para el control de errores pueden ser más eficientes cuanto menor sea el tamaño de la PDU. Al utilizar PDU menores, cuando la PDU tenga errores el número de bits a retransmitir será menor.
- El acceso a las facilidades de transmisión que sean compartidas será más equitativo y los retardos serán igualmente inferiores. Por ejemplo, si no se fijara un tamaño máximo cualquier estación podría monopolizar un medio compartido.
- Un tamaño de PDU menor implica que las entidades receptoras tienen que reservar menores tamaños de memoria temporal.
- A veces, una entidad necesitará que la transferencia de datos se interrumpa con cierta periodicidad para llevar a cabo tareas de comprobación y/o reinicio/recuperación.

Por el contrario, hay una serie de desventajas en la segmentación que justifican utilizar bloques de tamaño lo más grande posible:

- Como se acaba de explicar, cada PDU contiene cierta cantidad de información de control. Por tanto, cuanto menor sea el bloque, mayor será el porcentaje de información suplementaria.
- La llegada de un PDU genera una interrupción que se debe atender. Cuanto menor sean los bloques más interrupciones se generarán.
- EL tiempo necesario para procesar PDU que sean pequeñas, y por tanto más numerosas, será superior.

El diseñador de protocolos, a la hora de determinar el tamaño máximo y mínimo de las PDU deberá tener en cuenta todos los factores citados.

El procedimiento contrario a la segmentación se denomina ensamblado. Los datos segmentados tendrán que ensamblarse recuperando el formato de los mensajes originales para ser entregados a la entidad de aplicación destino. La tarea será más complicada si las PDU se reciben desordenadas.

En la Figura 1.7 se muestra el procedimiento de la segmentación.

---

[2] En la mayoría de protocolos de la familia TCP/IP se usa el término fragmentación en lugar de segmentación, aunque el significado sea el mismo.

Control de la conexión

En una transferencia de datos no orientada a conexión, la entidad emisora transmite los datos al otro extremo de forma tal que cada PDU se tratará independientemente de las PDUs recibidas con anterioridad. Un ejemplo de este tipo de transferencia es la utilización de datagramas, descrita más adelante en el Capítulo 10.

En los casos en que las estaciones prevén un intercambio voluminoso de datos y/o hay ciertos detalles del protocolo que se deben controlar dinámicamente será preferible (o incluso obligatorio) la transferencia orientada a conexión. Una asociación lógica, o conexión, se establece entre dos entidades. En este tipo de transferencia se dan tres fases (Figura 2.3):

- Establecimiento de la conexión.
- Transferencia de datos.
- Cierre de la conexión.

En protocolos que sean más sofisticados se darán, además de las anteriores, fases de interrupción de la conexión y fases de recuperación, siempre que se presenten errores y otros tipos de interrupciones.

Durante la fase de establecimiento de la conexión, las dos entidades acordarán el intercambio de datos. Normalmente, una de las estaciones enviará una solicitud de conexión (usando una transferencia no orientada a conexión) a la otra. Puede que en el proceso esté involucrada una autoridad central. En los protocolos más sencillos, la entidad de recepción aceptará o bien denegará la solicitud recibida, y consecuentemente la conexión se considerará estar establecida o no. En protocolos más complejos, esta fase incluirá una fase adicional en la que se negociarán aspectos relacionados con la sintaxis, semántica y temporización del protocolo. Evidentemente, ambas entidades deberán utilizar el mismo protocolo. No obstante, los protocolos pueden ofrecer una serie de opciones que deben ser pactadas mediante una negociación. Por ejemplo, aunque un protocolo pueda admitir un tamaño de PDU de hasta 8.000 octetos, una estación en particular puede tener limitaciones de PDU de 1.000 octetos.

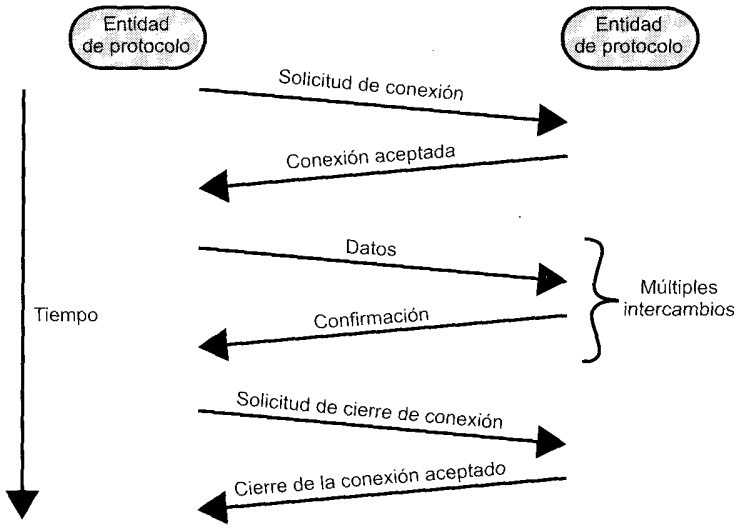


Figura 2.3. Las fases de la transferencia de datos orientada a conexión.

Tras el establecimiento de la conexión, se entra en la fase de transferencia de datos. Durante esta fase se intercambia tanto datos como información de control (por ejemplo, para el control del flujo o

control de errores). La Figura 2.3 muestra una situación en la que los datos se transmiten en un solo sentido, mientras que las confirmaciones se transmiten en el sentido contrario. La situación más típica es, si embargo, aquella en la que datos y confirmaciones se transmiten en ambos sentidos. Finalmente, cualquiera de las dos entidades puede desear terminar la conexión, y así lo hará enviando una solicitud de cierre de la conexión. O bien, alternativamente puede ser que el cierre esté ordenado por una autoridad central.

La característica principal de la transferencia orientada a conexión es que cada extremo numera secuencialmente las PDU que envía al otro extremo. Cada entidad sabe que está involucrada en una conexión lógica, por lo que podrá controlar los números de salida que ella genera así como de los números de entrada, los cuales habrán sido generados en el otro extremo. De hecho, se puede definir la transferencia orientada a conexión como aquella en la que los dos extremos numeran y controlan las PDU tanto de entrada como de salida. La numeración secuencial está relacionada con tres funciones fundamentales: la entrega en orden, el control del flujo y el control de errores.

Entrega en orden

Si dos entidades de comunicación residen en estaciones[3] diferentes conectadas a través de una red, habrá un cierto riesgo de que las PDU lleguen con un orden diferente al de partida, ya que puede que hayan seguido rutas distintas para llegar al destino. En los protocolos orientados a conexión, se suele exigir que se mantenga el orden en las PDU. Por ejemplo, si se está transfiriendo un fichero entre dos sistemas, es evidente, que se debe exigir que los registros del fichero se reciban en el mismo orden del fichero en el origen. Si cada PDU se numera secuencialmente y con un número distinto, mantener el orden en el receptor será una tarea sencilla, simplemente considerando los números de las PDU recibidas. Un problema en este tipo de esquema es que con un campo de números finitos, los números de secuencia se repetirán (módulo el máximo número posible de la secuencia). Evidentemente, el número máximo en la secuencia debe ser mayor que el máximo número de PDU pendientes. De hecho, en algunos casos (como por ejemplo, en ARQ con repetición selectiva, véase Capítulo 7) el máximo número tendrá que ser igual al doble del máximo número de PDU pendientes.

Control del flujo

El control del flujo es una operación realizada por la entidad receptora para limitar la velocidad o cantidad de datos que envía la entidad emisora.

La aproximación más sencilla para el control del flujo es el procedimiento de parada-y-espera, en el que cada PDU se debe confirmar antes de que se pueda enviar la siguiente. Los protocolos más eficientes implican la concesión de una especie de crédito al emisor, que no es sino la cantidad de datos que puede transmitir sin esperar confirmación. La técnica de ventana corredera del HDLC es un ejemplo típico de este procedimiento.

EL control del flujo es un ejemplo típico de una función que se debe realizar en varios protocolos. Considérese otra vez la Figura 1.6. La red necesitará controlar el flujo en el acceso a la red de X mediante el protocolo de control de acceso. Al mismo tiempo, el módulo de acceso a la red de Y tendrá un espacio limitado para la memoria temporal y por tanto tendrá que ejercer un control del flujo vía el protocolo de transporte. Por último, aunque el módulo de acceso a la red de Y puede controlar su flujo de datos, la aplicación en Y es igualmente vulnerable a una sobrecarga. Por ejemplo, la aplicación puede bloquearse esperando un acceso a disco. Por tanto, el control del flujo será necesario también en el nivel de aplicación.

---

[3] En la literatura inglesa se utiliza frecuentemente el término *host* (traducido por *estación*), y hace referencia a cualquier sistema final conectado a una red, como por ejemplo un PC, una estación de trabajo o un servidor.

Control de errores

Las técnicas de control de errores son necesarias para recuperar pérdidas o deterioros de los datos y de la información de control. Generalmente, el control de errores se implementa mediante dos funciones separadas: la detección de errores y la retransmisión. Para llevar a cabo la detección, el emisor inserta en cada PDU transmitida un código que sea capaz de detectar errores, este código será función de los bits que constituyan la PDU. El receptor comprobará el valor del código en la PDU recibida. Si se detecta un error, el receptor descartará la PDU. Si no se recibe una confirmación de la PDU transmitida dentro de un intervalo razonable de tiempo, el emisor retransmitirá la PDU. Algunos protocolos utilizan además algún código para la corrección de errores, el cual hace posible que el receptor no sólo detecte los errores, sino que además en algunos casos los corrija.

Al igual que el control del flujo, el control de errores es una función que se debe realizar en varios niveles de la arquitectura. Considérese de nuevo la Figura 1.6. El protocolo de acceso a la red debería incluir algún procedimiento para el control de errores para asegurar así que los datos se intercambian con garantía entre la estación y la red. No obstante, puede que dentro de la red se pierda algún paquete, por lo que el protocolo de transporte debería ser capaz de recuperar esta pérdida.

Direccionamiento

El concepto de direccionamiento dentro de una arquitectura es complejo y abarca una serie de cuestiones como las siguientes:

- El nivel del direccionamiento.
- El alcance del direccionamiento.
- Los identificadores de la conexión.
- El modo de direccionamiento.

Para la explicación se va a utilizar la Figura 2.4, en dicha figura se muestra una configuración en la que se utiliza la arquitectura TCP/IP. Los conceptos son esencialmente los mismos para la arquitectura OSI como para cualquier otra arquitectura.

El **nivel de direccionamiento** hace referencia al nivel de la arquitectura de comunicaciones en el que se identifica a la entidad. Normalmente, cada sistema (por ejemplo, un servidor o una estación de trabajo) o sistema intermedio (por ejemplo, un router) está asociado a una única dirección. Esa dirección por lo general es una dirección del nivel de red. En la arquitectura TCP/IP, esta dirección se denomina dirección IP, o simplemente dirección Internet. En el caso de la arquitectura OSI, se denominan punto de acceso al servicio de red (NSAP, Network Service Access Point). La dirección del nivel de red se utiliza para encaminar la PDU a través de la red o redes hasta el sistema destino, cuya dirección vendrá indicada en la dirección del nivel de red destino de la PDU.

Una vez que los datos llegan al destino, deberán cederse a algún proceso o aplicación dentro del sistema. Normalmente, el sistema destino podrá procesar varias aplicaciones y cada aplicación podrá servir a varios usuarios. A cada aplicación, y probablemente, a cada usuario concurrente de la aplicación se le asigna un identificador único, denominado en la arquitectura TCP/IP puerto o punto de acceso al servicio (SAP, Service Access Point) en la arquitectura OSI. Por ejemplo, una estación puede ejecutar simultáneamente una aplicación de correo electrónico y otra de transferencia de ficheros. Como mínimo cada aplicación deberá tener un número de puerto o SAP único dentro del sistema. Es más, la aplicación para la transferencia de ficheros puede dar servicio a varias transferencias simultáneas, en cuyo caso, cada transferencia deberá tener asignada de forma dinámica un número de puerto o SAP que sea único.

La Figura 2.4 muestra dos niveles de direccionamiento dentro del sistema. Éste es el caso típico de lo que ocurre en la arquitectura TCP/IP. No obstante, puede haber direccionamientos en cada nivel de la arquitectura. Por ejemplo, se puede asignar un SAP único para cada nivel de la arquitectura OSI.

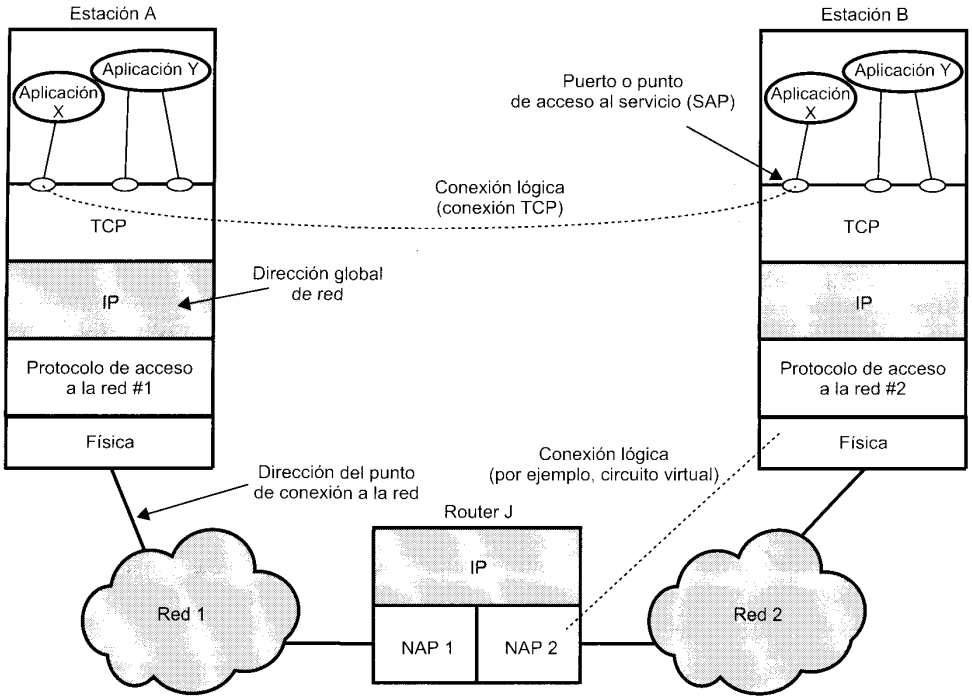


Figura 2.4. Conceptos de direccionamiento.

Otra cuestión relacionada en los sistemas finales o intermedios es el **alcance del direccionamiento**. La dirección Internet o NSAP que se han mencionado previamente son direcciones globales. Las características fundamentales de las direcciones globales son:

- **No ambigüedad global:** una dirección global identifica a un solo sistema. Los sinónimos están permitidos. Es decir, un sistema dado puede tener más de una dirección global.
- **Aplicabilidad global:** desde cualquier sistema se podrá identificar a cualquier otro, utilizando su dirección global.

Dado el carácter único y de aplicabilidad global de las direcciones, con ellas se hace posible que en Internet se encaminen datos desde cualquier sistema origen conectado a cualquier red hasta cualquier otro sistema destino situado en cualquier red distinta.

En la Figura 2.4 se muestra la necesidad de otro nivel adicional de direccionamiento. En cualquier red, todas las interfaces de cada dispositivo conectado deberán tener una única dirección. Como por ejemplo la dirección MAC en una red IEEE 802, o la dirección de la estación en una red X.25. Estas direcciones hacen posible que las redes encaminen las unidades de datos (por ejemplo, las tramas MAC o los paquetes X.25) y las hagan llegar al sistema destino. Este tipo de direcciones se denominan *direcciones del punto de conexión en la red.*

El alcance del direccionamiento es un concepto que sólo tiene sentido para direcciones del nivel de red. Por encima del nivel de red, un puerto o SAP debe ser único dentro del sistema destino pero no tiene por qué ser globalmente único. Por ejemplo, en la Figura 2.4, puede haber un puerto 1 en el sistema A y un puerto con igual número en el sistema B. La identificación completa de estos dos puertos podría ser de forma unívoca A.1 y B.1, respectivamente.

El concepto de **identificadores de la conexión** tiene sentido exclusivamente cuando se trata de transferencias orientadas a conexión (por ejemplo, circuitos virtuales), no siendo aplicables para el caso de transferencias no orientadas a conexión (por ejemplo, datagrama). Para estas últimas, se debe utilizar un nombre global para cada transmisión. En las transferencias orientadas a conexión, es a veces deseable utilizar un nombre de conexión durante la fase de transmisión. El escenario es como sigue: la entidad 1 en el sistema A solicita una conexión a la entidad 2 del sistema B, utilizando la dirección global B.2. Cuando B.2 acepta la conexión, se proporcionará un identificador de la conexión (normalmente un número), este identificador se utilizará por parte de las dos entidades en futuras transmisiones. La utilización de identificadores de la conexión tiene las siguientes ventajas:

- **Reducción de cabeceras:** los identificadores de la conexión son, por lo general, más cortos que los identificadores globales. Por ejemplo, en el protocolo X.25 (estudiado en el Capítulo 10) utilizado en las redes de conmutación de paquetes, los paquetes de solicitud de conexión contienen campos que especifican las direcciones origen y destino, con longitud predefinida del orden de varios octetos. Tras el establecimiento de la conexión lógica, denominada circuito virtual, los paquetes de datos contendrán un identificador para el circuito virtual de tan sólo 12 bits.
- **Encaminamiento:** al establecer la conexión se debe definir una ruta fija. El identificador de la conexión sirve para que los sistemas intermedios (por ejemplo, los nodos de conmutación de paquetes) identifiquen la ruta y puedan encaminar las PDU futuras.
- **Multiplexación:** esta función se estudiará posteriormente. No obstante, se puede adelantar que es posible que una entidad desee utilizar simultáneamente más de una conexión. Por tanto, las PDU se deben identificar mediante el identificador de la conexión.
- **Uso de la información de estado:** una vez que la conexión se haya establecido, los sistemas finales deben mantener información del estado relativa a la conexión. Esto posibilita funciones tales como el control del flujo o el control de errores mediante la utilización de números de secuencia. En los Capítulos 7 y 10 se considerarán ejemplos de estas técnicas en HDLC y X.25, respectivamente.

La Figura 2.4 muestra varios ejemplos de conexiones. La conexión lógica entre el router J y la estación B se lleva a cabo en el nivel de red. Por ejemplo, si la red 2 es una red de conmutación de paquetes que utilizara X.25, entonces esta conexión lógica debería ser un circuito virtual. En niveles superiores, muchos protocolos de transporte, como, por ejemplo, TCP proporcionan conexiones lógicas entre los usuarios del servicio de transporte. De esta manera, el TCP puede establecer una conexión entre dos puertos de diferentes sistemas.

Otro concepto relacionado es el **modo de direccionamiento**. En la mayoría de los casos, una dirección alude a un único sistema o puerto, en estas circunstancias el modo de direccionamiento se denomina *unidestino* (*unicast*). Ahora bien, es igualmente posible que una dirección aluda a más de una entidad o puerto. Este tipo de direcciones identifican simultáneamente a varios destinos. Por ejemplo, un usuario podría desear enviar un documento a una serie de destinos. O, por ejemplo, el centro de control de una red puede anunciar a todos los usuarios que la red se va a caer. Una dirección que identifique a varios usuarios puede ser de tipo *difusión* (*broadcast*) cuando aluda a todas las entidades dentro de un dominio, o puede ser de tipo *multidestino* (*multicast*) cuando se refiera a un subconjunto específico de entidades. En la Tabla 2.1 se ilustran las posibilidades.

Multiplexación

La multiplexación es un concepto relacionado con el direccionamiento. Un posible esquema de multiplexación es aquel en el que se establecen varias conexiones dentro de un único sistema. Por ejemplo, en X.25 puede haber varios circuitos virtuales que terminen en un sistema dado. En este caso, se podría decir que los circuitos virtuales se han multiplexado sobre una única interfaz física entre el sistema final y la red. La multiplexación también se puede llevar a cabo usando los nombres de los puertos, los cuales permiten a su vez múltiples conexiones. Por ejemplo, puede haber una serie de conexiones TCP que terminen en un sistema dado, cada una de ellas entre pares diferentes de puertos.

Tabla 2.1. Modos de direccionamiento.

Destino	Dirección de red	Dirección del sistema	Dirección de puerto/SAP
Unidestino	Individual	Individual	Individual
Multidestino	Individual Individual Todos	Individual Todos Todos	Grupo Grupo Grupo
Difusión	Individual Individual Todos	Individual Todos Todos	Todos Todos Todos

La multiplexación se utiliza en otros contextos distintos, en particular en la asignación de conexiones de un nivel a otro. Considérese de nuevo la Figura 2.4. La red 1 puede proporcionar un servicio de circuitos virtuales. Para cada conexión que se establezca en el nivel superior, se deberá establecer una conexión de circuito virtual en el nivel de acceso a la red. Ésta es una relación uno-a-uno que evidente-

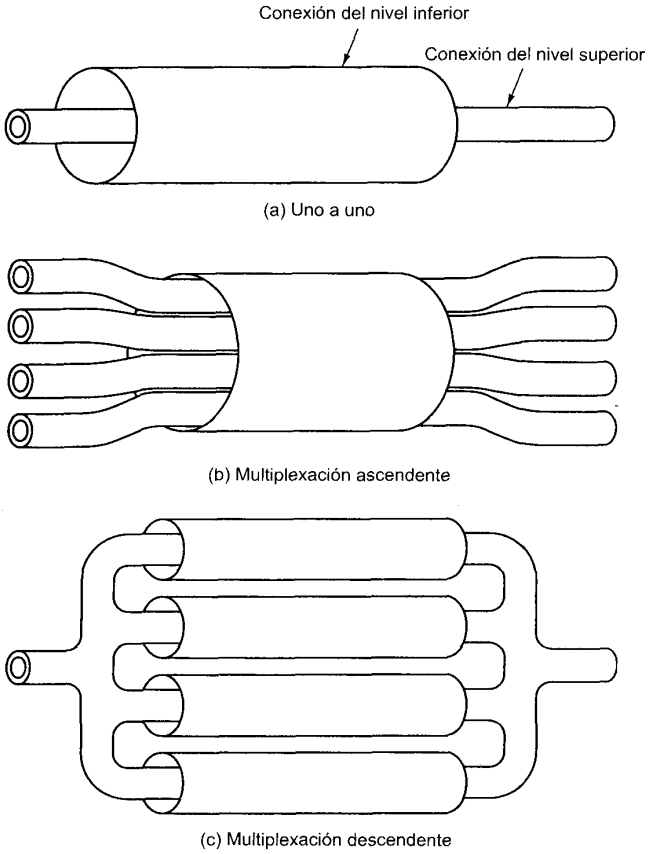


Figura 2.5. Multiplexación y conexiones de protocolos.

mente no tendrá siempre que ser necesariamente así. La multiplexación puede realizarse de dos formas distintas (Figura 2.5). La multiplexación ascendente (o hacia adentro), consiste en que varias conexiones del nivel superior comparten, o se multiplexan sobre una única conexión del nivel inferior. Esta técnica puede ser útil para hacer un uso más eficaz del servicio del nivel inferior o para proporcionar varias conexiones del nivel superior en un entorno donde sólo exista una única conexión de nivel inferior. En la Figura 2.5 se muestra un ejemplo de multiplexación ascendente. La multiplexación descendente, o división, consiste en establecer una única conexión del nivel superior utilizando varias conexiones del nivel inferior, el tráfico de la conexión del nivel superior se divide así entre las conexiones inferiores. Esta técnica se puede utilizar para añadir seguridad a la conexión, mejorar las prestaciones o la eficacia.

Servicios de transmisión

Un protocolo puede proporcionar una serie de servicios adicionales a las entidades que lo utilicen. Por ejemplo, cabe mencionar los siguientes ejemplos:

- **Prioridad:** ciertos mensajes, como, por ejemplo, los de control, puede que necesiten llegar a la entidad destino con el mínimo retardo posible. Un ejemplo de esta necesidad podría ser la solicitud de cierre de una conexión. En definitiva, las prioridades deberían estar asignadas a cada mensaje individualmente. Además de esto, cabría igualmente una asignación de prioridades por conexión.
- **Calidad de servicio:** ciertos tipos de datos requieren una velocidad de transmisión mínima o un retardo máximo.
- **Seguridad:** a veces ciertos mecanismos de seguridad, como, por ejemplo, el acceso restringido, pueden ser necesarios.

Todos estos sistemas dependerán del sistema de transmisión subyacente y de cualquiera de las entidades que intervengan en los niveles inferiores. Si los niveles inferiores pueden ofrecer estos servicios, las entidades superiores podrán hacer uso de los mismos invocando al protocolo correspondiente.

2.2. OSI

Como se estudió en el Capítulo 1, los estándares son necesarios para facilitar la interoperatividad entre equipos de distintos fabricantes y para estimular la economía de gran escala. Es evidente que una sola normalización no es suficiente, ya que las tareas en la comunicaciones son muy complejas. Es más, las funciones se deberían dividir en tareas más manejables y deberían organizarse como una arquitectura de comunicaciones. La arquitectura constituiría así un marco de referencia para la normalización.

Esta línea argumental llevó al ISO en 1977 a definir un subcomité que desarrollara tal arquitectura. El resultado fue el modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection). Aunque los elementos esenciales del modelo se definieron rápidamente, el estándar final de ISO, ISO 7498, no se publicó hasta 1984. La CCITT (ahora ITU-T) especificó una versión técnicamente compatible denominada X.200.

EL MODELO

Una técnica de estructuración muy utilizada, y elegida por ISO, es la jerarquización en capas. En esta técnica, las funciones de comunicación se distribuyen en un conjunto jerárquico de capas. Cada capa realiza un conjunto de funciones relacionadas entre sí, necesarias para comunicarse con otros sistemas. Cada capa se sustenta en la capa inmediatamente inferior, la cual realizará funciones más primitivas, ocultando los detalles a las capas superiores. Una capa proporciona servicios a la capa inmediatamente

superior. Idealmente, las capas deberían estar definidas para que los cambios en una capa no implicaran cambios en las otras capas. De esta forma, el problema se descompone en varios subproblemas más abordables.

La especificación de ISO consistió en definir el conjunto de capas y los servicios que cada una de ellas debería realizar. La división resultante debería agrupar a las funciones que fueran conceptualmente próximas, y a su vez, debiera implicar el suficiente número de capas como para que su complejidad fuera pequeña, pero por otro lado, este número no debiera ser muy elevado de forma que el procesamiento de la información suplementaria impuesta por la colección de capas fuera muy costoso. Los principios que guiaron el diseño se resumen en la Tabla 2.2. El modelo de referencia resultante tiene siete capas, que se describen con una breve definición en la Figura 1.10. En la Tabla 2.3 se da la explicación argumentada por el ISO para la selección de las siete capas.

En la Figura 2.6 se muestra la arquitectura OSI. Cada sistema contiene las siete capas. La comunicación se realiza entre las aplicaciones de dos computadores, denominadas en la Figura aplicaciones X e Y. Si la aplicación X desea enviar un mensaje a la aplicación Y, invoca a la capa de aplicación (capa 7). La capa 7 establece una relación paritaria con la capa 7 del computador destino, utilizando un protocolo de la capa 7 (protocolo de aplicación). Este protocolo necesita los servicios de la capa 6, por lo tanto las dos entidades de la capa 6 utilizan un protocolo propio, y así hacia abajo hasta la capa física, que transmite realmente los bits a través del medio de transmisión.

Obsérvese que, exceptuando la capa física, no existe una comunicación directa entre capas paritarias. Esto es, por encima de la capa física cada entidad de protocolo pasa los datos hacia la capa inferior contigua, para que ésta los envíe a su entidad par. Es más, el modelo OSI no requiere que los dos siste-

Tabla 2.2. Principios utilizados en la definición de las capas OSI (ISO 7498).

1. No crear demasiadas capas de forma que la descripción e integración de las capas sea más difícil de lo estrictamente necesario.
2. Definir separaciones entre capas tal que la descripción de servicios sea pequeña y el número de interacciones entre capas sea mínimo.
3. Definir capas separadas para funciones que sean claramente diferentes, en lo que respecta al servicio ofrecido como a la tecnología implicada.
4. Definir funciones similares en la misma capa.
5. Seleccionar los límites o separación entre capas de acuerdo con lo que la experiencia previa aconseje.
6. Definir las capas tal que las funciones se puedan localizar fácilmente de forma que la capa se pueda rediseñar completamente y tal que sus protocolos se puedan modificar para adaptarse a las innovaciones en la arquitectura, la tecnología hardware o en el software sin necesidad de cambiar los servicios que se usan o proporcionan en las capas adyacentes.
7. Definir una separación entre capas allí donde pueda ser útil tener la interfaz correspondiente normalizada.
8. Crear una capa donde exista la necesidad de un nivel diferente de abstracción en el procesamiento de los datos (por ejemplo, morfológico, sintáctico, semántico).
9. Permitir modificaciones de funciones o protocolos dentro de una capa, siempre que no afecten a otras capas.
10. Crear para cada capa límites o separaciones sólo con su capa superior e inferior.

Principios similares han sido aplicados para la creación de subcapas.

11. Crear subgrupos y organizaciones adicionales de funciones en subcapas dentro de una capa sólo en los casos donde se necesiten servicios distintos de comunicación.
12. Crear, donde sea necesario, dos o más subcapas con una funcionalidad común y por lo tanto mínima para permitir la operación de la interfaz con capas adyacentes.
13. Permitir la no utilización de todas las subcapas.

Tabla 2.3. Justificación de las capas OSI (ISO 7498).

1. Es esencial que la arquitectura permita la utilización de una realización realista de medios físicos para la interconexión con diferentes procedimientos de control (por ejemplo, V.24, V.25, etc.). La aplicación de los principios 3, 5 y 8 (Tabla 2.2) nos conduce a la identificación de la **Capa Física** como la capa más baja en la arquitectura.

2. Algunos medios de comunicación físicos (por ejemplo, la línea telefónica) requieren técnicas específicas para usarlos al transmitir datos entre sistemas a pesar de sufrir una tasa de error elevada (inaceptable para la gran mayoría de las aplicaciones). Estas técnicas específicas se utilizan en procedimientos de control del enlace de datos que han sido estudiados y normalizados durante varios años. También se debe reconocer que los nuevos medios de comunicación (por ejemplo, la fibra óptica) requerirán diferentes procedimientos de control del enlace de datos. La aplicación de los principios 3, 5 y 8 nos conduce a la identificación de la **Capa del Enlace de Datos** situada encima de la Capa Física en la arquitectura.

3. En la arquitectura OSI, algunos sistemas serán (actuarán como) el destino final de los datos. Algunos sistemas abiertos podrían actuar solamente como nodos intermedios (reenviando los datos a otros sistemas). La aplicación de los principios 3, 5 y 7 conduce a la identificación de la Capa de Red encima de la Capa del Enlace de Datos. Así, la Capa de Red proporcionará un camino de conexión (conexión de red) entre un par de entidades de transporte incluyendo el caso en el que estén involucrados nodos intermedios.

4. El control del transporte de los datos desde el sistema final origen al sistema final destino (que no se lleva a cabo en nodos intermedios) es la función que realiza el servicio de transporte. Así, la capa superior situada justo encima de la Capa de Red es la **Capa de Transporte**. Esta Capa libera a las entidades de capas superiores de cualquier preocupación sobre el transporte de datos entre ellas.

5. Existe una necesidad de organizar y sincronizar el diálogo, y controlar el intercambio de datos. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **Capa de Sesión**, situada sobre la Capa de Transporte.

6. El conjunto restante de funciones de interés general son aquellas relacionadas con la representación y la manipulación de datos estructurados para el beneficio de los programas de aplicación. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **Capa de Presentación** situada sobre la Capa de Sesión.

7. Finalmente, están las aplicaciones que llevan a cabo el procesamiento de la información. La **Capa de Aplicación**, que es la más alta de la arquitectura aborda parcialmente este procesamiento junto con los protocolos involucrados.

mas estén conectados directamente, ni siquiera en la capa física. Por ejemplo, para proporcionar el enlace de comunicación se puede utilizar una red de conmutación de paquetes o de conmutación de circuitos.

La Figura 2.6 también muestra las unidades de datos de protocolo (PDU, Protocol Data Unit) en la arquitectura OSI. En primer lugar, considérese la forma más habitual de implementar un protocolo. Cuando la aplicación X tiene un mensaje para enviar a la aplicación Y, transfiere estos datos a una entidad de la capa de aplicación. A los datos se les añade una cabecera que contiene información necesaria para el protocolo de la capa 7 (encapsulado). Seguidamente, los datos originales más la cabecera se pasan como una unidad a la capa 6. La entidad de presentación trata la unidad completa como si de datos se tratara y le añade su propia cabecera (un segundo encapsulado). Este proceso continúa hacia abajo hasta llegar a la capa 2, que normalmente añade una cabecera y una cola (como así lo hace el protocolo HDLC). La unidad de datos de la capa 2, llamada trama, se pasa al medio de transmisión mediante la capa física. En el destino al recibir la trama ocurre el proceso inverso. Conforme los datos ascienden, cada capa elimina la cabecera más externa, actúa sobre la información de protocolo contenida en ella y pasa el resto de la información hacia la capa inmediatamente superior.

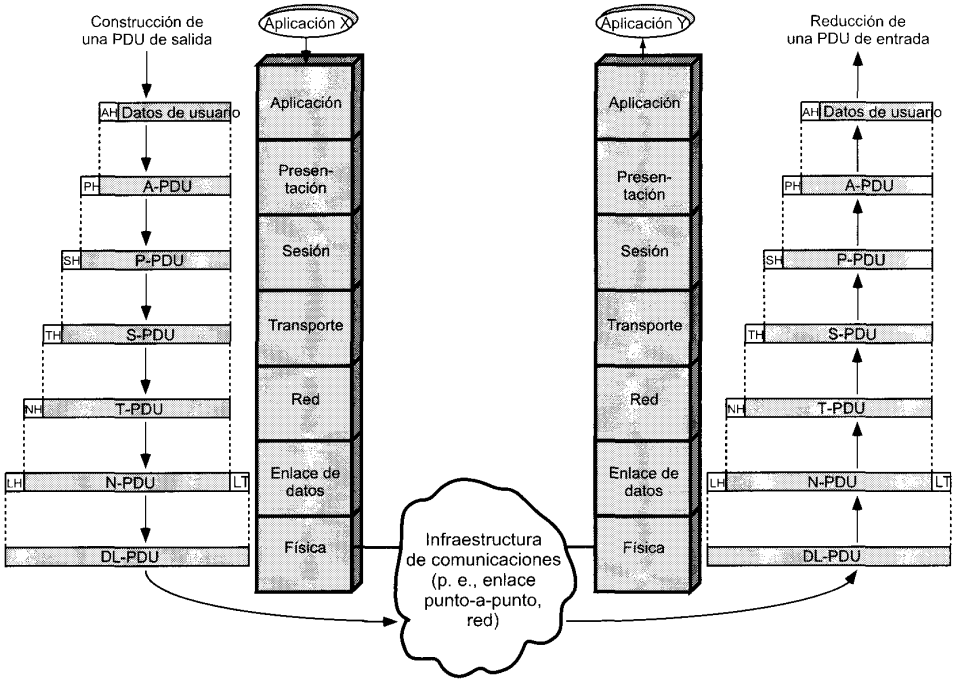


Figura 2.6. El entorno OSI.

En cada nivel, cada capa puede fragmentar en varias partes la unidad de datos que recibe de la capa superior adyacente, de acuerdo con sus propias necesidades. Las unidades de datos deben ser ensambladas por la entidad par correspondiente antes de pasarlas a la capa superior.

NORMALIZACIÓN DENTRO DEL MODELO DE REFERENCIA OSI[4]

La principal motivación para el desarrollo del modelo OSI fue proporcionar un modelo de referencia para la normalización. Dentro del modelo, en cada capa se pueden desarrollar uno o más protocolos. El modelo define en términos generales las funciones que se deben realizar en cada capa y simplifica el procedimiento de la normalización ya que:

- Como las funciones de cada capa están bien definidas, para cada una de las capas, el establecimiento de normas o estándares se pueden desarrollar independiente y simultáneamente. Esto acelera el proceso.
- Como los límites entre capas están bien definidos, los cambios que se realicen en los estándares para una capa dada no afectan al software de las otras. Esto hace que sea más fácil introducir nuevas normalizaciones.

La Figura 2.7 muestra el uso del modelo de referencia OSI. La función global de comunicación se descompone en 7 capas distintas, utilizando los principios indicados en la Tabla 2.2. Estos principios esencialmente vienen a ser los mismos que rigen en el diseño modular. Esto es, la función total se descompone en una serie de módulos, haciendo que las interfaces entre módulos sean tan sencillas como

[4] Los conceptos que aquí se introducen son válidos igualmente para la arquitectura TCP/IP.

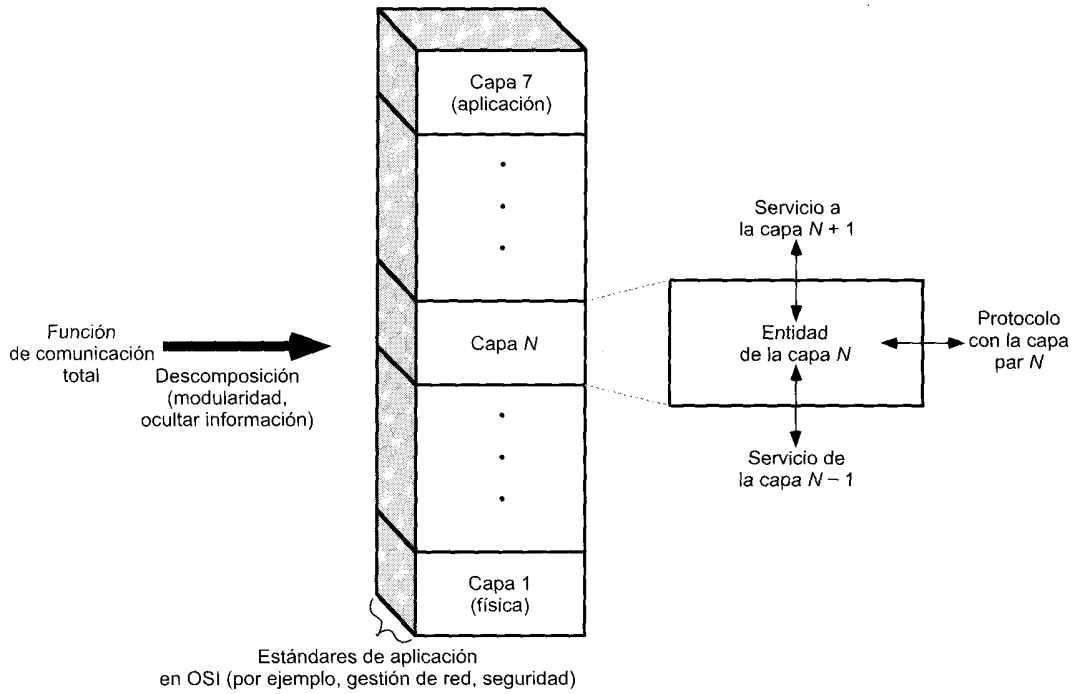


Figura 2.7. La arquitectura OSI como un modelo de referencia para la normalización.

sea posible. Además, se utiliza el principio de ocultación de la información: las capas inferiores abordan ciertos detalles de tal manera que las capas superiores sean ajenas a las particularidades de estos detalles. Dentro de cada capa, se suministra tanto el servicio proporcionado a la capa superior adyacente, como el protocolo a la capa par en el sistema remoto.

La Figura 2.8 muestra de una forma más específica la naturaleza de la normalización requerida en cada capa. Existen tres elementos clave:

- **Especificación del protocolo:** dos entidades en la misma capa en sistemas diferentes cooperan e interactúan por medio del protocolo. El protocolo se debe especificar con precisión ya que están implicados dos sistemas abiertos diferentes. Esto incluye al formato de la unidad de datos del protocolo, la semántica de todos los campos, así como a la secuencia permitida de PDU.
- **Definición del servicio:** además del protocolo o protocolos que operan en una capa dada, se necesitan normalizaciones para los servicios que cada capa ofrece a la capa superior contigua. Normalmente, la definición de los servicios es equivalente a una descripción funcional que define *qué* servicios se están proporcionando, pero no *cómo* se están proporcionando.
- **Direccionamiento:** cada capa suministra servicios a las entidades en la capa superior adyacente. Las entidades se identifican mediante un punto de acceso al servicio (SAP, Service Access Point), Así, un punto de acceso al servicio de red (NSAP, Network SAP) indica una entidad de transporte que es usuaria del servicio de red.

En los sistemas abiertos, la necesidad de proporcionar una especificación del protocolo precisa evidencia por sí sola. Los otros dos elementos de la lista anterior requieren más comentarios. Con respecto a la definición de servicios, la motivación para proporcionar sólo una definición funcional es por lo siguiente. Primero, la interacción entre capas adyacentes tiene lugar dentro de los confines de un único sistema abierto y por tanto le incumbe sólo a él. Así, mientras las capas pares en diferentes sistemas

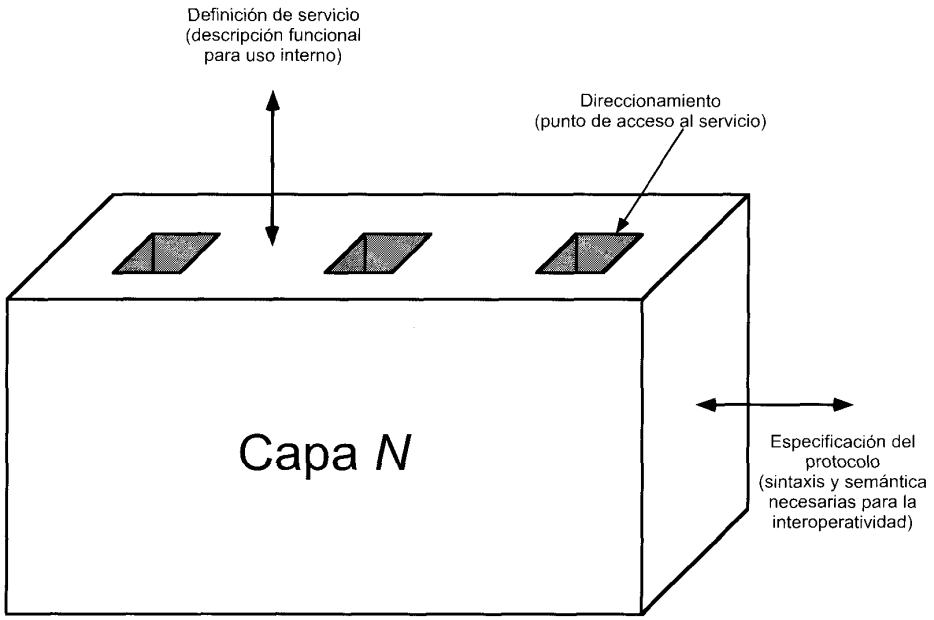


Figura 2.8. Normas específicas de capa.

proporcionen los mismos servicios a las capas superiores adyacentes, los detalles de cómo se suministran los servicios pueden diferir de un sistema a otro sin que ello implique pérdida de interoperatividad. Segundo, es frecuente que las capas adyacentes estén implementadas en el mismo procesador. En estas circunstancias, sería interesante dejar libre al programador del sistema para que utilice el hardware y el sistema operativo para que proporcionen una interfaz que sea lo más eficiente posible. En lo que se refiere al direccionamiento, la utilización de un mecanismo de direccionamiento en cada capa, materializado en el SAP, permite que cada capa multiplexe varios usuarios de la capa inmediatamente superior. La multiplexación no se lleva a cabo en todos los niveles, no obstante el modelo lo permite.

PRIMITIVAS DE SERVICIO Y PARÁMETROS

En la arquitectura OSI los servicios entre capas adyacentes se describen en términos de primitivas y mediante los parámetros involucrados. Una primitiva especifica la función que se va a llevar a cabo y los parámetros se utilizan para pasar datos e información de control. La forma concreta que adopte la primitiva dependerá de la implementación. Un ejemplo es la llamada a un procedimiento.

Para definir las interacciones entre las capas adyacentes de la arquitectura se utilizan cuatro primitivas (X.210). Éstas se definen en la Tabla 2.4. En la Figura 2.9a se muestra la ordenación temporal de estos eventos. Por ejemplo, considere la transferencia de datos desde una entidad (N) a su entidad par (N) en otro sistema. En esta situación se verifican los siguientes hechos:

1. La entidad origen (N) invoca a su entidad ($N - 1$) con una primitiva de solicitud. Asociado a esta primitiva están los parámetros necesarios, como, por ejemplo, los datos que se van a transmitir y la dirección destino.
2. La entidad origen ($N - 1$) prepara una PDU ($N - 1$) para enviársela a su entidad par ($N - 1$).
3. La entidad destino ($N - 1$) entrega los datos al destino apropiado (N) a través de la primitiva de indicación, que incluye como parámetros los datos y la dirección origen.

Tabla 2.4. Tipos de primitivas de servicio.

SOLICITUD	Primitiva emitida por el usuario del servicio para invocar algún servicio y pasar los parámetros necesarios para especificar completamente el servicio solicitado.
INDICACIÓN	Primitiva emitida por el suministrador del servicio para: 1. indicar que se ha sido invocado un procedimiento por el usuario de servicio par en la conexión y para suministrar los parámetros asociados, o 2. notificar al usuario del servicio sobre una acción iniciada por el suministrador.
RESPUESTA	Primitiva emitida por el usuario del servicio para confirmar o completar algún procedimiento invocado previamente mediante una indicación a ese usuario.
CONFIRMACIÓN	Primitiva emitida por el suministrador del servicio para confirmar o completar algún procedimiento invocado previamente mediante una solicitud por parte del usuario del servicio.

4. Si se requiere una confirmación, la entidad destino (N) emite una primitiva de respuesta a su entidad ($N - 1$).
5. La entidad ($N - 1$) convierte la confirmación en una PDU ($N - 1$).
6. La confirmación se entrega a la entidad (N) como una primitiva de confirmación.

Esta secuencia de eventos se conoce como un **servicio confirmado**, ya que el que inicia la transferencia recibe una confirmación de que el servicio solicitado ha tenido el efecto deseado en el otro extremo. Si solamente se invocan las primitivas de solicitud e indicación (correspondientes a los pasos 1 a 3), entonces se denomina **servicio no confirmado**; la entidad que inicia la transferencia no recibe confirmación de que la acción solicitada haya tenido lugar (Figura 2.9b).

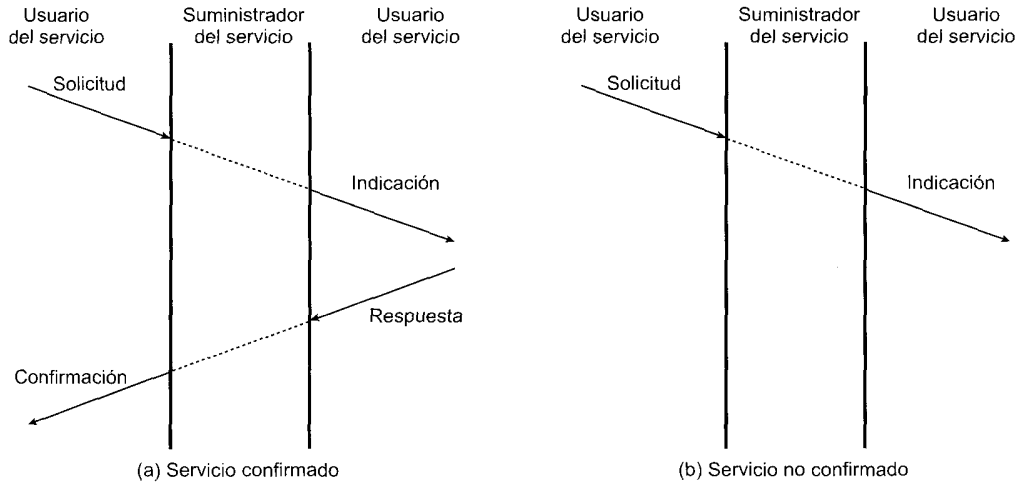


Figura 2.9. Diagramas de la secuencia temporal de las primitivas de servicio.

LAS CAPAS DE OSI

En este apartado se estudian brevemente cada una de la capas y, donde sea apropiado, se dan ejemplos de normalizaciones para los protocolos de estas capas.

Capa Física

La capa física se encarga de la interfaz física entre los dispositivos, además define las reglas que rigen en la transmisión de los bits. La capa física tiene cuatro características importantes:

- **Mecánicas:** relacionadas con las propiedades físicas de la interfaz y con el medio de transmisión. Normalmente, dentro de estas características se incluye la especificación del conector que transmite las señales a través de conductores. A estos últimos se les denominan circuitos.
- **Eléctricas:** especifican cómo se representan los bits (por ejemplo, en términos de niveles de tensión), así como su velocidad de transmisión.
- **Funcionales:** especifican las funciones que realiza cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión.
- **De procedimiento:** especifican la secuencia de eventos que se llevan a cabo en el intercambio del flujo de bits a través del medio físico.

En el Capítulo 6 se estudian con detalle los protocolos de la capa física. Algunos ejemplos de estándares de esta capa son el EIA-232-F y algunas secciones de los estándares RDSI y de LAN.

Capa del Enlace de Datos

Mientras que la capa física proporciona exclusivamente un servicio de transmisión de datos, la capa de enlace de datos intenta hacer que el enlace físico sea seguro, además proporciona los medios para activar, mantener y desactivar el enlace. El servicio principal proporcionado por la capa de enlace de datos a las capas superiores es el de detección y control de errores. Así, si se dispone de un protocolo en la capa del enlace de datos completamente operativo, la capa adyacente superior puede suponer que la transmisión está libre de errores. Sin embargo, si la comunicación se realiza entre dos sistemas que no están directamente conectados, la conexión constará de varios enlaces de datos en serie, cada uno operando independientemente. Por tanto, en este último caso, la capa superior no estará libre de la responsabilidad del control de errores.

El Capítulo 7 se dedica a los protocolos de enlace de datos. Algunos ejemplos de estándares en esta capa son HDLC, LAPB, LLC y LAPD.

Capa de Red

La capa de red realiza la transferencia de información entre sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacente y las tecnologías de conmutación utilizadas para conectar los sistemas. En esta capa, el computador establecerá un diálogo con la red para especificar la dirección destino y solicitar ciertas facilidades, como, por ejemplo, la gestión de prioridades.

Existe un amplio abanico de posibilidades para que los servicios de comunicación intermedios sean gestionados por la capa de red. En el extremo más sencillo están los enlaces punto-a-punto directos entre estaciones. En este caso, no se necesita capa de red ya que la capa de enlace de datos puede proporcionar las funciones necesarias de gestión. Siguiendo en orden de complejidad creciente podemos considerar un sistema conectado a través de una única red, como una red de conmutación de circuitos o de conmutación de paquetes. Un ejemplo de esta situación es el nivel de paquete del estándar X.25. La Figura 2.10 muestra cómo la presencia de una red se encuadra dentro de la arquitectura OSI. Las tres capas inferiores están relacionadas con la conexión y la comunicación con la red. Los paquetes creados por el sistema final pasan a través de uno o más nodos de la red que actúan como retransmisores entre los dos sistemas finales. Los nodos de la red implementan las capas 1 a 3 de la arquitectura. En la figura anterior se muestran dos sistemas finales conectados a través de un único nodo de red. La capa 3 en el

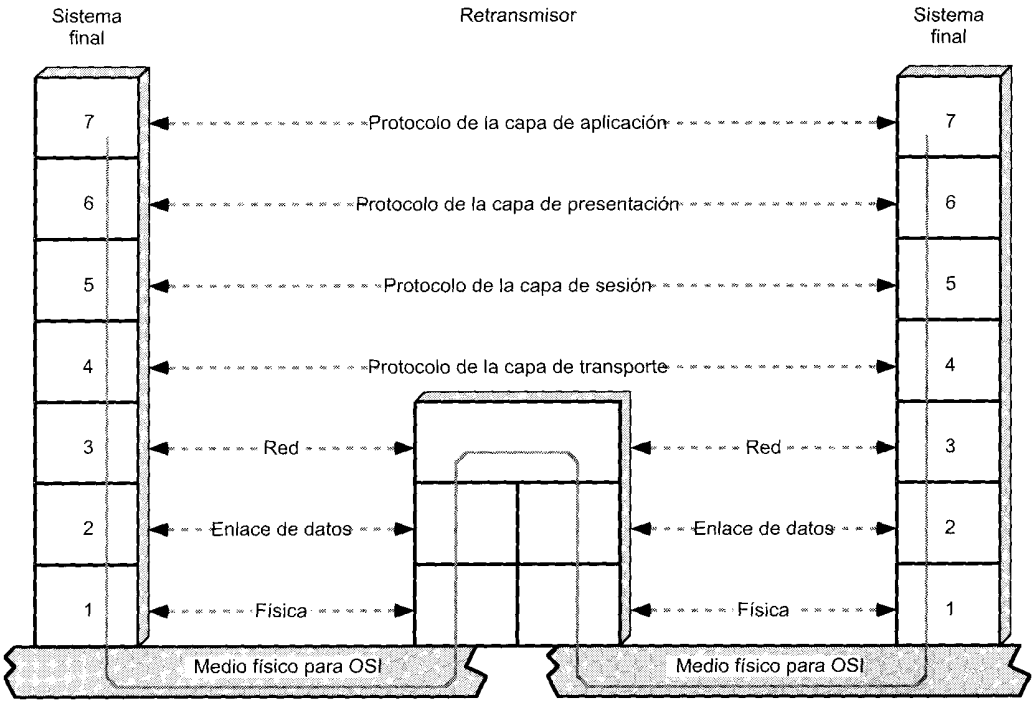


Figura 2.10. Utilización de un retransmisor.

nodo realiza las funciones de conmutación y encaminamiento. Dentro del nodo, existen dos capas de enlace de datos y dos capas físicas, correspondientes a los enlaces con los dos sistemas finales. Cada capa de enlace de datos (y física) opera independientemente para proporcionar el servicio a la capa de red sobre su respectivo enlace. Las cuatro capas superiores son protocolos «extremo-a-extremo» entre los sistemas finales.

En el otro extremo de complejidad, una configuración para la capa de red puede consistir en dos sistemas finales que necesitan comunicarse sin estar conectados a la misma red. Más bien, supondremos que están conectados a redes que, directamente o indirectamente, estén conectadas entre sí. Este caso requiere el uso de alguna técnica de interconexión entre redes; estas técnicas se estudiarán en el Capítulo 16.

Capa de Transporte

La capa de transporte proporciona un mecanismo para intercambiar datos entre sistemas finales. El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en orden y sin pérdidas ni duplicaciones. La capa de transporte también puede estar involucrada en la optimización del uso de los servicios de red, proporcionando la calidad del servicio solicitada. Por ejemplo, la entidad de sesión puede solicitar una tasa de error determinada, un retardo máximo, una prioridad y un nivel de seguridad dado.

El tamaño y la complejidad del protocolo de transporte dependen de cómo de seguras o inseguras sean las redes subyacentes y los servicios de red. Consecuentemente, ISO ha desarrollado una familia de 5 estándares de protocolos de transporte, cada uno de ellos especificado para un determinado servicio subyacente. En la arquitectura de protocolos TCP/IP, se han especificado dos protocolos para la capa de transporte: el orientado a conexión TCP (protocolo de control de la transmisión, «Transmission Control

Protocol») y el no orientado a conexión UDP (protocolo de datagrama de usuario, «User Datagram Protocol»).

Capa de Sesión

Las cuatro capas inferiores del modelo OSI proporcionan un medio para el intercambio seguro de datos y proporcionan a su vez, distintos niveles de calidad de servicio. Para muchas aplicaciones el servicio más básico es a todas luces insuficiente. Por ejemplo, una aplicación de acceso a un terminal remoto puede requerir un diálogo semi-duplex. Por el contrario, una aplicación para el procesamiento de transacciones puede necesitar la inclusión puntos de comprobación en el flujo de transferencia para poder hacer operaciones de respaldo y recuperación. De igual manera, otra aplicación para procesar mensajes puede requerir la posibilidad de interrumpir el diálogo, generar más mensaje y posteriormente continuar el diálogo desde donde se dejó.

Todas estas capacidades se podrían incorporar en las aplicaciones de la capa 7. Sin embargo, ya que todas estas herramientas para el control del diálogo son ampliamente aplicables, parece lógico organizarlas en una capa separada, denominada la capa de sesión.

La capa de sesión proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos los servicios de la capa de sesión son parcialmente, o incluso totalmente prescindibles, no obstante en algunas aplicaciones su utilización es ineludible. La capa de sesión proporciona los siguientes servicios:

- **Control del diálogo:** éste puede ser simultáneo en los dos sentidos (*full duplex*) o alternado en ambos sentidos (*half duplex*).
- **Agrupamiento:** el flujo de datos se puede marcar para definir grupos de datos. Por ejemplo, si una empresa está transmitiendo los datos correspondientes a las ventas hacia una oficina regional, éstos se pueden marcar de tal manera que se indique por grupos el final de las ventas realizadas en cada departamento. Este servicio permitiría que el computador destino calcule los totales de las ventas realizadas en cada departamento.
- **Recuperación:** la capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

ISO ha definido una normalización para la capa de sesión que incluye como opciones los servicios que se acaban de describir.

Capa de Presentación

La capa de presentación define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. La capa de presentación define la sintaxis utilizada entre las entidades de aplicación y proporciona los medios para seleccionar y modificar la representación utilizada. Algunos ejemplos de servicios específicos que se pueden realizar en esta capa son los de comprensión y cifrado de datos.

Capa de Aplicación

La capa de aplicación proporciona a los programas de aplicación un medio para que accedan al entorno OSI. Esta capa incluye a las funciones de administración y en general, a los mecanismos necesarios en la implementación de las aplicaciones distribuidas. Además, a esta capa pertenecen las aplicaciones de uso general como, por ejemplo, la transferencia de ficheros, el correo electrónico y el acceso desde terminales a computadores remotos, entre otras.

2.3. ARQUITECTURA DE PROTOCOLOS TCP/IP

Durante muchos años, la literatura técnica que trataba las arquitecturas de protocolos estaba dominada por las discusiones relacionadas con OSI, así como por el desarrollo de protocolos y servicios para cada capa. Durante los años ochenta la creencia más extendida era que OSI llegaría a imponerse frente a arquitecturas comerciales como la SNA de IBM y frente a esquemas no propietarios («multivendor») como TCP/IP. Esta previsión nunca se cumplió. En los noventa, TCP/IP ha conseguido erigirse como la arquitectura comercial dominante, a la vez que se ha convertido en la familia o conjunto de protocolos sobre la que se desarrollaran los protocolos futuros.

Existe una serie de razones que justifican el éxito de los protocolos TCP/IP sobre OSI. Ente ellas se pueden enumerar a las siguientes:

1. Los protocolos TCP/IP se especificaron y se utilizaron de una forma generalizada antes de la normalización ISO. Así, en los años ochenta las instituciones que tenían necesidades apremiantes de intercambio de información se enfrentaron al dilema de esperar a la disponibilidad del paquete siempre prometido y nunca entregado de OSI, o por el contrario utilizar el conjunto TCP/IP de disponibilidad inmediata y operatividad cada vez más contrastada. Una vez hecha la elección de TCP/IP, el coste y los riesgos de la migración a un entorno nuevo, inhibió la aceptación de ISO.
2. Los protocolos TCP/IP se desarrollaron inicialmente como resultado del esfuerzo investigador en el entorno militar de los EE.UU., financiado por el Departamento de Defensa (DOD, Department Of Defense). Aunque el DOD, como el resto del gobierno de los EE.UU., estaba involucrado en los procesos internacionales de normalizaciones, el DOD tenía una necesidad imperiosa e inmediata de conectividad, tal que no le permitía esperar hasta los años ochenta o incluso principios de los noventa a productos basados en OSI. Por consiguiente, el DOD exigió el uso de los protocolos TCP/IP en todas sus adquisiciones de software. Debido a que el DOD es el consumidor más grande de software en el mundo, esta política creó un mercado enorme, animando a los vendedores a desarrollar productos basados en TCP/IP.
3. Internet está construida sobre el conjunto de protocolos TCP/IP. El crecimiento impresionante de Internet y especialmente de la «World Wide Web» (red extendida mundial) ha cimentado la victoria de TCP/IP sobre OSI.

LA APROXIMACIÓN DE TCP/IP

El conjunto de protocolos TCP/IP reconoce que la tarea de la comunicación es lo suficientemente compleja y diversa como para realizarla en una única unidad. Consecuentemente, la tarea se descompone en diversos módulos o entidades, que se pueden comunicar con sus entidades pares del sistema remoto. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras entidades. Las reglas de diseño del software de calidad dictan que estas entidades se deben agrupar en una forma modular y jerárquica.

El modelo OSI se basa en el mismo razonamiento, pero introduce un paso más. El siguiente paso en OSI está en reconocer que, en muchos aspectos, los protocolos en el mismo nivel de la jerarquía tienen algunas características comunes. Esto desemboca ineludiblemente en el concepto de nivel o capa, así como en el intento de describir de una forma abstracta las características comunes de los protocolos en un nivel dado.

Como herramienta didáctica, un modelo en capas tiene un valor significativo y, de hecho, el modelo OSI se utiliza por ese motivo en muchos textos de telecomunicaciones. Los diseñadores del conjunto de protocolos TCP/IP ponen la objeción que el modelo OSI es más prescriptivo que descriptivo. El modelo OSI ordena que los protocolos dentro de una capa dada realicen unas determinadas funciones. Esto puede no ser siempre deseable. Es posible definir más de un protocolo en una capa dada, y en este caso

puede que la funcionalidad de estos protocolos no sea la misma o ni incluso similar. Ahora bien, lo que tienen en común un conjunto de protocolos de la misma capa es que se sustentan sobre el mismo conjunto de protocolos de la capa inferior adyacente.

Además, debido a que en el modelo OSI las interfaces entre capas están bien definidas es posible sustituir un protocolo de una capa por otra versión más reciente, sin que ello implique modificar las capas adyacentes (véase principio 6, Tabla 2.2). Esto no es siempre deseable o incluso posible. Por ejemplo, una LAN se presta fácilmente para un esquema de direccionamiento con difusión y multidifusión en el nivel de enlace. Si el nivel de enlace de IEEE 802 se situara debajo de una entidad de protocolo de red que no permitiera difusión ni multidifusión, este servicio sería inaccesible para las capas superiores en la jerarquía. Para eludir este tipo de problemas, los especificadores de OSI introducen el concepto de capas o subcapas nulas. A veces, parece que estos artificios salvan al modelo a expensas de diseño no adecuado de los protocolos.

En el modelo TCP/IP, el uso estricto de todas las capas no es obligatorio. Por ejemplo, hay protocolos de aplicación que operan directamente sobre IP.

LA ARQUITECTURA DE PROTOCOLOS TCP/IP

En el Capítulo 1 se presentó la familia de protocolos TCP/IP. Como ya se señaló no existe un modelo de protocolos TCP/IP «oficial». Sin embargo, es de utilidad considerar que el conjunto de protocolos está involucrado en cinco capas. Para resumir el Capítulo 1, estas capas son:

- **Capa de aplicación:** proporciona la comunicación entre procesos o aplicaciones de computadores separados.
- **Capa de transporte o extremo-a-extremo:** proporciona un servicio de transferencia de datos extremo-a-extremo. Esta capa puede incluir mecanismos de seguridad. Oculta los detalles de la red, o redes subyacentes, a la capa de aplicación.
- **Capa Internet:** relacionada con el encaminamiento de los datos del computador origen al destino a través de una o más redes conectadas por dispositivos de encaminamiento.
- **Capa de acceso a la red:** relacionada con la interfaz lógica entre un sistema final y una subred.
- **Capa física:** define las características del medio de transmisión, la tasa de señalización y el esquema de codificación de las señales.

FUNCIONAMIENTO DE TCP E IP

La Figura 2.4 muestra cómo se configuran los protocolos TCP/IP. Para conectar un computador a una subred se utiliza algún tipo de protocolo de acceso como, por ejemplo, Ethernet. Este protocolo permite al computador enviar datos a través de la subred a otro computador o, en caso de que el destino final esté en otra subred, a un dispositivo de encaminamiento. IP se implementa en todos los sistemas finales y dispositivos de encaminamiento. Actúa como un porteador que transportara bloques de datos desde un computador hasta otro, a través de uno o varios dispositivos de encaminamiento. TCP se implementa solamente en los sistemas finales; guarda un registro de los bloques de datos para asegurar que todos se entregan de forma segura a la aplicación apropiada.

Para tener éxito en la transmisión, cada entidad en el sistema global debe tener una única dirección. En realidad, se necesitan dos niveles de direccionamiento. Cada computador en la red debe tener una única dirección internet que permita enviar los datos al computador adecuado. Además, cada proceso que se ejecute dentro de un computador en red debe tener a su vez una dirección que sea única dentro del mismo; esto permite al protocolo extremo-a-extremo (TCP) entregar los datos al proceso adecuado. Estas últimas direcciones se denominan puertos.

A continuación, se va a describir paso a paso el funcionamiento de la Figura 2.4. Supóngase que un proceso, asociado al puerto 1 en el computador A, desea enviar un mensaje a otro proceso, asociado al puerto 2 del computador B. El proceso en A pasa el mensaje al TCP con la instrucción de enviarlo al puerto 2 del computador B. EL TCP pasa el mensaje al IP con instrucciones de que lo envíe al computador B. Obsérvese que no es necesario comunicarle al IP la identidad del puerto destino. Todo lo que necesita saber es que los datos van dirigidos al computador B. A continuación, IP pasa el mensaje a la capa de acceso a la red (por ejemplo, a la lógica Ethernet) con el mandato expreso de enviarlo al dispositivo de encaminamiento X (el primer salto en el camino a B).

Para controlar esta operación se debe transmitir información de control junto con los datos de usuario, como así se sugiere en la Figura 2.11. Supongamos que el proceso emisor genera un bloque de datos y lo pasa al TCP. El TCP puede que divida este bloque en fragmentos más pequeños para hacerlos más manejables. A cada uno de estos fragmentos le añade información de control, denominada cabecera TCP, formando un segmento TCP. La información de control la utilizará la entidad par TCP en el computador B. Entre otros, en la cabecera se incluyen los siguientes campos:

- **Puerto destino:** cuando la entidad TCP en B recibe el segmento, debe conocer a quién se le deben entregar los datos.
- **Número de secuencia:** TCP numera secuencialmente los segmentos que envía a un puerto destino dado, para que si llegan desordenados la entidad TCP en B pueda reordenarlos.
- **Suma de comprobación:** la entidad emisora TCP incluye un código calculado en función del resto del segmento. La entidad receptora TCP realiza el mismo cálculo y compara el resultado con el código recibido. Si se observa alguna discrepancia implicará que ha habido algún error en la transmisión.

A continuación, TCP pasa cada segmento al IP con instrucciones para que los transmita a B. Estos segmentos se transmitirán a través de una o varias subredes y serán retransmitidos en uno o más dispositivos de encaminamiento intermedios. Esta operación también requiere el uso de información de control. Así, el IP añade una cabecera de información de control a cada segmento para formar un datagrama IP. En la cabecera IP, además de otros campos, se incluirá la dirección del computador destino (en nuestro ejemplo B).

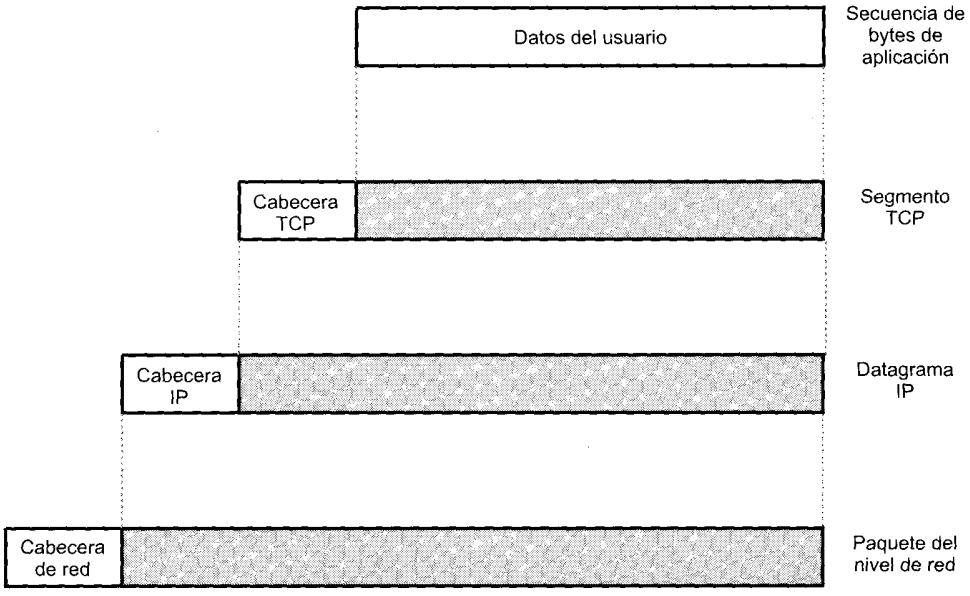


Figura 2.11. Unidades de datos de protocolo en la arquitectura TCP/IP.

Finalmente, cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red añade su propia cabecera, creando un paquete, o trama. El paquete se transmite a través de la red al dispositivo de encaminamiento J. La cabecera del paquete contiene la información que la red necesita para transferir los datos. La cabecera puede contener, entre otros, los siguientes campos:

- **Dirección de la red destino:** la red debe conocer a qué dispositivo conectado se debe entregar el paquete.
- **Funciones solicitadas:** el protocolo de acceso a la red podría solicitar la utilización de ciertas funciones que ofrezca la red, como, por ejemplo, la utilización de prioridades.

En el dispositivo de encaminamiento J se elimina la cabecera del paquete y se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la red 2 hacia B basándose en la dirección destino que contenga la cabecera IP. Para hacer esto, se le añade al datagrama una cabecera de acceso a la red.

Cuando se reciben los datos en B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos de usuario alcancen al proceso destino.

INTERFACES DE PROTOCOLO

En la familia de protocolos TCP/IP cada capa interacciona con sus capas adyacentes. En el origen, la capa de aplicación utilizará los servicios de la capa extremo-a-extremo, pasándole los datos. Este procedimiento se repite en la interfaz entre la capa extremo-a-extremo y la capa internet, e igualmente en la interfaz entre la capa internet y la capa de acceso a la red. En el destino, cada capa entrega los datos a la capa superior adyacente.

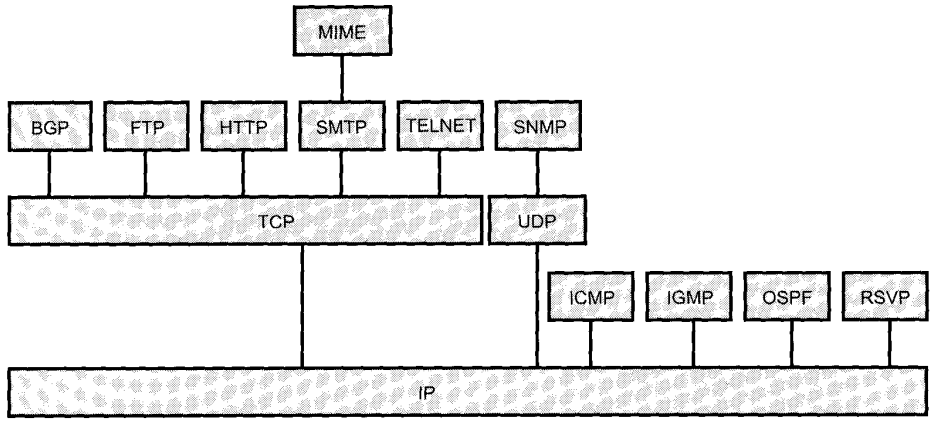
La arquitectura de TCP/IP no exige que se haga uso de todas las capas. Como así se sugiere en la Figura 2.12, es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa. La mayoría de las aplicaciones requieren un protocolo extremo-a-extremo seguro y por tanto utilizan TCP. Algunas de estas aplicaciones, como el protocolo sencillo de gestión de red (SNMP, Simple Network Management Protocol), utilizan un protocolo extremo-a-extremo alternativo denominado protocolo de datagrama de usuario (UDP, User Datagram Protocol); otras, en cambio, pueden hacer uso de IP directamente. Las aplicaciones que no necesiten interconexión de redes y que no necesiten TCP pueden invocar directamente los servicios de la capa de acceso a la red.

LAS APLICACIONES

La Figura 2.12 muestra la organización de los protocolos más importantes de la familia de TCP/IP. La mayoría de estos protocolos se estudiarán en la Parte V de este texto. En esta sección, resaltaremos tres protocolos que históricamente han sido considerados esenciales en TCP/IP, y que se diseñaron por el DOD como estándares militares junto a TCP e IP.

El **protocolo sencillo de transferencia de correo (SMTP, Simple Mail Transfer Protocol)** proporciona una función básica de correo electrónico. Proporciona un mecanismo para transferir mensajes entre computadores remotos. Entre las propiedades del SMTP cabe destacar la utilización de listas de mensajería, la gestión de acuses de recibo y el reenvío de mensajes. El protocolo SMTP no especifica cómo se crean los mensajes, para este fin se necesita un programa de correo electrónico nativo o un editor local. Una vez que se ha creado el mensaje, SMTP lo acepta y hace uso del TCP para enviarlo al módulo SMTP en el computador remoto. En el receptor, el módulo SMTP utilizará su aplicación de correo electrónico local para almacenar el mensaje recibido en el buzón de correo del usuario destino.

El **protocolo de transferencia de ficheros (FTP, File Transfer Protocol)** se utiliza para enviar ficheros de un sistema a otro bajo el control del usuario. Se permite transmitir ficheros tanto de texto



BGP = Protocolo de pasarela frontera
FTP = Protocolo de transferencia de ficheros
HTTP = Protocolo para la transferencia de hipertextos
ICMP = Protocolo de mensajes de control en Internet
IP = Protocolo Internet
MIME = Extesiones multipropósito de correo electrónico en Internet
OSPF = Protocolo abierto del primer camino más corto
RSVP = Protocolo de reserva de recursos
SMTP = Protocolo sencillo de transferencia de correo electrónico
SNMP = Protocolo sencillo de gestión de redes
TCP = Protocolo de control de transmisión
UDP = Protocolo de datagramas de usuario

Figura 2.12. Algunos protocolos en la familia de protocolos TCP/IP.

como en binario, además el protocolo permite controlar el acceso de los usuarios. Cuando un usuario solicita la transferencia de un fichero, el FTP establece una conexión TCP con el sistema destino para intercambiar mensajes de control. Esta conexión permite al usuario transmitir su identificador y contraseña, además de la identificación del fichero junto con las acciones a realizar sobre el mismo. Una vez que el fichero se haya especificado y su transferencia haya sido aceptada, se establecerá una segunda conexión TCP a través de la cual se materializará la transferencia. El fichero se transmite a través de la segunda conexión, sin necesidad de enviar información extra, o cabeceras generadas por la capa de aplicación. Cuando la transferencia finaliza, se utiliza la conexión de control para indicar el fin, además esta misma conexión estará disponible para aceptar nuevas órdenes de transferencia.

TELNET facilita la posibilidad de conexión remota, mediante la cual el usuario en un terminal o computador personal se conecta a un computador remoto y trabaja como si estuviera conectado directamente a ese computador. El protocolo se diseñó para trabajar con terminales poco sofisticados en modo *scroll (avance de pantalla)*. En realidad, TELNET se implementa en dos módulos: el usuario TELNET interactúa con el módulo de E/S para comunicarse con terminal local. Éste convierte las particularidades de los terminales reales a una definición normalizada de terminal de red, y viceversa. El servidor TELNET interactúa con la aplicación, actuando como un sustituto del gestor del terminal, para que de esta forma el terminal remoto le parezca local a la aplicación. El tráfico entre el terminal del usuario y el servidor TELNET se transmite sobre una conexión TCP.

2.4. LECTURAS RECOMENDADAS

Para el lector que tenga interés en conocer con mayor detalle el TCP/IP, existen dos trabajos de tres volúmenes que son más que adecuados. El trabajo de Comer y Stevens ha llegado a ser un clásico y se considera definitivo [COME99, COME97, COME95]. El trabajo de Stevens y Wright es también destacable, en él se presenta más detalles en lo referente al funcionamiento de los protocolos [STEV94, STEV96, WRIG95]. Un trabajo más compacto y muy útil es [MURP98], en el que se estudia el abanico

de protocolos relacionados con TCP/IP de una forma técnicamente concisa y a la vez completa, se incluyen el estudio de algunos protocolos que no se consideran en los otros dos trabajos.

Uno de los mejores textos sobre OSI y sobre protocolos relacionados es [JAIN93]. [HALS96] también proporciona un tratamiento completo.

COME99 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume II: Design Implementation, and Internals.* Upper Saddle River, NJ: Prentice Hall, 1999.

COME97 Comer, D., y Stevens, D. *Internetworking with TCP/IP, Volume III: Client-Server Programming and Applications.* Upper Saddle River, NJ: Prentice Hall, 1997.

COME95 Comer D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 1995.

HALS96 Halsall, F. *Data Communications, Computer Networks, and Open Systems.* Reading. MA: Addison-Wesley, 1996.

JAIN93 Jain, B., and Agrawala, A. *Open Systems Interconnection.* New York: McGraw-Hill, 1993.

MURH98 Murhammer, M., *et al. TCP/IP: Tutorial and Technical Overview.* Upper Saddle River: NJ: Prentice Hall, 1998.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

STEV96 Stevens, W. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX(R) Domain Protocol.* Reading, MA: Addison-Wesley, 1996.

WRIG95 Wright, G., y Stevens, W. *TCP/IP Illustrated, Volume* 2: *The Implementation.* Reading, MA: Addison-Wesley, 1995.

2.5. PROBLEMAS

2.1. Dos cuerpos de ejército (de color azul), situados sobre dos colinas, están preparando un ataque a un único ejército (de color rojo) situado en el valle que las separa. El ejército rojo puede vencer por separado a cada cuerpo del ejército azul pero fracasará si los dos ejércitos azules atacan simultáneamente. Los cuerpos de ejército azules se comunican mediante un sistema de comunicación no seguro (un soldado de infantería). El comandante de uno de los cuerpos de ejército azul, desearía atacar al mediodía. Su problema es éste: si envía un mensaje ordenando el ataque, no puede estar seguro de que el mensaje haya llegado. Podría solicitar una confirmación pero ésta también podría ser interceptada. ¿Existe algún protocolo que pueda utilizar el ejército azul para evitar la derrota?

2.2. Enumere las desventajas del diseño en capas para los protocolos.

2.3. Usando los modelos de capas de la Figura 2.13, describa el procedimiento de pedir y enviar una pizza, indicando las interacciones habidas en cada nivel.

2.4. **a)** Los primeros ministros de China y Francia necesitan alcanzar un acuerdo por teléfono, pero ninguno de los dos habla el idioma de su interlocutor. Es más, ninguno tiene cerca un traductor que traduzca el idioma del otro. No obstante, ambos tienen un traductor de inglés. Dibuje un diagrama similar al de la Figura 2.13 que describa la situación, y describa la interacciones que haya en cada nivel.

b) Suponga ahora que el traductor del primer ministro chino puede traducir sólo al japonés y que el primer ministro francés tiene un traductor alemán. Dibuje el diagrama que refleje esta nueva situación y describa la hipotética conversación telefónica.

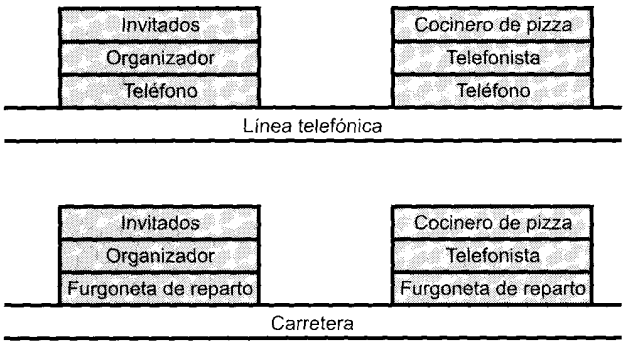


Figura 2.13. Arquitectura para el Problema 2.3.

2.5. Basándose en los principios enunciados en la Tabla 2.2, diseñe una arquitectura con ocho capas y ponga un ejemplo de su utilización. Diseñe otra con seis capas y de otro ejemplo para ésta.

2.6. Discuta si es necesaria o no una capa de red (capa 3 de OSI) en una red de difusión.

2.7. En la Figura 2.11 la unidad de datos del protocolo (PDU) de la capa N se encapsula en una PDU de la capa $(N - 1)$. Igualmente, se puede partir la PDU del nivel N en varias PDU del nivel $(N - 1)$ (segmentación), o agrupar varias PDU del nivel N en una única PDU del nivel $(N - 1)$ (agrupamiento).

a) En la segmentación, ¿es necesario que cada segmento del nivel $(N - 1)$ contenga una copia de la cabecera del nivel N?

b) En el agrupamiento, ¿es necesario que cada una de las PDU conserve su cabecera o se pueden agrupar los datos en una única PDU de nivel N con una única cabecera de nivel N?

PARTE II

COMUNICACIONES DE DATOS

CUESTIONES DE LA PARTE II

La Parte II trata sobre la transferencia de datos entre dos dispositivos que están directamente conectados; es decir, dos dispositivos que están enlazados por medio de un único camino, y no por una red. Incluso para este contexto tan restringido hay una cantidad considerable de cuestiones técnicas y de diseño que hay que analizar. En primer lugar, de alguna manera se tiene que entender bien el procedimiento para transmitir señales a través de un enlace de comunicación. Para tal fin, se utilizan técnicas analógicas y digitales. En ambos casos, la señal se puede describir como un conjunto de componentes que barren un rango de frecuencias electromagnéticas. Las propiedades de transmisión de la señal dependerán de las frecuencias que estén involucradas. Igualmente, los defectos y limitaciones que sufre la señal en la transmisión, como, por ejemplo, la atenuación, son dependientes de la frecuencia. Un aspecto independiente es el propio medio que se utilice para la transmisión de la señal, el cual será factor determinante de las prestaciones que se puedan conseguir, en términos de velocidad de transmisión y distancia. Íntimamente relacionado con las señales y los medios de transmisión está el problema de cómo codificar los datos en las señales a transmitir. Las técnicas de codificación son igualmente un factor que influirá en las prestaciones del sistema de transmisión.

Además de los conceptos fundamentales de la señal, el medio y la codificación, la Parte II estudia otros dos aspectos importantes en las comunicaciones de datos: la fiabilidad y la eficacia. En todo esquema de comunicaciones, durante la transmisión siempre habrá una tasa determinada de errores. Un protocolo para el control del enlace de datos proporcionará mecanismos para la detección y recuperación de los errores, de tal manera que una línea que no sea fiable se convertirá en un enlace de datos fiable. Finalmente, si la capacidad del enlace es superior a los requisitos de una transmisión típica, en aras a proporcionar un uso eficaz del medio de transmisión es necesario la utilización de varias técnicas de multiplexación.

ESQUEMA DE LA PARTE II

CAPÍTULO 3. TRANSMISIÓN DE DATOS

Los principios generales que rigen la transmisión de datos están siempre subyacentes en todos los conceptos y técnicas que se presentan en el libro. Para comprender la necesidad de la codificación, la mul-

tiplexación, la conmutación, el control de errores, y otros, el lector debería comprender previamente el comportamiento de la propagación de las señales a través de los medios de transmisión. En el Capítulo 3 se discuten las diferencias entre datos analógicos o digitales y entre transmisión analógica o digital. En este capítulo también se estudian los conceptos de atenuación y ruido.

CAPÍTULO 4. MEDIOS DE TRANSMISIÓN

Los medios de transmisión se pueden clasificar en guiados o inalámbricos. Los medios guiados más utilizados son el par trenzado, el cable coaxial y la fibra óptica. Entre las técnicas inalámbricas cabe destacar las microondas terrestres y vía satélite, la radiodifusión, y los infrarrojos. En el Capítulo 4 se estudian todos estos conceptos.

CAPÍTULO 5. CODIFICACIÓN DE DATOS

Los datos pueden ser analógicos (continuos) o digitales (discretos). Para su transmisión, se deben codificar mediante señales eléctricas de características acordes con el medio de transmisión. Tanto los datos analógicos como digitales se pueden representar mediante señales analógicas o digitales; en el Capítulo 5 se estudian cada una de las cuatro posibilidades. Además se estudian también las técnicas de espectro expandido.

CAPÍTULO 6. LA INTERFAZ PARA LA COMUNICACIÓN DE DATOS

En el Capítulo 6, el interés se desplaza de la transmisión a la comunicación de datos. Para que dos dispositivos que están conectados mediante un medio de transmisión puedan intercambiar datos digitales, se exige un alto grado de cooperación. Típicamente, los datos se transmiten bit a bit. La temporización (la velocidad, la duración y la separación) de estos bits debe ser común en el transmisor y en el receptor. Se exploran dos técnicas habituales en la transmisión: asíncrona y síncrona. Este capítulo también analiza las interfaces con la línea de transmisión. Normalmente, los dispositivos de datos digitales no se conectan y se transmite directamente al medio. En su lugar, este proceso se lleva a cabo mediante la intervención de una interfaz normalizada.

CAPÍTULO 7. CONTROL DEL ENLACE DE DATOS

El intercambio cooperativo de datos digitales entre dos dispositivos exige algún mecanismo para el control del enlace de datos. El Capítulo 7 estudia las técnicas fundamentales comunes a todos los protocolos para el control del enlace de datos, incluyendo el control del flujo, la detección y corrección de errores, posteriormente se considera el protocolo más utilizado: HDLC.

CAPÍTULO 8. MULTIPLEXACIÓN

Las facilidades y servicios de transmisión son caros. Es habitual que dos estaciones que se vayan a comunicar no utilicen toda la capacidad del enlace de datos. Por cuestiones de rendimiento, es conveniente compartir esa capacidad. El término genérico que alude a esa compartición es la *multiplexación*.

El Capítulo 8 se centra en las tres técnicas más habituales de multiplexación. En primer lugar se estudia la multiplexación más utilizada, la división en frecuencias (FDM, Frecuency Division Multiplexing), familiar para cualquiera que haya utilizado la radio o la televisión. La segunda técnica es un caso particular de multiplexación por división en el tiempo (TDM, Time Division Multiplexing) habitualmente denominada TDM asíncrona. Esta técnica es habitual para la multiplexación de secuencias de voz digitalizada. El tercer tipo es otro caso particular de TDM, más compleja que la anterior pero potencialmente más eficaz, denominada TDM estadística o asíncrona.

CAPÍTULO 3

Transmisión de datos

- Todos los formatos de información considerados en este texto (voz, datos, imágenes, vídeo) se pueden representar mediante señales electromagnéticas. Dependiendo del medio de transmisión y del entorno donde se realicen las comunicaciones, se pueden utilizar señales analógicas o digitales para transportar la información.
- Cualquier señal electromagnética, analógica o digital, está conformada por una serie de frecuencias constituyentes. Un parámetro clave en la caracterización de la señal es el ancho de banda, definido como el rango de frecuencias contenidas en la señal. En términos generales, cuanto mayor es el ancho de banda de la señal, mayor es su capacidad de transportar información.
- Uno de los problemas principales en el diseño de un sistema de comunicaciones reside en las dificultades o defectos de las líneas de transmisión. Las dificultades más importantes a superar son la atenuación, la distorsión de atenuación, la distorsión de retardo, así como los distintos tipos de ruido. Entre otros, el ruido puede ser de tipo térmico, ruido de intermodulación, diafonía e impulsivo. Las dificultades en la transmisión usando señales analógicas causan efectos aleatorios que degradan la calidad de la información recibida y pueden afectar a la inteligibilidad. Cuando se utilizan señales digitales, los defectos en la transmisión pueden introducir bits erróneos en la recepción.
- El diseñador de un sistema de comunicaciones debe tener presente cuatro factores determinantes: el ancho de banda de la señal, la velocidad de transmisión de la información digital, la cantidad de ruido junto a otros defectos en la transmisión, y por último la proporción o tasa de errores tolerable. El ancho de banda disponible está limitado por el medio de transmisión así como por la necesidad de evitar interferencias con señales cercanas. Debido a que el ancho de banda es un recurso escaso, es conveniente maximizar la velocidad de transmisión de los datos para el ancho de banda disponible. La velocidad de transmisión está limitada por el ancho de banda, la presencia ineludible de defectos en la transmisión, como, por ejemplo, el ruido, y finalmente por la tasa de errores que sea tolerable como máximo.

El éxito en la transmisión de datos depende fundamentalmente de dos factores: la calidad de la señal que se transmite y las características del medio de transmisión. El objetivo de este capítulo es proporcionar al lector un conocimiento intuitivo de la naturaleza de estos dos factores.

La primera sección introduce algunos conceptos y terminología comúnmente aceptada en el campo de la ingeniería eléctrica, proporcionando una base suficiente para abordar el resto del capítulo. La Sección 3.2 clarifica el uso de los conceptos *analógico* y *digital*. Tanto los datos analógicos como los digitales se pueden transmitir usando señales analógicas o digitales. Es más, esto es ampliable al procesamiento intermedio que se haga entre la fuente y el destino, pudiendo ser de nuevo analógico o digital.

En la Sección 3.3 se estudian los defectos en la transmisión que pueden introducir errores en los datos. Dichos errores son fundamentalmente: la atenuación, el retardo, y los diversos tipos de ruido existentes. Por último, se estudia el concepto fundamental de capacidad del canal.

3.1. CONCEPTOS Y TERMINOLOGÍA

En esta sección se introducen algunos conceptos y términos que se utilizarán a lo largo del capítulo, y de hecho en toda la Parte II.

TERMINOLOGÍA UTILIZADA EN TRANSMISIÓN DE DATOS

La transmisión de datos entre un emisor y un receptor siempre se realiza a través de un medio de transmisión. Los medios de transmisión se pueden clasificar como guiados y no guiados. En ambos casos, la comunicación se realiza con ondas electromagnéticas. En los **medios guiados**, como, por ejemplo, en los pares trenzados, los cables coaxiales y las fibras ópticas, las ondas se transmiten confinándolas a lo largo del camino físico. Por el contrario, los medios **no guiados** proporcionan una forma de transmitir las ondas electromagnéticas sin confinarlas, como, por ejemplo, en la propagación a través del aire, el mar o el vacío.

El término **enlace directo** hace referencia al camino de transmisión entre dos dispositivos en el que la señal se propaga directamente del emisor al receptor sin ningún otro dispositivo intermedio que no sea un amplificador o repetidor. Estos últimos se usan para incrementar la energía de la señal. Obsérvese que este término se puede aplicar tanto a medios guiados como no guiados.

Un medio de transmisión guiado es **punto a punto** si proporciona un enlace directo entre los dos únicos dispositivos que comparten el medio. En una configuración guiada **multipunto**, el mismo medio es compartido por más de dos dispositivos. Por ejemplo, en la Figura 3.1, el enlace entre los dos nodos de conmutación de la parte superior de la figura son punto a punto; el enlace que une a las estaciones de trabajo conectadas usando una LAN según se muestra en la parte inferior de la figura es un enlace multipunto.

Un medio de transmisión puede ser simplex, half-duplex o full-duplex. En la transmisión simplex, las señales se transmiten sólo en una única dirección; siendo una estación la emisora y otra la receptora. En half-duplex, ambas estaciones pueden transmitir pero no simultáneamente. En full-duplex, ambas estaciones pueden igualmente transmitir, pero ahora simultáneamente. En este último caso, el medio transporta señales en ambos sentidos al mismo tiempo. Posteriormente se explicará cómo se realiza este tipo de transmisión. Nótese que estas definiciones son de uso común en los Estados Unidos (son definiciones ANSI). En otros lugares (donde prevalecen las definiciones UIT-T) el término «*simplex*» corresponde a «half-duplex», tal y como se ha definido antes, y «*duplex*» se usa por lo que se entiende como «full-duplex» en ANSI.

FRECUENCIA, ESPECTRO Y ANCHO DE BANDA

En este libro, consideraremos las señales electromagnéticas desde el punto de vista de la transmisión de datos. En el punto 3 de la Figura 1.2 se genera una señal en el transmisor que se envía a través del medio. La señal, que es una función del tiempo, se puede expresar también en función de la frecuencia; es decir, la señal está constituida por componentes a diferentes frecuencias. Para comprender y caracterizar mejor el funcionamiento de la transmisión de datos, el *dominio de la frecuencia* resulta ser más ilustrativo que *el dominio del tiempo*. A continuación, se introducen ambos dominios.

Conceptos en el dominio temporal

La señal electromagnética considerada como función del tiempo, puede ser tanto continua como discreta. Una **señal continua** es aquella en la que la intensidad de la señal varía suavemente en el tiempo. Es decir, no se presentan saltos o discontinuidades[1]. Una **señal discreta** es aquella en la que la intensidad se mantiene constante durante un determinado intervalo de tiempo, tras el cual la señal cambia a otro valor constante. En la Figura 3.1 se muestran ejemplos de ambos tipos de señales. La señal continua puede corresponder a voz y la señal discreta puede representar valores binarios (0 y 1).

[1] La definición matemática es: una señal $s(t)$ es continua si $\lim_{t \to a} s(t) = s(a)$ para todo a.

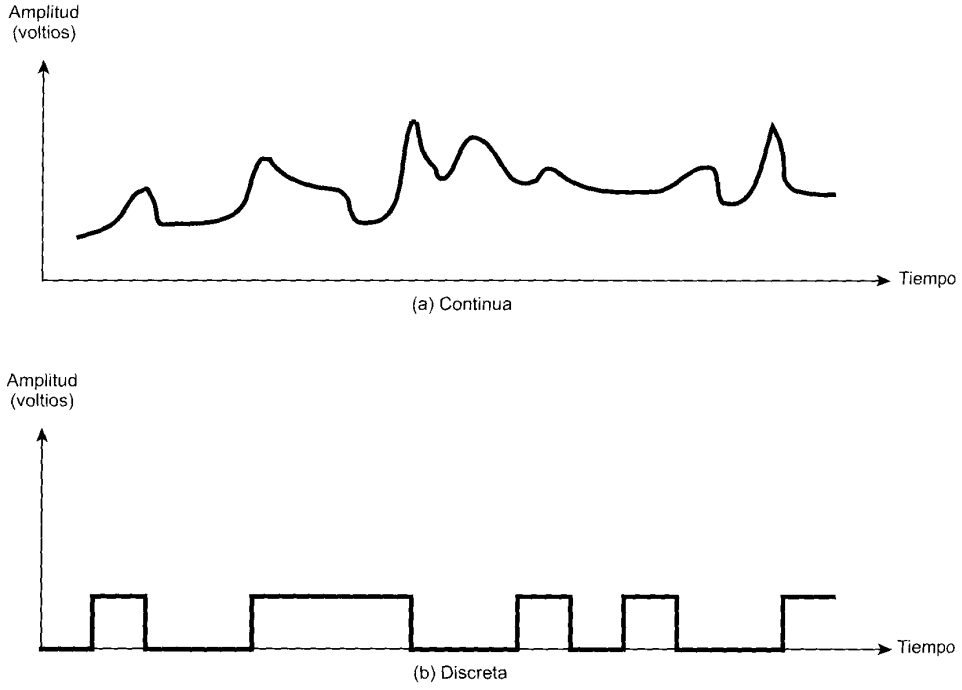


Figura 3.1. Señales continua y discreta.

El tipo de señales más sencillas que se pueden considerar son las **señales periódicas**, que se caracterizan por contener un patrón que se repite a lo largo del tiempo. En la Figura 3.2 se muestra un ejemplo de señal periódica continua (una onda sinusoidal) y un ejemplo de señal periódica digital (una onda cuadrada). Matemáticamente, una señal $s(t)$ se dice periódica si y solamente si

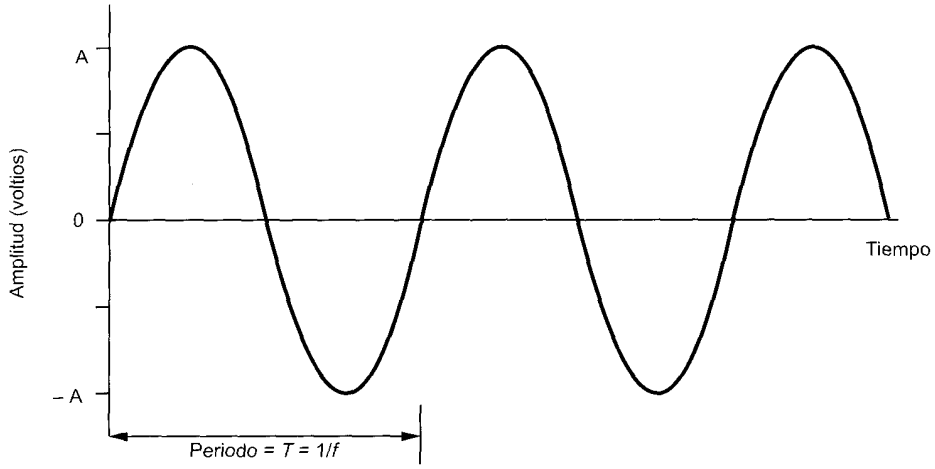
$$s(t + T) = s(t) \qquad -\infty < t < +\infty$$

donde la constante T es el periodo de la señal (T debe ser el menor valor que verifique la ecuación). En cualquier otro caso la señal es **no periódica**.

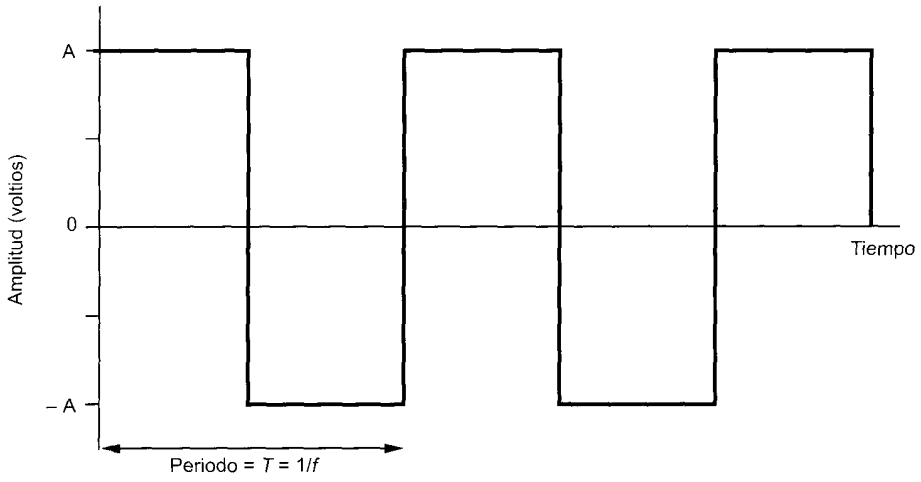
La onda seno es la señal continua fundamental por excelencia. Cualquier onda seno se representa mediante tres parámetros: la amplitud (A), la frecuencia (f) y la fase (ϕ). La **amplitud de pico** es el valor máximo (o energía) de la señal en el tiempo; normalmente este valor se mide en voltios. La **frecuencia** es la razón [en ciclos por segundo o Hertzios (Hz)] a la que la señal se repite. Un parámetro equivalente es el **periodo** (T), definido como la cantidad de tiempo transcurrido entre dos repeticiones consecutivas de la señal; por tanto, $T = 1/f$. La **fase** es una medida de la posición relativa de la señal dentro de un periodo de la misma; este concepto se ilustra más adelante. Más formalmente, para una señal periódica $f(t)$, la fase es la fracción t/P del periodo P, en la que t ha avanzado respecto un origen arbitrario. El origen se considera normalmente como el último cruce por cero desde valores negativos a positivos.

La expresión general para una onda sinusoidal es:

$$s(t) = A \operatorname{sen}(2\pi f t + \phi)$$



(a) Onda sinusoidal



(b) Onda cuadrada

Figura 3.2. Señales periódicas.

En la Figura 3.3 se muestra el efecto de la variación de cada uno de los tres parámetros antes mencionados. En la parte (a), la frecuencia es 1 Hz, por tanto el periodo es $T = 1$ segundo. En la Figura 3.3(b) se representa una onda seno con la misma fase y frecuencia pero con una amplitud de 1/2. En la Figura 3.3(c) se tiene una señal con frecuencia $f = 2$, lo cual es equivalente a considerar un periodo $T = 1/2$. Por último, en la parte (d) de la misma figura se muestra el efecto de un desplazamiento en fase de $\pi/4$ radianes, que corresponde a 45 grados (2π radianes = 360° = 1 periodo).

En la Figura 3.3 el tiempo se representa en el eje horizontal; la curva representa el valor de la señal para un punto del espacio dado, en función del tiempo. Este tipo de representación, con un cambio adicional de escala, se puede usar representando en el eje horizontal el espacio. En este caso, la curva muestra el valor de la señal para un instante de tiempo dado en función de la distancia. Por ejemplo,

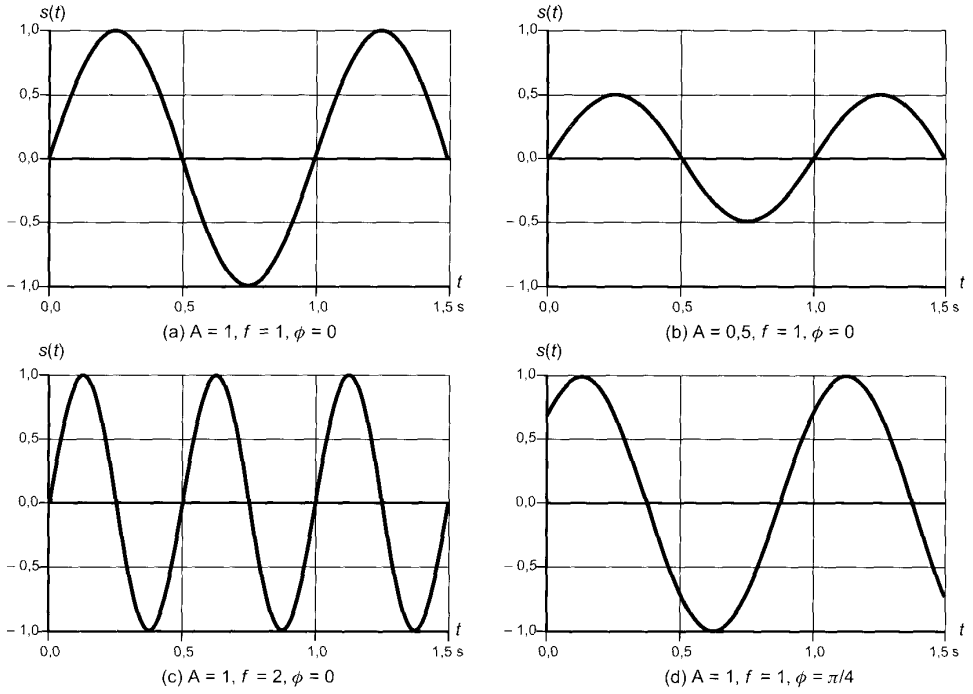


Figura 3.3. $s(t) = A \operatorname{sen}(2\pi ft + \phi)$.

para la transmisión de una señal sinusoidal (digamos una onda electromagnética de radio-frecuencia alejada una cierta distancia de la antena, o un sonido alejado a cierta distancia del altavoz), en un instante determinado de tiempo, la intensidad de la señal varía sinusoidalmente en función de la distancia media desde la fuente.

Es obvio que existe una relación sencilla entre las dos señales seno anteriores (en el tiempo y en el espacio). Para una señal, se define la **longitud de onda** λ como la distancia que ocupa un ciclo, en otras palabras, la distancia entre dos puntos de igual fase en dos ciclos consecutivos. Supóngase que la señal se propaga a una velocidad v. En ese caso, la longitud de onda se puede relacionar con el periodo de la señal a través de la siguiente expresión: $\lambda = vT$. O equivalentemente $\lambda f = v$. Es frecuente el caso en que $v = c$; es decir, cuando la velocidad de propagación en el medio es igual a la de la luz en el espacio libre, que como es sabido es $c = 3 \times 10^8$ m/s.

Conceptos del dominio de la frecuencia

En la práctica, la señal electromagnética puede estar compuesta de muchas frecuencias, por ejemplo, en la Figura 3.4c se muestra la siguiente señal

$$s(t) = (4/\pi) \times (\operatorname{sen}(2\pi ft) + (1/3)\operatorname{sen}(2\pi(3f)t))$$

en este ejemplo la señal está compuesta por dos términos correspondientes a las frecuencias f y $3f$; dichas componentes se muestran en las partes (a) y (b) de la mencionada figura. Hay varias consideraciones interesantes que se pueden hacer a la vista de estas figuras:

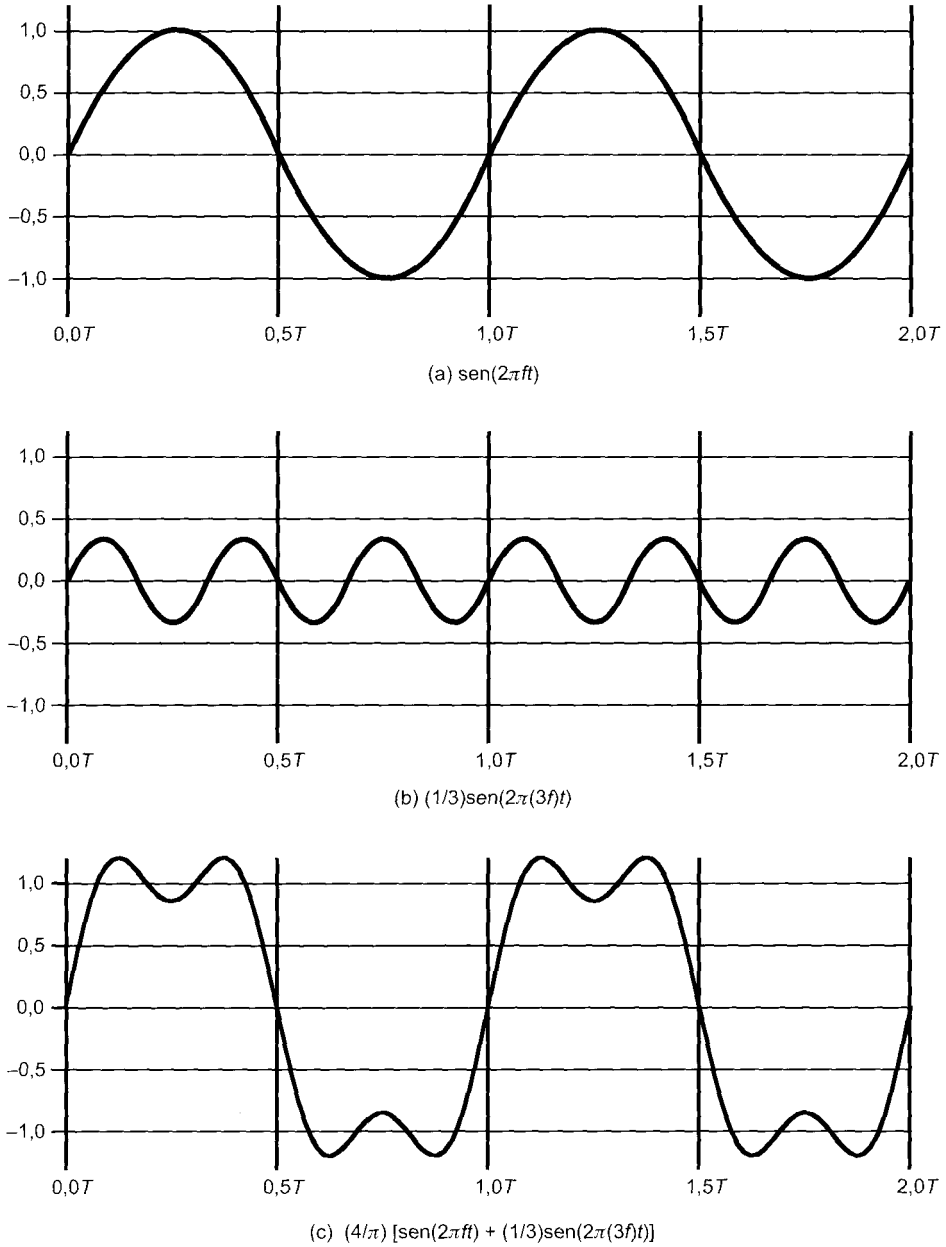


Figura 3.4. Suma de componentes en frecuencia ($T = 1/f$).

- La frecuencia de la segunda componente es un múltiplo entero de la frecuencia de la primera. Cuando todas las componentes de una señal tienen frecuencias múltiplo de una dada, ésta se denomina **frecuencia fundamental**.

- El periodo de la señal suma de componentes es el periodo correspondiente a la frecuencia fundamental. El periodo de la componente ($2\pi ft$) es $T = 1/f$, y el periodo de $s(t)$ es también T, como se puede observar en la Figura 3.4c.

Se puede demostrar, usando el análisis de Fourier, que cualquier señal está constituida por componentes sinusoidales de distintas frecuencias. Este resultado es de vital importancia, ya que los efectos de los medios de transmisión sobre las señales se pueden expresar en el dominio de la frecuencia, como se discutirá posteriormente en este capítulo. Para el lector interesado al final del capítulo, en el Apéndice 3A, se presenta una introducción al análisis de Fourier.

Por lo tanto, para cada señal se puede decir que hay una función en el dominio del tiempo $s(t)$ que determina la amplitud de la señal en cada instante de tiempo. Igualmente, hay una función $S(f)$ en el dominio de la frecuencia que especifica las frecuencias constitutivas de la señal. En la Figura 3.5a se

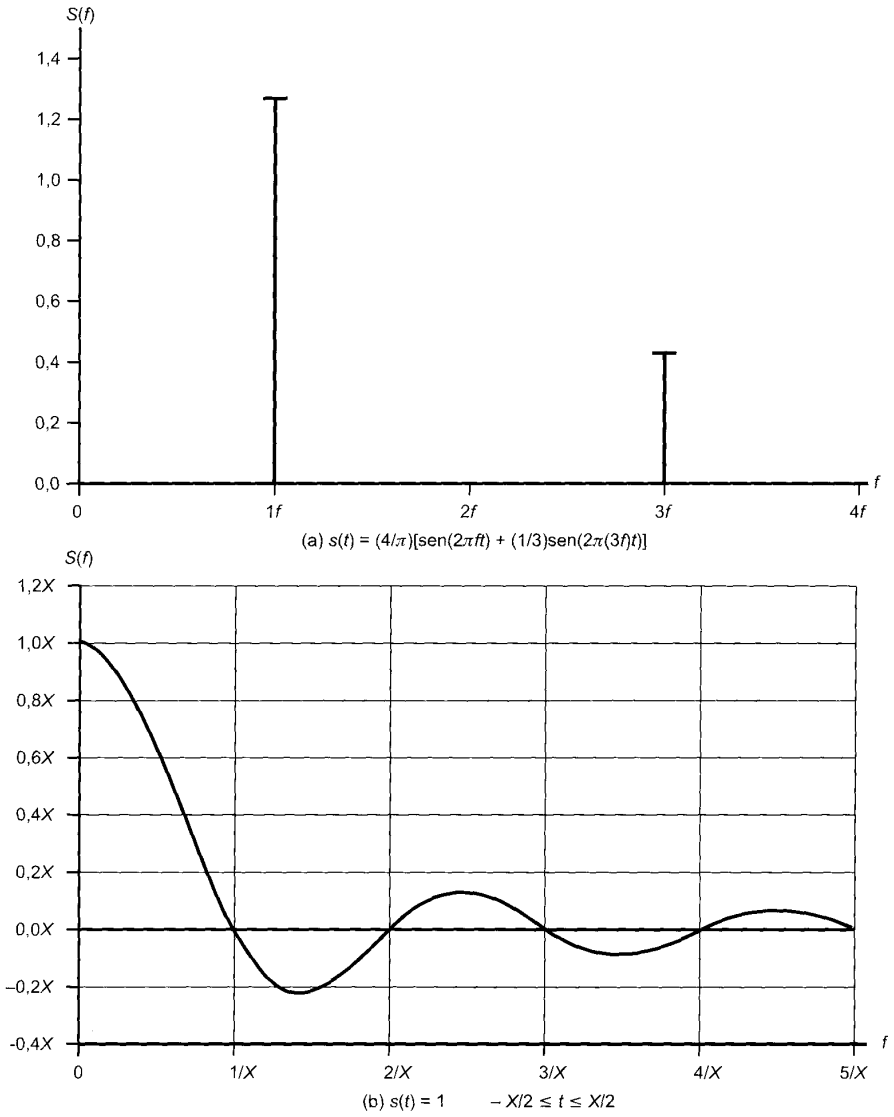
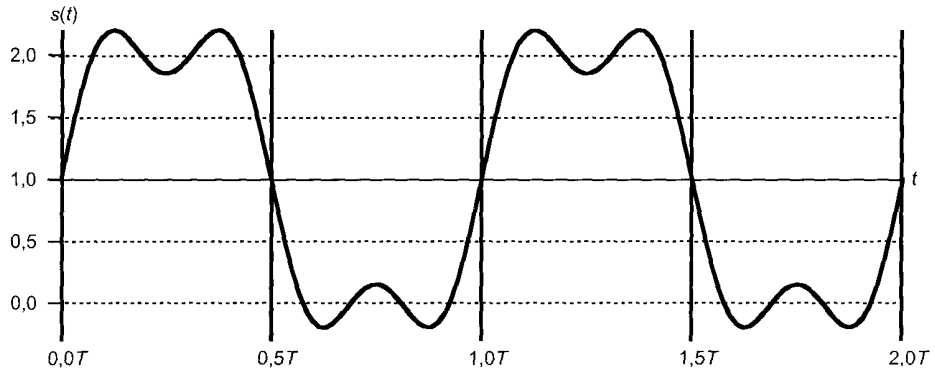


Figura 3.5. Representaciones en el dominio de la frecuencia.

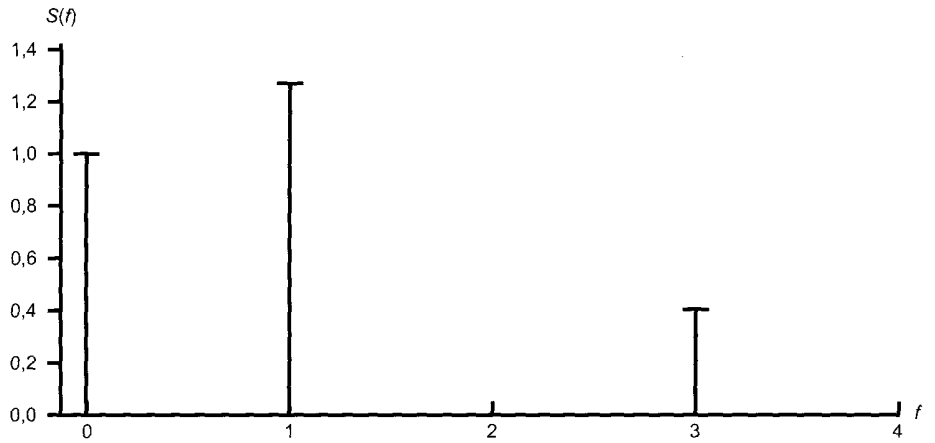
muestra la señal de la Figura 3.4c en el dominio de la frecuencia. Obsérvese, que en este caso $S(f)$ es discreta. En la Figura 3.5b se muestra la función en el dominio de la frecuencia correspondiente a una señal pulso cuadrado, con valor 1 entre $-X/2$ y $X/2$, y 0 en cualquier otro caso[2]. Obsérvese que en este caso $S(f)$ es continua y tiene valores distintos de cero indefinidamente, aunque la magnitud de las frecuencias se hace pequeña para frecuencias f grandes. Estas características son comunes en las señales reales.

Se define el **espectro** de una señal como el conjunto de frecuencias que la constituyen. Para la señal de la Figura 3.4c, el espectro se extiende desde f a $3f$. Se define el **ancho de banda absoluto** de una señal como la anchura del espectro. En el caso de la Figura 3.4c el ancho de banda absoluto es $2f$. Muchas señales, como la de la Figura 3.5b, tienen un ancho de banda infinito. No obstante, la mayor parte de la energía de la señal se concentra en una banda de frecuencias relativamente estrecha. Esta banda se **denomina ancho de banda efectivo** o simplemente *ancho de banda*.

Para concluir definiremos el término **componente continua (dc)**. Si una señal contiene una componente de frecuencia cero, esa componente se denomina continua (dc, direct current). Por ejemplo, en la Figura 3.6 se muestra el resultado de sumarle una componente continua a la señal de la Figura 3.4c. Sin



(a) $s(t) = 1 + (4/\pi)[\text{sen}(2\pi ft) + (1/3)\text{sen}(2\pi(3f)t)]$



(b) $S(f)$

Figura 3.6. Señal con componente continua (dc).

[2] De hecho, la función $S(f)$ en este ejemplo es simétrica respecto $f = 0$, y por tanto, está definida para valores negativos de la frecuencia. La existencia de frecuencias negativas es un artificio matemático cuya justificación cae fuera del propósito de este libro.

componente continua, la señal tiene una amplitud media igual a cero, vista en el dominio del tiempo. Si tiene componente continua, tendrá un término a frecuencia $f = 0$, y por tanto, una amplitud promedio distinta de cero.

Relación entre la velocidad de transmisión y el ancho de banda

Se ha definido el ancho de banda efectivo como la banda en la que se concentra la mayor parte de la energía de la señal. *La mayor parte* es un concepto algo impreciso. La cuestión importante aquí, es que aunque una forma de onda dada contenga frecuencias en un rango extenso, por cuestiones prácticas, el sistema de transmisión (transmisor más medio más receptor) sólo podrá transferir una banda limitada de frecuencias. Esto hace que la velocidad de transmisión máxima en el medio sea limitada.

Para explicar esta cuestión, consideremos la onda cuadrada de la Figura 3.2b. Supongamos que un 1 binario se representa mediante un pulso positivo y un 0 por un pulso negativo. Por tanto, la forma de onda representa la secuencia binaria 1010... La duración de cada pulso es $1/2f$; luego, la velocidad de transmisión es $2f$ bits por segundo (bps). ¿Cuáles son las componentes en frecuencia de esta señal? Para responder a esta cuestión, consideremos de nuevo la Figura 3.4. Al sumar las ondas seno de frecuencias f y $3f$, se obtiene una forma de onda que empieza a parecerse a una onda cuadrada. Continuemos el proceso sumando otra onda seno con frecuencia $5f$, como se muestra en la Figura 3.7a, y posteriormente sumando otra onda seno de frecuencia $7f$, también mostrado en la Figura 3.7b. Al sumar más términos múltiplos impares de la frecuencia f, convenientemente escalados, iremos aproximando cada vez mejor la onda cuadrada.

De hecho, se puede demostrar que las componentes en frecuencia de una onda cuadrada con amplitudes A y $-A$ se pueden expresar como:

$$s(t) = A \times \frac{4}{\pi} \times \sum_{k \text{ impar}, k=1}^{\infty} \frac{\text{sen}(2\pi k f t)}{k}$$

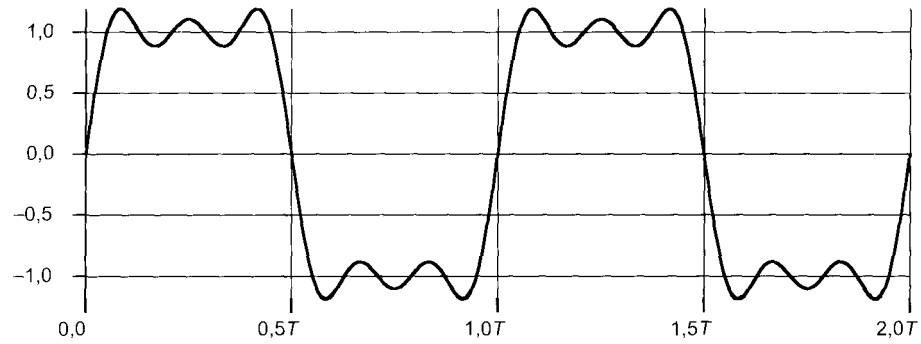
Luego, esta forma de onda tiene un número infinito de componentes en frecuencia y por lo tanto un ancho de banda infinito. Sin embargo, la amplitud de la componente k-ésima, kf, es solamente $1/k$, por tanto, la mayor parte de la energía de esta forma de onda está contenida en las primeras componentes. ¿Qué ocurre si se limita el ancho de banda sólo a las tres primeras componentes? Ya hemos visto la respuesta en la Figura 3.7a. Como se puede ver, la forma de la onda resultante aproxima razonablemente a la onda cuadrada original.

Las Figuras 3.4 y 3.7 pueden servir para ilustrar la relación entre la velocidad de transmisión y el ancho de banda. Supongamos que se está utilizando un sistema de transmisión digital capaz de transmitir señales con un ancho de banda de 4MHz. Intentemos transmitir una secuencia de unos y ceros alternantes, como una onda cuadrada de la Figura 3.7c. ¿Qué velocidad de transmisión se puede conseguir? Para responder a esta pregunta consideremos los siguientes tres casos:

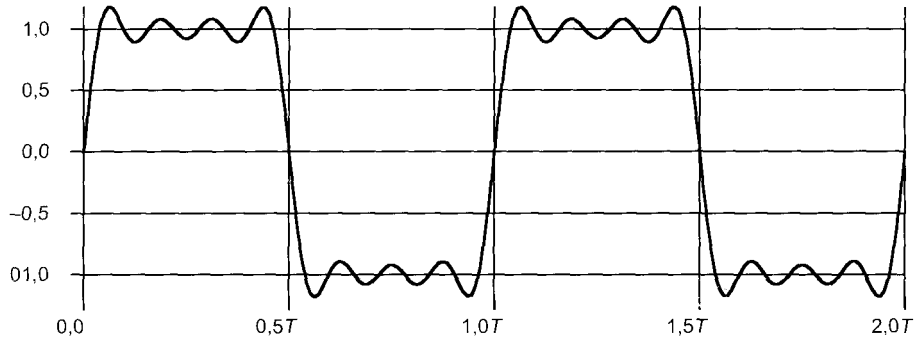
Caso I. Aproximemos la onda cuadrada con una forma de onda como la de la Figura 3.7a. Aunque es una forma de onda «distorsionada», es suficiente para que el receptor sea capaz de discriminar entre un 0 o un 1 binarios. Ahora, si tomamos una $f = 10^6$ ciclos/segundo = 1 MHz, entonces el ancho de banda de la señal

$$s(t) = \frac{4}{\pi} \times \left[\text{sen}((2\pi \times 10^6)t) + \frac{1}{3}\text{sen}((2\pi \times 3 \times 10^6)t) + \frac{1}{5}\text{sen}((2\pi \times 5 \times 10^6)t) \right]$$

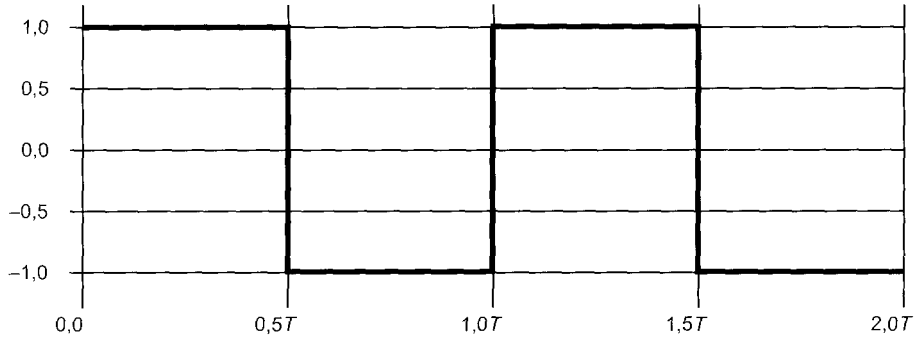
es $(5 \times 10^6) - 10^6 = 4$ MHz. Obsérvese que para $f = 1$ MHz, el periodo de la frecuencia fundamental es $T = 1/10^6 = 10^{-6} = 1$ μs. Luego, si se considera esta forma de onda como una cadena de 0 y 1, un bit aparecerá cada 0,5 μs, para una velocidad de $2 \times 10^6 = 2$ Mbps. Así, para un ancho de banda de 4 MHz, se consigue una velocidad de transmisión de 2 Mbps.



(a) $(4/\pi)$ [sen$(2\pi ft)$ + (1/3)sen$(2\pi(3f)t)$ + (1/5)sen$(2\pi(5f)t)$]



(b) $(4/\pi)$ [sen$(2\pi ft)$ + (1/3)sen$(2\pi(3f)t)$ + (1/5)sen$(2\pi(5f)t)$ + (1/7)sen$(2\pi(7f)t)$]



(c) $(4/\pi) \sum$ (1/k)sen$(2\pi(kf)t)$

Figura 3.7. Componentes en frecuencia de una onda cuadrada ($T = 1/f$).

Caso II. Ahora supongamos que se dispone de un ancho de banda de 8 MHz. Considérese de nuevo la Figura 3.7a, pero ahora con $f = 2$ MHz. Usando un razonamiento idéntico al anterior, el ancho de banda de la señal es $(5 \times 2 \times 10^6) - (2 \times 10^6) = 8$ MHz. Pero en este caso $T = 1/f = 0{,}5$ μs. Por tanto, aparece un bit cada 0,25 μs siendo la velocidad de transmisión en este caso de 4 Mbps. Como conclusión, al duplicar el ancho de banda solamente, se duplica potencialmente la velocidad de transmisión.

Caso III. Ahora supongamos que la forma de onda de la Figura 3.4c se considera adecuada para aproximar una onda cuadrada. Es decir, la diferencia entre un pulso positivo y un pulso

negativo en la Figura 3.4c es suficientemente grande para que la forma de onda pueda representar adecuadamente la secuencia de unos y ceros. Supóngase, como en el caso II, que $f = 2$ MHz y que $T = 1/f = 0{,}5$ μs, de tal manera que aparece un bit cada 0,25 μs siendo la velocidad de transmisión 4 Mbps. Considerando la Figura 3.4c, el ancho de banda de la señal es $(3 \times 2 \times 10^6) - (2 \times 10^6) = 4$ MHz. Por tanto, un ancho de banda dado puede proporcionar varias velocidades de transmisión, dependiendo de la habilidad que exhiba el receptor para distinguir diferencias entre los 1 y 0 en presencia de ruido y otras dificultades en la transmisión.

Resumiendo,

- **Caso I**: Ancho de banda = 4 MHz, velocidad de transmisión = 2 Mbps.
- **Caso II**: Ancho de banda = 8 MHz, velocidad de transmisión = 4 Mbps.
- **Caso III**: Ancho de banda = 4 MHz, velocidad de transmisión = 4 Mbps.

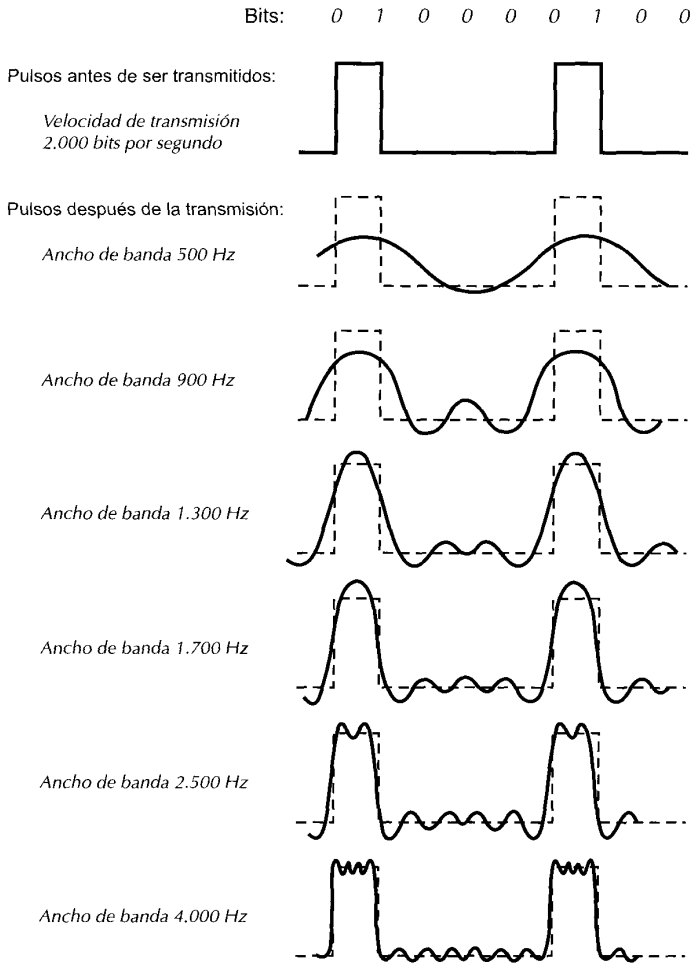


Figura 3.8. Efecto del ancho de banda en las señales digitales.

De las observaciones precedentes, se puede obtener las siguientes conclusiones. En general, cualquier onda digital tendrá un ancho de banda infinito. Si se intenta transmitir esta forma de onda como una señal por cualquier medio, la naturaleza del medio, limitará el ancho de banda que se puede transmitir. Es más, para cualquier medio, cuanto mayor sea el ancho de banda transmitido, mayor será el coste. Luego, por un lado, por razones prácticas y económicas, la información digital se aproxima por una señal de banda limitada. Por otro lado, la limitación del ancho de banda introduce distorsiones, que hacen que la interpretación de la señal recibida sea más difícil. Cuanto mayor es la limitación en el ancho de banda, mayor es la distorsión, y mayor es la posibilidad de que se cometan errores en el receptor.

Una explicación adicional puede servir para reforzar estos conceptos. En la Figura 3.8 se muestra una cadena de bits a una velocidad de transmisión de 2.000 bits por segundo. Con un ancho de banda igual a 2.500 Hz, o incluso 17.000 Hz, la representación es bastante buena. Es más, estos resultados son generalizables de la siguiente manera. Si la velocidad de transmisión de la señal digital es W bps, entonces se puede obtener una representación muy buena con un ancho de banda de $2W$ Hz. No obstante, a menos que el ruido sea muy elevado, la secuencia de bits se puede recuperar con un ancho de banda menor (véase el apartado dedicado a la capacidad del canal en la Sección 3.3).

Por tanto, hay una relación directa entre la velocidad de transmisión y el ancho de banda: cuanto mayor es la velocidad de transmisión de la señal, mayor es el ancho de banda efectivo. Visto de otra manera, cuanto mayor es el ancho de banda de un sistema de transmisión, mayor es la velocidad con la que se pueden transmitir los datos en el sistema.

Otra observación que merece la pena establecerse es la siguiente: si consideramos que el ancho de banda de una señal está centrado sobre una frecuencia dada, denominada **frecuencia central**, cuanto mayor sea dicha frecuencia central mayor es el ancho de banda potencial, y por tanto, mayor puede ser la velocidad de transmisión. Por ejemplo, una señal centrada en torno a 2 MHz, su ancho de banda máximo es de 4 MHz.

Posteriormente, en este capítulo, tras el estudio de las dificultades presentes en la transmisión, en la Sección 3.3 se volverá a la discusión de la relación entre el ancho de banda y la velocidad de transmisión.

3.2. TRANSMISIÓN DE DATOS ANALÓGICOS Y DIGITALES

En la transmisión de datos desde una fuente a un destino, se debe tener en cuenta la naturaleza de los datos, cómo se propagan físicamente dichos datos, y qué procesamiento o ajustes se necesitarán a lo largo del camino para asegurar que los datos que se reciban sean inteligibles. Para todas estas consideraciones, el punto crucial es si se tratan de entidades digitales o analógicas.

Los términos *analógico* y *digital* corresponden, en términos generales a *continuo* y *discreto*, respectivamente. Estos dos términos se aplican con frecuencia en las comunicaciones de datos a:

- Datos.
- Señalización.
- Transmisión.

Se define **dato** como cualquier entidad capaz de transportar información. Las **señales** son representaciones eléctricas o electromagnéticas de los datos. La **señalización** es el hecho de la propagación física de las señales a través de un medio adecuado. Por último, se define **transmisión** como la comunicación de datos mediante la propagación y el procesamiento de señales. En lo que sigue, se intentará clarificar estos conceptos abstractos, considerando las diferencias entre los términos *analógico* y *digital* referidos a datos, señales y a la transmisión.

DATOS

Los conceptos de datos analógicos o digitales son bastante sencillos. Los datos analógicos pueden tomar valores en algún intervalo continuo. Por ejemplo, el vídeo y la voz son valores de intensidad que varían continuamente. La mayoría de los datos que se capturan con sensores, tal como los de temperatura y de presión, son continuos. Los datos digitales toman valores discretos, como, por ejemplo, los textos o los números enteros.

El ejemplo más familiar o cercano de datos analógicos es la señal de **audio**, que en forma de ondas de sonido se puede percibir directamente por los seres humanos. La Figura 3.9 muestra el espectro acústico de la voz humana y de la señal de música. Se pueden encontrar componentes en frecuencia entre 100 Hz y 7 kHz. Aunque la mayor parte de la energía de la voz está concentrada en las frecuencias bajas, experimentalmente se ha demostrado que las frecuencias por debajo de 600 o 700 Hz contribuyen poco a la inteligibilidad de la voz en el oído humano. Una señal de voz típica tiene un rango dinámico aproximadamente de 25 dB[3], es decir, la potencia máxima es del orden de 300 veces superior a la potencia mínima. La Figura 3.9 también muestra el espectro y rango dinámico de la señal de música.

Otro ejemplo típico de datos analógicos es el **vídeo**. En este caso, es más fácil caracterizar los datos en términos del espectador (o destino) de la pantalla de TV que la escena original (o fuente) que se graba en la cámara de TV. Para producir una imagen en la pantalla, un haz de electrones barre la superficie de la pantalla de izquierda a derecha y de arriba a abajo. En la televisión en blanco y negro la luminancia (en una escala del negro a blanco) que se produce en un punto determinado es proporcional a la intensidad del haz cuando pasa por ese punto. Por tanto, en cualquier instante de tiempo el haz toma un valor de intensidad analógico para así producir el brillo deseado en ese punto de la pantalla. Es más, cuando el haz hace el barrido, el valor analógico cambia. Por tanto, la imagen de vídeo se puede considerar como una señal analógica variable en el tiempo.

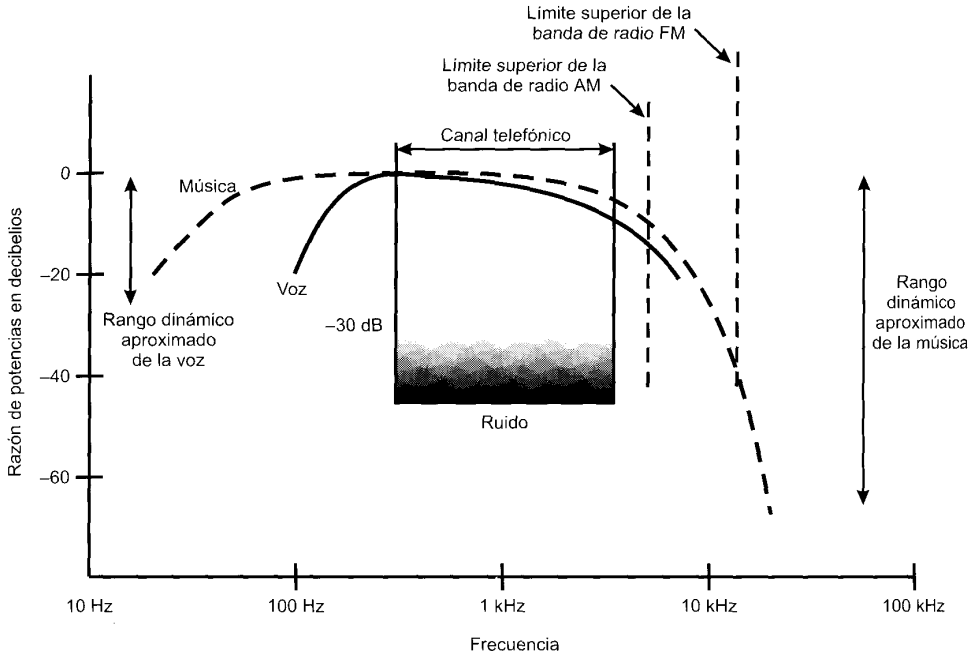
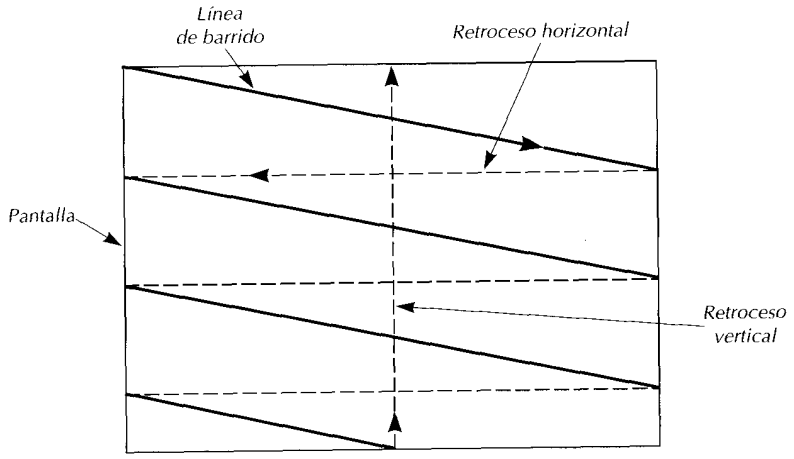


Figura 3.9. Espectro acústico de la voz y música [CARN95].

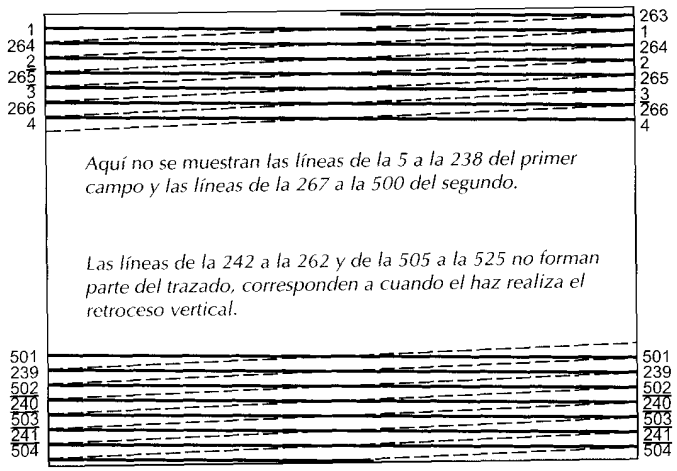
[3] El concepto de decibelio se explicará en el Apéndice 3B.

La Figura 3.10a muestra el proceso de barrido. Al final de cada línea de barrido, el haz se vuelve rápidamente hacia la izquierda (retroceso horizontal). Cuando al haz alcanza la parte más baja, se vuelve rápidamente a la línea superior (retroceso vertical). Obsérvese que el haz se anula durante los retrocesos.

Para conseguir una resolución adecuada, el haz describe un total de 483 líneas horizontales a una velocidad de 30 barridos de pantalla por segundo. Después de diversas pruebas se ha demostrado que esa velocidad produciría una sensación de parpadeo en lugar de movimiento suave como sería deseable. No obstante, el parpadeo se elimina con un proceso de entrelazado, tal y como se muestra en la Figura 3.10b. El haz de electrones barre la pantalla empezando por la izquierda, muy cerca de la línea superior. El haz alcanza la mitad de la línea inferior de la pantalla tras barrer 214,5 líneas. En ese instante, el haz se reposiciona rápidamente a la mitad de la línea superior de la pantalla, volviendo a barrer las restantes 214,5 líneas entrelazadas con las anteriores. Así pues, la pantalla se refresca 60 veces por segundo, en lugar de las 30 anteriores, y con ello se elimina el parpadeo.



(a) Barrido de la pantalla de TV



(b) Técnica de vídeo entrelazado

Figura 3.10. Producción de una imagen de TV.

Las cadenas de caracteres o **textos** son un ejemplo típico de datos digitales. Mientras que los datos en formato de texto son más adecuados para los seres humanos, en general, no se pueden transmitir o almacenar fácilmente (en forma de caracteres) en los sistemas de procesamiento o comunicación. Tales sistemas están diseñados para tratar datos binarios. Para esto se han diseñado un gran número de códigos mediante los cuales los caracteres se representan mediante secuencias de bits. Quizás el ejemplo más antiguo y conocido es el código Morse. En nuestros días, el código más utilizado es el Alfabeto de Referencia Internacional (IRA, International Reference Alphabet)[4], mostrado en la Tabla 3.1. Cada carácter se representa en este código por un patrón único de 7 bits; por lo tanto, se pueden representar 128 caracteres distintos. Esto implica un número mayor del que se necesita, y algunos patrones de entre los 128 se utilizan como *caracteres de control* (Tabla 3.2). Entre estos últimos, algunos están relacionados con el control de la impresión de los caracteres en una página. Otros están relacionados con los procedimientos de comunicación, que serán explicados más adelante. Los caracteres codificados con IRA se

Tabla 3.1. Alfabeto de referencia internacional (IRA, International Reference Alphabet).

Posición del bit				0	0	0	0	1	1	1	1
				0	0	1	1	0	0	1	1
				0	1	0	1	0	1	0	1
b_7	b_6	b_5	b_4	b_3	b_2	b_1					
			0	0	0	0	NUL	DLE	SP	0	@	P		p
			0	0	0	1	SOH	DC1	!	1	A	Q	a	q
			0	0	1	0	STX	DC2	"	2	B	R	b	r
			0	0	1	1	ETX	DC3	#	3	C	S	c	s
			0	1	0	0	EOT	DC4	$	4	D	T	d	t
			0	1	0	1	ENQ	NAK	%	5	E	U	e	u
			0	1	1	0	ACK	SYN	&	6	F	V	f	v
			0	1	1	1	BEL	ETB	'	7	G	W	g	w
			1	0	0	0	BS	CAN	(	8	H	X	h	x
			1	0	0	1	HT	EM	)	9	I	Y	i	y
			1	0	1	0	LF	SUB	*	:	J	Z	j	z
			1	0	1	1	VT	ESC	+	;	K	[	k	{
			1	1	0	0	FF	IS4	,	<	L	\	l	|
			1	1	0	1	CR	IS3	-	=	M	]	m	}
			1	1	1	0	SO	IS2	.	>	N	^	n	~
			1	1	1	1	SI	IS1	/	?	O	_	o	DEL

[4] IRA se define en la Recomendación de la UIT-T T.50, inicialmente se denominó «International Alphabet Number 5» (IA5). La versión del IRA en U.S.A. se denomina «American Standard Code for Information Interchange» (ASCII).

Tabla 3.2. Caracteres de control IRA.

Control de formato

BS (Backspace, «espacio atrás»): indica un movimiento de retroceso en una posición del mecanismo de impresión o del cursor.

HT (Horizontal Tab, «tabulación horizontal»): indica un desplazamiento hacia delante del mecanismo de impresión o del cursor hasta el siguiente tabulador preasignado.

LF (Line Feed, «avance de línea»): indica un desplazamiento del mecanismo de impresión o del cursor hacia el principio de la siguiente línea preasignada.

VT (Vertical Tab, «tabulación vertical»): indica un desplazamiento vertical del mecanismo de impresión o del cursor hasta la siguiente línea preasignada.

FF (Form Feed, «avance de página»): indica un desplazamiento del mecanismo de impresión o del cursor hasta el comienzo de la siguiente página o pantalla.

CR (Carriage Return, «retorno de carro»): indica un desplazamiento del mecanismo de impresión o del cursor hacia la primera posición de la línea actual.

Control de transmisión

SOH (Start of Heading, «comienzo de cabecera»): se utiliza para indicar el comienzo de una cabecera, que puede contener una dirección o información para el encaminamiento.

STX (Start of Text, «comienzo de texto»): se utiliza para indicar el comienzo del texto y para indicar también el final de la cabecera.

ETX (End of Text, «final de texto»): se utiliza para finalizar el texto que empezó con STX.

EOT (End of Transmission, «final de transmisión»): indica el final de la transmisión, en la que se han podido incluir varios «textos» con sus correspondientes cabeceras.

ENQ (Enquiry, «interrogación»): es una solicitud de respuesta emitida por una estación remota. Se puede usar para preguntar «QUIÉN ERES TÚ», formulada por otra estación.

ACK (Acknowledge, «reconocimiento»): es un carácter transmitido por el receptor a modo de confirmación hacia el emisor. Se usa como respuesta afirmativa a los mensajes sondeo.

NAK (Negative Acknowledgement, «reconocimiento negativo»): es un carácter transmitido por el receptor a modo de confirmación negativa hacia el emisor. Se usa como respuesta negativa a los mensajes sondeo.

SYN (Synchronous/Idle, «síncrono/parado»): se utiliza en los sistemas de transmisión síncrona para llevar a cabo la sincronización. Mientras no se envían datos, el sistema de transmisión síncrono puede transmitir continuamente caracteres SYN.

ETB (End of Transmission Block, «final del bloque transmitido»): indica el final de un bloque de datos. Se utiliza para delimitar datos cuando la estructura del bloque no está necesariamente relacionada con el formato de procesamiento.

Separadores de información

IS4 (File Separator, «separador de fichero»).
IS3 (Group Separator, «separador de grupo»).
IS2 (Record Separator, «separador de registro»).
IS1 (United Separator, «separador unido»).

Separadores de información que se usan opcionalmente, teniendo en cuenta que se debe respetar su dependencia jerárquica que va del IS4 (el más genérico) al IS1 (el menos genérico).

Miscelánea

NUL (Null, «nulo»): ausencia de carácter. Se utiliza para rellenar el tiempo o el espacio cuando no hay datos.

BEL (Bell, «pitido»): se utiliza para cuando hay necesidad de llamar la atención del usuario. Puede controlar alarmas u otros dispositivos.

SO (Shift Out, «fuera de código»): indica que los códigos que siguen se deben interpretar como si no pertenecieran al código estándar, hasta que aparezca el carácter SI.

SI (Shif In, «dentro de código»): indica que los códigos que siguen se deban interpretar de acuerdo con el conjunto estándar.

DEL (Delete, «borrar»): se usa para borrar caracteres no deseados, por ejemplo, para sobreescribir.

SP (Space, «espacio»): es un carácter no imprimible que se utiliza para separar palabras o para desplazar el mecanismo de impresión o el cursor una posición hacia adelante.

DLE (Data Link Escape, «salir del enlace de datos»): este carácter cambia el significado de uno o más caracteres contiguos tras su aparición. Puede proporcionar control suplementario o permite enviar datos que correspondan a cualquier combinación de bits.

DC1, DC2, DC3, DC4 (Device Controls, «controles de dispositivo»): caracteres para controlar dispositivos o terminales con características especiales.

CAN (Cancel, «cancelar»): indica que los datos que lo preceden en el mensaje o bloque se deben descartar (normalmente porque se haya detectado un error).

EM (End od Medium, «fin del medio»): indica el final físico de una cinta magnética o cualquier otro medio; o el final de la fracción del medio que se haya solicitado o utilizado.

SUB (Substitute, «sustituir»): sustituido por un carácter que se haya encontrado erróneo o inválido.

ESC (Escape, «salir»): este carácter está dedicado a proporcionar una extensión de código, de tal manera que cambia el significado de un número determinado de caracteres que sigan a continuación.

almacenan o transmiten casi siempre usando 8 bits por carácter (un bloque de 8 bits se denomina octeto o byte). El bit número 8 se utiliza como bit de paridad para la detección de errores. Este bit se elige de forma tal que el número de unos binarios en el octeto sea siempre impar (paridad impar) o siempre par (paridad par). Así pues, se podrán detectar los errores de transmisión que cambien un solo bit.

SEÑALES

En un sistema de comunicaciones, los datos se propagan de un punto a otro mediante señales eléctricas. Una señal analógica es una onda electromagnética que varía continuamente y que, según sea su espectro, puede propagarse a través de una serie de medios; por ejemplo, a través de un medio conductor como un par trenzado, un cable coaxial, un cable de fibra óptica, o a través de la atmósfera o el espacio. Una señal digital es una secuencia de pulsos de tensión que se pueden transmitir a través de un medio conductor; por ejemplo, un nivel de tensión positiva constante puede representar un 1 binario y un nivel de tensión negativa constante puede representar un 0.

A continuación se darán algunos ejemplos específicos de tipos de señales y posteriormente se discutirán las relaciones existentes entre datos y señales.

Ejemplos

Volvamos a los tres ejemplos de la sección anterior. Para cada uno de ellos, se describirá la señal y la estimación de su ancho de banda.

En el caso de datos acústicos (voz), los datos se pueden representar directamente mediante una señal electromagnética que ocupe el mismo espectro. Sin embargo, es necesario establecer un compromiso entre la fidelidad del sonido cuando se vaya a transmitir eléctricamente y el coste de la transmisión, el cual aumentará al aumentar el ancho de banda. Aunque, como ya se ha mencionado, el espectro de la voz está aproximadamente entre 100 Hz y 7 kHz, un ancho de banda mucho más estrecho producirá una calidad aceptable. El espectro estándar para las señales de voz está entre 300 y 3400 Hz. Esta reducción es adecuada para la transmisión de la voz, ya que a la vez se reduce la capacidad de transmisión necesaria y posibilita el uso de teléfonos de coste muy bajo. Así pues, el teléfono transmisor convierte la señal acústica de entrada en una señal electromagnética en el rango de 300 a 3.400 Hz. Esta señal se transmite a través del sistema telefónico al receptor, el cual la reproduce generando un sonido acústico.

Ahora consideremos la señal de vídeo. Para generar la señal de vídeo, se usa una cámara de TV, que en realidad realiza funciones similares a un receptor de TV. Un componente de la cámara es una placa fotosensible, sobre la que se enfoca ópticamente la imagen. Al efectuar el barrido, se genera una señal eléctrica proporcional a la intensidad de la imagen en cada punto particular. Como ya se ha mencionado, se barren 483 líneas a una frecuencias de 30 escenas por segundo. Estos números son aproximados, ya que hay tiempo que se pierde en el retroceso vertical del haz de barrido. El estándar en U.S.A. es de 525 líneas, de las cuales se pierden 42 durante el retroceso vertical. Por tanto, la frecuencia de barrido es (525 líneas) $\times$ (30 barridos/s) = 15.750 líneas por segundo, o lo que es lo mismo 63,5 μs. De estos 63,5 μs, aproximadamente 11 μs están reservados para el retroceso horizontal, quedando pues un total de 52,5 μs por línea de vídeo.

Estamos ya en disposición de estimar el ancho de banda que se necesita para la señal de vídeo. Para hacer esto se deben estimar las frecuencias superior (máxima) e inferior (mínima) de la banda. Utilizaremos el siguiente razonamiento para determinar la frecuencia máxima: dicha frecuencia ocurriría durante el barrido horizontal si la imagen cambiara alternativamente de blanco a negro tan rápido como fuera posible. Se puede estimar el valor máximo considerando la resolución de la imagen de vídeo. En la dimensión vertical, hay 438 líneas, de forma tal que la resolución vertical máxima sería 483. Experimentalmente se ha demostrado que la resolución real subjetiva es alrededor del 70 por ciento de ese número, es decir, 338 líneas. Para conseguir una imagen compensada, las resoluciones vertical y horizontal deberán ser aproximadamente las mismas. La resolución horizontal debería ser $4/3 \times 338 = 450$

líneas, ya que la relación de la anchura de la pantalla de TV respecto a la altura es de 4:3. En el peor de los casos, la línea de barrido consistiría en 450 elementos alternantes de blanco y negro. El barrido resultante sería una onda en la que cada ciclo consistiría en dos niveles de tensión correspondientes al negro (el mayor) y al blanco (el inferior). Por lo tanto habría 450/2 = 255 ciclos de la onda cada 53,5 μs, para una frecuencia máxima de 4,2 MHz. Este razonamiento aproximado, es en realidad bastante preciso. El límite inferior será una frecuencia cero o continua, donde el valor de continua corresponde a la iluminación promedio de la imagen (es decir, el valor promedio en el que la señal supera el nivel de referencia del blanco). Por lo tanto, el ancho de banda de la señal de vídeo es aproximadamente 4 MHz − 0 = 4 MHz.

En la discusión anterior no se han considerado ni las componentes de color ni las de audio. Obsérvese que si se incluyen dichas componentes el ancho de banda sigue siendo aproximadamente 4 MHz.

Finalmente, el tercer ejemplo mencionado anteriormente es un caso de datos binarios digitales. Normalmente para estos datos se usan dos niveles de tensión constante (dc), un nivel para el 1 binario y un nivel para el 0. (En el Capítulo 5, se verá que ésta es una de las posibles alternativas, llamada NRZ.) Lo interesante aquí es el ancho de banda de dicha señal. Éste dependerá de la forma de la onda exacta y de la secuencia de unos y ceros. Para una mejor comprensión, considérese la Figura 3.8 y compárese con la Figura 3.7. Como se puede observar, al aumentar el ancho de banda de la señal, la aproximación a la cadena de pulsos digitales es mejor.

Datos y señales

En la discusión anterior, se han considerado señales analógicas para representar datos analógicos, y señales digitales para representar datos digitales. Generalmente, los datos analógicos son función del tiempo y ocupan un espectro en frecuencias limitado, estos datos se pueden representar mediante una señal electromagnética que ocupe el mismo espectro. Los datos digitales se pueden representar por señales digitales, con un nivel de tensión diferente para cada uno de los dígitos binarios.

Como se muestra en la Figura 3.11, éstas no son las únicas posibilidades. Los datos digitales se pueden también representar mediante señales analógicas usando *modems* (modulador/demodulador). El modem convierte la serie de pulsos de tensión binarios (bi-valuados) en una señal analógica, codificando los datos digitales haciendo variar alguno de los parámetros característicos de una señal denominada *portadora*. La señal resultante ocupa un cierto espectro de frecuencias centrado en torno a la frecuencia de la portadora. De esta manera se podrán transmitir datos digitales a través de medios adecuados a la naturaleza de la señal portadora. Los modems más convencionales representan los datos binarios en el espectro de la voz y por lo tanto, hacen posible que los datos se propaguen a través de líneas telefónicas convencionales. En el otro extremo de la línea, el modem demodula la señal para con ello recuperar los datos originales.

Realizando una operación muy similar a la que realizan los modems, los datos analógicos se pueden representar mediante señales digitales. El dispositivo que realiza esta función para la voz se denomina *codec* (codificador- decodificador). Esencialmente, el codec aproxima a la señal analógica que representa directamente a la voz, mediante una cadena de bits. En el receptor, dichos bits se usan para reconstruir los datos analógicos.

Así pues, la Figura 3.11 sugiere que los datos se pueden codificar de varias maneras. Este punto se volverá a tratar en el Capítulo 5.

TRANSMISIÓN

Queda por hacer una consideración final. Tanto las señales analógicas como las digitales se pueden transmitir a través del medio de transmisión adecuado. El medio de transmisión en concreto determinará cómo se tratan estas señales. En la Tabla 3.3 se resumen los métodos de transmisión de datos. La transmisión analógica es una forma de transmitir las señales analógicas independientemente de su contenido;

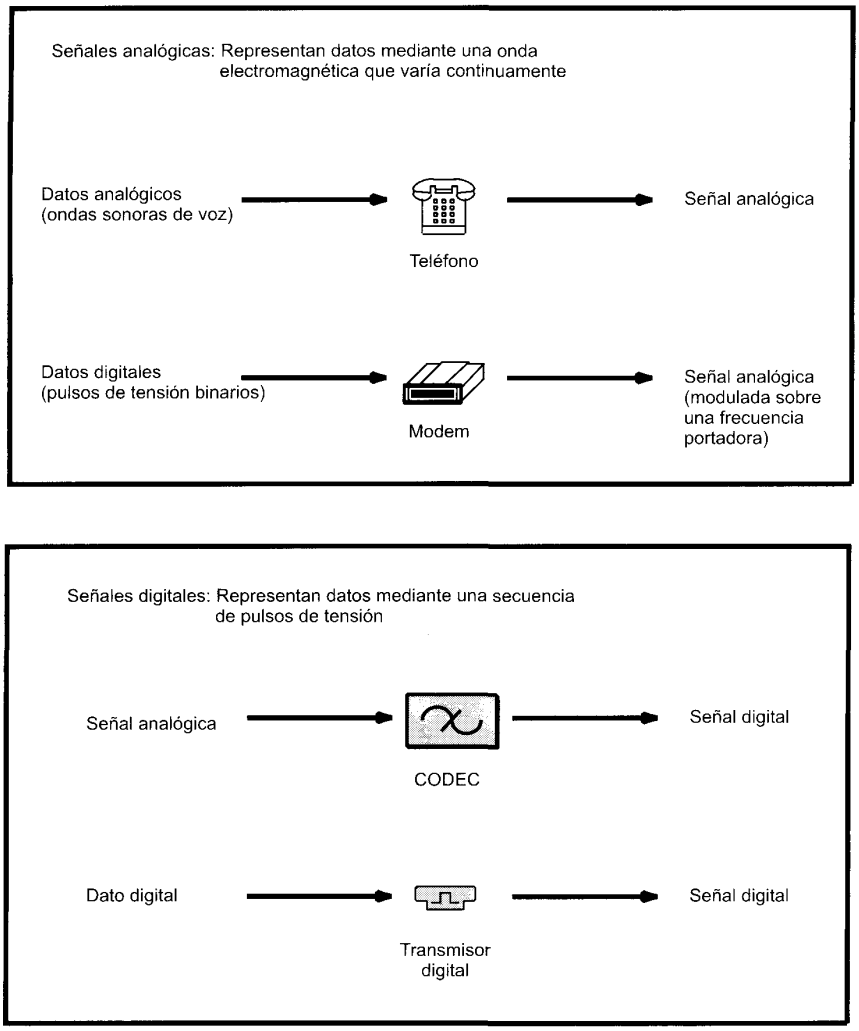


Figura 3.11. Señalización analógica y digital de datos analógicos y digitales.

las señales pueden representar datos analógicos (por ejemplo, voz) o datos digitales (por ejemplo, los datos binarios modulados en un modem). En cualquier caso, la señal analógica se irá debilitando (atenuándose) con la distancia. Para conseguir distancias más largas, el sistema de transmisión analógico incluye amplificadores que inyectan energía en la señal. Desgraciadamente, el amplificador también inyecta energía en las componentes de ruido. Para conseguir distancias mayores, al utilizar amplificadores en cascada, la señal se distorsiona cada vez más. Para datos analógicos, como la voz, se puede tolerar una pequeña distorsión, ya que en ese caso los datos siguen siendo inteligibles. Sin embargo, para los datos digitales los amplificadores en cascada introducirán errores.

La transmisión digital, por contra, es dependiente del contenido de la señal. Una señal digital sólo se puede transmitir a una distancia limitada, ya que la atenuación y otros aspectos negativos pueden afectar a la integridad de los datos transmitidos. Para conseguir distancias mayores se usan repetidores. Un re-

Tabla 3.3. Transmisión analógica y digital.

(a) Datos y señales

	Señal analógica	Señal digital
Señal analógica	Hay dos alternativas (1) la señal ocupa el mismo espectro que los datos analógicos; (2) los datos analógicos se codifican ocupando una porción distinta del espectro.	Los datos analógicos se codifican utilizando un codec para generar una cadena de bits.
Datos digitales	Los datos digitales se codifican usando un modem para generar señal analógica.	Hay dos alternativas (1) la señal consiste en dos niveles de tensión que representan dos valores binarios (2) los datos digitales se codifican para producir una señal digital con las propiedades deseadas.

(b) Procesamiento de señales

	Transmisión analógica	Transmisión digital
Señal analógica	Se propaga a través de amplificadores; se trata de igual manera si la señal se usa para representar datos analógicos o digitales.	Se supone que la señal analógica representa datos digitales. La señal se propaga a través de repetidores; en cada repetidor, los datos digitales se obtienen de la señal de entrada y se usan para regenerar una nueva señal analógica de salida.
Señal digital	No se usa.	La señal digital representa una cadena de unos o ceros, los cuales pueden representar datos digitales o pueden ser resultado de la codificación de datos analógicos. La señal se propaga a través de repetidores; en cada repetidor, se recupera la cadena de unos y ceros a partir de la señal de entrada, a partir de los cuales se genera la nueva cadena de salida.

petidor recibe la señal digital, regenera el patrón de ceros y unos y los retransmite. De esta manera se evita la atenuación.

Para señales analógicas se puede usar la misma técnica anterior si la señal transmitida transporta datos digitales. En este caso, el sistema de transmisión tendrá repetidores convenientemente espaciados en lugar de amplificadores. Dichos repetidores recuperan los datos digitales a partir de la señal analógica y generan una señal analógica limpia. De esta manera el ruido no es acumulativo.

Un problema a resolver es la elección del mejor método de transmisión. A pesar de que los sistemas de transmisión analógica han absorbido grandes inversiones, la industria de las telecomunicaciones y los usuarios han optado por la transmisión digital. Tanto las comunicaciones a larga distancia como los servicios de comunicación a distancias muy cortas (por ejemplo, entre edificios) se están reconvirtiendo gradualmente a digital, y es más, igualmente se está introduciendo la señalización digital en todos los sistemas donde sea factible. Las razones más importantes que justifican esta elección son:

- **Tecnología digital:** las mejoras en las tecnologías de integración a gran escala (LSI) y muy gran escala (VLSI) se han traducido en una disminución continua tanto en coste como en el tamaño de la circuitería digital. El instrumental analógico no ha experimentado una reducción similar.

- **Integridad de los datos:** al usar repetidores en lugar de amplificadores, el ruido y otros efectos negativos no son acumulativos. Por tanto, usando tecnología digital es posible transmitir datos conservando su integridad a distancias mayores utilizando incluso líneas de calidad inferior.
- **Utilización de la capacidad:** en términos económicos, el tendido de líneas de transmisión de banda ancha ha llegado a ser factible, incluso para medios tales como canales vía satélite y fibra óptica. Para usar eficazmente todo ese ancho de banda se necesita un alto grado de mutiplexación. La multiplexación, se puede realizar más fácilmente y con menor coste usando técnicas digitales (división en el tiempo) que con técnicas analógicas (división en frecuencia). Estas cuestiones se estudiarán en el Capítulo 8.
- **Seguridad y privacidad:** las técnicas de encriptación se pueden aplicar fácilmente a los datos digitales, o a los analógicos que se hayan previamente digitalizado.
- **Integración:** en el tratamiento digital de datos analógicos y digitales, todas las señales tienen igual forma y pueden ser procesadas de una forma similar. Este hecho posibilita la integración de voz, vídeo y datos usando la misma infraestructura.

3.3. PERTURBACIONES EN LA TRANSMISIÓN

En cualquier sistema de comunicaciones se debe aceptar que la señal que se recibe diferirá de la señal transmitida debido a varias adversidades y dificultades sufridas en la transmisión. En las señales analógicas, estas dificultades introducen alteraciones aleatorias que degradan la calidad de la señal. En las señales digitales, se producen bits erróneos: un 1 binario se transformará en un 0 y viceversa. En este apartado se van a estudiar las dificultades mencionadas, comentando sus efectos sobre la capacidad de transportar información en los enlaces de transmisión; en el Capítulo 5 se presentan algunas medidas a tomar para paliar el efecto de estas dificultades.

Las perturbaciones más significativas son:

- La atenuación y la distorsión de atenuación.
- La distorsión de retardo.
- El ruido.

ATENUACIÓN

La energía de la señal decae con la distancia en cualquier medio de transmisión. En medios guiados, esta reducción de la energía es por lo general logarítmica y por lo tanto, se expresa típicamente como un número constante en decibelios por unidad de longitud. En medios no guiados, la atenuación es una función más compleja de la distancia y dependiente a su vez de las condiciones atmosféricas. Se pueden establecer tres consideraciones respecto a la atenuación. Primera, la señal recibida debe tener suficiente energía para que la circuitería electrónica en el receptor pueda detectar e interpretar la señal adecuadamente. Segunda, para ser recibida sin error, la señal debe conservar un nivel suficientemente mayor que el ruido. Tercera, la atenuación es una función creciente de la frecuencia.

Los dos primeros problemas se resuelven controlando la energía de la señal, para ello se usan amplificadores o repetidores. En un enlace punto a punto, la energía de la señal en el transmisor debe ser lo suficientemente elevada para que se reciba con inteligibilidad, pero no tan elevada, tal que sature la circuitería del transmisor, lo que generaría una señal distorsionada. A partir de cierta distancia, la atenuación es inaceptable, lo que requiere la utilización de repetidores o amplificadores que realcen la señal periódicamente. Este tipo de problemas son todavía más complejos en líneas multipunto, en las que la distancia entre el transmisor y el receptor es variable.

El tercer problema es especialmente relevante para el caso de las señales analógicas. Debido a que la atenuación varía en función de la frecuencia, la señal recibida está distorsionada, reduciéndose así la inteligibilidad. Para soslayar este problema, existen técnicas para ecualizar la atenuación en una banda de frecuencias. En las líneas telefónicas esto se realiza normalmente usando bobinas de carga que cambian las propiedades eléctricas de la línea, dando lugar a un suavizado de los efectos de la atenuación. Otra aproximación alternativa es la utilización de amplificadores que amplifiquen más las frecuencias altas que las bajas.

En la Figura 3.12a se incluye un ejemplo, en el que se representa la atenuación como función de la frecuencia para una línea alquilada convencional. En dicha figura, la atenuación se ha obtenido como una medida relativa respecto de la atenuación a 1.000 Hz. Los valores positivos en el eje *y* representan atenuaciones mayores que la sufrida a 1.000 Hz. A la entrada se aplica un tono a 1.000 Hz con una potencia conocida, posteriormente se mide la potencia $P_{1.000}$ en la salida. Este procedimiento se repite para cualquier otra frecuencia f, y la atenuación relativa en decibelios es[5]

$$N_f = -10 \log_{10} \frac{P_f}{P_{1.000}}$$

La línea continua en la Figura 3.12a muestra la atenuación sin ecualización. Como se puede observar, las componentes en frecuencia en el extremo superior de la banda de voz se atenúan mucho más que las componentes en bajas frecuencias. Es evidente que esto distorsiona la señal de voz recibida. La línea discontinua muestra los efectos de la ecualización. Al aplanar la atenuación relativa, se consigue una mejora en la calidad de la señal de voz. Esto también permite, al usar un modem, una velocidad de transmisión superior.

La distorsión de atenuación es un problema mucho menor para las señales digitales. Como ya se ha mencionado, la energía de la señal digital decae rápidamente con la frecuencia (Figura 3.5b); la mayor parte de sus componentes están concentradas en torno a la frecuencia fundamental o velocidad de transmisión (en bits/segundo o bps) de la señal.

DISTORSIÓN DE RETARDO

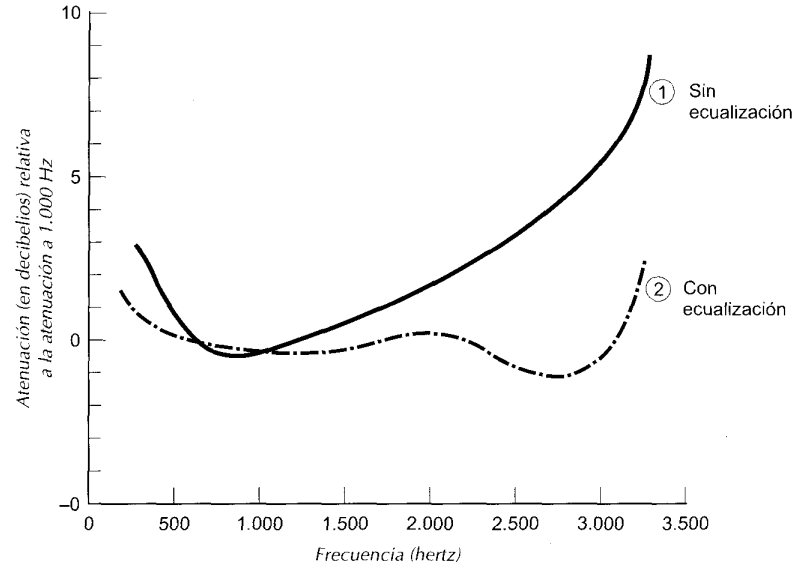
La distorsión de retardo es un fenómeno peculiar de los medios guiados. Esta distorsión está causada por el hecho de que la velocidad de propagación de la señal en el medio varía con la frecuencia. Para una señal de banda limitada, la velocidad tiende a ser mayor cerca de la frecuencia central y disminuye al acercarse a los extremos de la banda. Por tanto, las distintas componentes en frecuencia de la señal llegarán al receptor en instantes diferentes de tiempo, dando lugar a desplazamientos en fase entre las diferentes frecuencias.

Este efecto se llama distorsión de retardo, ya que la señal recibida está distorsionada debido al retardo variable que sufren sus componentes. La distorsión de retardo es particularmente crítica en la transmisión de datos digitales. Supóngase que se está transmitiendo una secuencia de bits, utilizando una señal analógica o digital. Debido a la distorsión de retardo, algunas de las componentes de la señal en un bit se desplazarán hacia otras posiciones, provocando interferencia entre símbolos. Este hecho es el factor que limita principalmente la velocidad de transmisión máxima en un canal de transmisión.

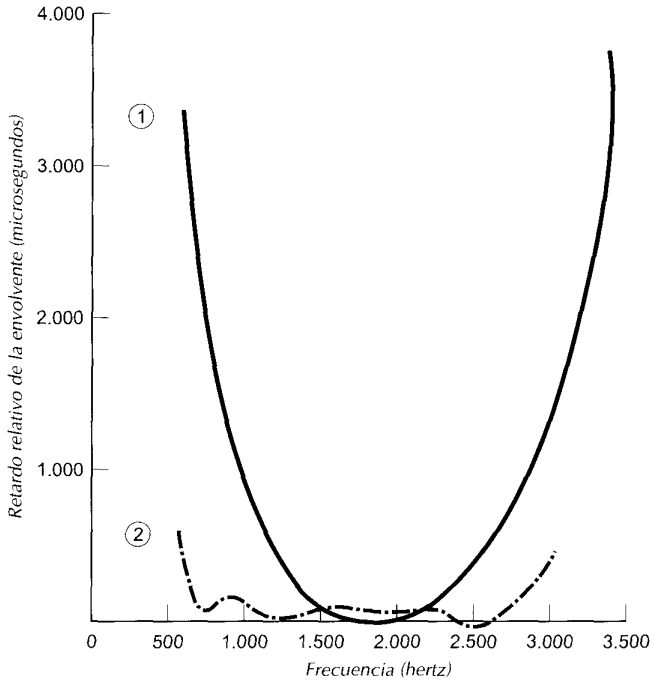
Las técnicas de ecualización también se pueden emplear para compensar la distorsión de retardo. Usando de nuevo como ejemplo una línea telefónica alquilada, en la Figura 3.12b se muestra el efecto de la ecualización del retardo en función de la frecuencia.

---

[5] En todo el libro, a menos que se indique lo contrario, $\log(x)$ significa $\log_{10}(x)$.



(a) Atenuación



(b) Distorsión de retardo

Figura 3.12. Curvas correspondientes a las distorsiones de atenuación y retardo para un canal de voz.

RUIDO

En cualquier dato transmitido, la señal recibida consistirá en la señal transmitida modificada, debido a las distorsiones introducidas por el sistema de transmisión, además de señales no deseadas que se insertarán en algún punto entre el emisor y el receptor. A estas últimas señales no deseadas se les denomina ruido. El ruido es el factor de mayor importancia a la hora de limitar las prestaciones de un sistema de comunicación.

La señal de ruido se puede clasificar en cuatro categorías:

- Ruido térmico.
- Ruido de intermodulación.
- Diafonía.
- Ruido impulsivo.

El **ruido térmico** se debe a la agitación térmica de los electrones. Está presente en todos los dispositivos electrónicos y medios de transmisión; como su nombre indica es función de la temperatura. El ruido térmico está uniformemente distribuido en el espectro de frecuencias y es por esto por lo que a veces se denomina ruido blanco. El ruido térmico no se puede eliminar y, por tanto, impone un límite superior en las prestaciones de los sistemas de comunicación. La cantidad de ruido térmico en un ancho de banda de 1 Hz en cualquier dispositivo o conductor es

$$N_0 = kT \text{ (W/Hz)}$$

donde[6]

N_0 = densidad de potencia del ruido, en vatios por 1 Hz de ancho de banda.

k = constante de Boltzmann = $1{,}3803 \times 10^{-23}$ J/°K.

T = temperatura, en grados Kelvin.

Ejemplo

A temperatura ambiente, $T = 17$ °C, o 290 °K, la densidad de potencia del ruido térmico es:

$$N_0 = (1{,}3803 \times 10^{-23}) \times 290 = 4 \times 10^{-21} \text{ W/Hz} = -204 \text{ dBW/Hz}$$

donde dBW corresponde a decibelio-vatio, unidad definida en el Apéndice 3B.

Se supone que el ruido es independiente de la frecuencia. Así pues, el ruido térmico presente en un ancho de banda de B hertzios se puede expresar en vatios como

$$N = kTB$$

o, en decibelio-vatios

$$\begin{aligned} N &= 10 \log k + 10 \log T + 10 \log B \\ &= -228{,}6 \text{ dBW} + 10 \log T + 10 \log B \end{aligned}$$

[6] Un julio (J) en el Sistema Internacional (SI) es la unidad de energía eléctrica, mecánica o térmica. Un vatio es la unidad de potencia en SI, igual a un julio por segundo. El Kelvin (K) es la unidad de temperatura termodinámica en el SI. Una temperatura de grados kelvin igual a T, expresada en grados Celsius será igual a $T - 273{,}15$.

Ejemplo

Dado un receptor con una temperatura del ruido efectiva de 100° y 10 MHz de ancho de banda, el nivel del ruido térmico a la salida del receptor es

$$\begin{aligned} N &= -228{,}6\,\text{dBW} + 10\log 10^2 + 10\log 10^7 \\ &= -228{,}6 + 20 + 70 \\ &= -138{,}6\,\text{dBW} \end{aligned}$$

Cuando señales de distintas frecuencias comparten el mismo medio de transmisión puede producirse un **ruido de intermodulación**. El efecto del ruido de intermodulación es la aparición de señales a frecuencias que sean suma o diferencia de las dos frecuencias originales, o múltiplos de éstas. Por ejemplo, la mezcla de las señales de frecuencias f_1 y f_2 puede producir energía a frecuencias $f_1 + f_2$. Estas componentes espurias podrían interferir con otras componentes a frecuencia $f_1 + f_2$.

El ruido de intermodulación se produce cuando hay alguna no linealidad en el transmisor, receptor, o en el sistema de transmisión. Normalmente, estos sistemas se comportan como sistemas lineales; es decir, la salida es igual a la entrada multiplicada por una constante. En los sistemas no lineales, la salida es una función más compleja de la entrada. Estas componentes pueden aparecer debido al funcionamiento incorrecto de los sistemas o por el uso de excesiva energía en la señal. Bajo estas circunstancias aparecen términos suma o diferencia, o lo que es lo mismo ruido de intermodulación.

La **diafonía** la ha podido experimentar todo aquel que al usar un teléfono, haya oído otra conversación; se trata en realidad de un acoplamiento no deseado entre las líneas que transportan las señales. Esto puede ocurrir por el acoplamiento eléctrico entre cables de pares cercanos, o en raras ocasiones, en líneas de cable coaxial que transporten varias señales. La diafonía también puede aparecer cuando las señales no deseadas se captan en las antenas de microondas; aunque éstas se caracterizan por ser altamente direccionales, la energía de las microondas se dispersa durante la transmisión. Normalmente, la diafonía es del mismo orden de magnitud (o inferior) que el ruido térmico.

Los ruidos antes descritos son de magnitud constante y razonablemente predecible. Así pues, es posible idear un sistema de transmisión que les haga frente. Por el contrario, el **ruido impulsivo** es no continuo y está constituido por pulsos o picos irregulares de corta duración y de amplitud relativamente grande. Se generan por una gran diversidad de causas, como, por ejemplo, por perturbaciones electromagnéticas exteriores producidas por tormentas atmosféricas, o fallos y defectos en los sistemas de comunicación.

Generalmente, el ruido impulsivo no tiene mucha transcendencia para los datos analógicos. Por ejemplo, la transmisión de voz se puede perturbar mediante chasquidos o crujidos cortos sin ninguna pérdida de inteligibilidad. Sin embargo, el ruido impulsivo es una de las fuentes principales de error en la comunicación digital de datos. Por ejemplo, un pico de energía con duración de 0,01 s no inutilizaría datos de voz, pero podría corromper 560 bits aproximadamente si se transmiten a 56 kbps. La Figura 3.13 muestra un ejemplo del efecto del ruido sobre una señal digital. Aquí el ruido consiste en un nivel relativamente pequeño de ruido térmico más picos ocasionales de ruido impulsivo. Los datos digitales se recuperan muestreando la señal recibida una vez por cada intervalo de duración del bit. Como se puede observar, el ruido es a veces suficiente para convertir un 1 en un 0 o un 0 en un 1.

CAPACIDAD DEL CANAL

Se ha visto que hay una gran variedad de efectos nocivos que distorsionan o corrompen la señal. Para los datos digitales, la cuestión a resolver es en qué medida estos defectos limitan la velocidad con la que se pueden transmitir. Se denomina **capacidad del canal** a la velocidad a la que se pueden transmitir los datos en un canal o ruta de comunicación datos.

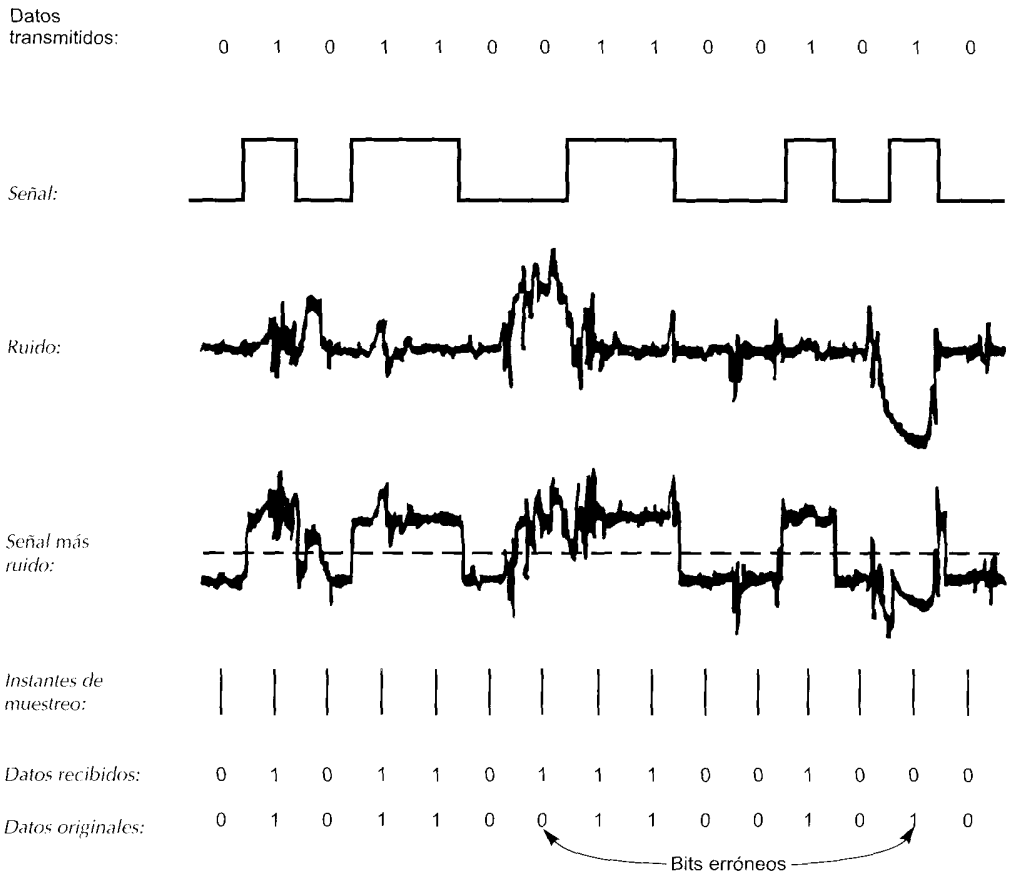


Figura 3.13. Efecto del ruido en una señal digital.

Hay cuatro conceptos relacionados con la capacidad, que son:

- **La velocidad de transmisión de los datos:** es la velocidad expresada en bits por segundo (bps), a la que se pueden transmitir los datos.
- **El ancho de banda:** es el ancho de banda de la señal transmitida que estará limitado por el transmisor y por la naturaleza del medio de transmisión; se mide en ciclos por segundo o hertzios.
- **El ruido:** es el nivel medio de ruido a través del camino de transmisión.
- **La tasa de errores:** es la tasa a la que ocurren los errores. Se considera que ha habido un error cuando se recibe un 1 habiendo transmitido un 0 o se recibe un 0 habiendo transmitido un 1.

El problema considerado aquí es el siguiente: los servicios de comunicaciones son, por lo general, caros, y normalmente cuanto mayor es el ancho de banda requerido por el servicio, mayor es el costo. Es más, todos los canales de transmisión de interés práctico están limitados en banda. Las limitaciones surgen de las propiedades físicas de los medios de transmisión o por limitaciones que se imponen deliberadamente en el transmisor para prevenir interferencias con otras fuentes. Por consiguiente, es deseable hacer un uso tan eficiente como sea posible, dado un ancho de banda limitado. Para los datos digitales, esto significa que para un ancho de banda determinado sería deseable conseguir la mayor velocidad de datos posible no superando la tasa de errores permitida. El mayor inconveniente para conseguir este propósito es la existencia de ruido.

Ancho de banda de Nyquist

Para comenzar, considérese el caso de un canal exento de ruido. En este entorno, la limitación en la velocidad de los datos está impuesta simplemente por el ancho de banda de la señal. Nyquist formalizó esta limitación, afirmando que si la velocidad de transmisión de la señal es $2B$, entonces una señal con frecuencias no superiores a B es suficiente para transportar esta velocidad de transmisión de la señal. Y viceversa: dado un ancho de banda de B, la velocidad mayor de transmisión de la señal que se puede conseguir es $2B$. Esta limitación está provocada por la interferencia entre símbolos, que se produce por la distorsión de retardo. Este resultado, desarrollado en el Apéndice 5A, es de utilidad en el diseño de convertidores digital a analógico.

Obsérvese que en el último párrafo, nos hemos referido a la velocidad de la señal. Si las señales a transmitir son binarias (dos niveles de tensión), la velocidad de transmisión de datos que se puede conseguir con B Hz es de $2B$ bps. Por ejemplo, considérese un canal de voz que se utiliza mediante un modem para transmitir datos digitales. Supóngase un ancho de banda de 3.100 Hz. Entonces la capacidad, C del canal es $2B = 6.200$ bps. No obstante, como se verá en el Capítulo 5, se pueden usar señales con más de dos niveles; es decir, cada elemento de señal puede representar a más de dos bits. Por ejemplo, si se usa una señal con cuatro niveles de tensión, cada elemento de dicha señal podrá representar dos bits. La formulación de Nyquist para el caso de señales multinivel es

$$C = 2B \log_2 M$$

donde M es el número de señales discretas o niveles de tensión. Así pues, para $M = 8$, valor típico que se usa en algunos modems, la capacidad resulta ser 18.600 bps.

Por tanto, para un ancho de banda dado, la velocidad de transmisión de datos se puede incrementar considerando un número mayor de señales diferentes. Sin embargo, esto supone una dificultad mayor en el receptor: en lugar de tener que distinguir una de entre dos señales, deberá distinguir una de entre M posibles señales. El ruido y otras dificultades en la línea de transmisión limitarán el valor de M.

Fórmula para la capacidad de Shannon

La fórmula de Nyquist implica que al duplicar el ancho de banda se duplica la velocidad de transmisión, si todo lo demás se mantiene inalterado. Ahora establezcamos una relación entre la velocidad de transmisión, el ruido y la tasa de errores. Para una explicación intuitiva considérese de nuevo la Figura 3.13. La presencia de ruido puede corromper uno o más bits. Si se aumenta la velocidad de transmisión, el bit se hace más «corto» de tal manera que dado un patrón de ruido, éste afectará a un mayor número de bits. Así pues, dado un nivel de ruido, cuanto mayor es la velocidad de transmisión, mayor es la tasa de errores.

Todos estos conceptos se pueden relacionar con la formula desarrollada por el matemático Claude Shannon. Como se ha comentado, cuanto mayor es la velocidad de transmisión, mayor es el daño que puede ocasionar el ruido. Dado un nivel de ruido, es de esperar que incrementando la energía de la señal se mejoraría la recepción de datos en presencia de ruido. Un parámetro fundamental en el desarrollo de este razonamiento es la relación señal-ruido (SNR), que se define como el cociente entre la potencia de la señal y la potencia del ruido presente en un punto determinado en el medio de transmisión. Generalmente, este cociente se mide en el receptor, ya que es aquí donde se realiza el procesado de la señal y la eliminación del ruido no deseado. Por cuestiones de comodidad, la SNR se proporciona en decibelios:

$$(\text{SNR})_{\text{dB}} = 10 \log_{10} \frac{\text{potencia de señal}}{\text{potencia de ruido}}$$

Esta expresión muestra, en decibelios, cuanto excede la señal al nivel de ruido. Una SNR alta significará una señal de alta calidad y la necesidad de un reducido número de repetidores.

La relación señal-ruido es importante en la transmisión de datos digitales, ya que determina la máxima velocidad de transmisión que se puede conseguir. Una conclusión de Shannon es que la capacidad máxima del canal, en bits por segundo, verifica la ecuación

$$C = B \log_2 (1 + \text{SNR})$$

donde C es la capacidad del canal en bits por segundo y B es el ancho de banda del canal en hertzios. La fórmula de Shannon representa el máximo límite teórico que se puede conseguir. Sin embargo, en la práctica, se consiguen razones de bits mucho menores. Una razón para esto reside en el hecho de que la fórmula anterior supone ruido blanco (ruido térmico). Además no se han tenido en cuenta el ruido impulsivo, la atenuación o la distorsión de retardo.

La capacidad tal como se ha calculado en la formula precedente se denomina capacidad libre de errores. Shannon probó que si la tasa de información real en el canal es menor que la capacidad libre de errores, entonces es posible teóricamente usar una codificación de la señal que consiga una transmisión exenta de errores a través del canal. Desafortunadamente, el teorema de Shannon no sugiere la manera de encontrar dicho código, pero proporciona un criterio de referencia con el que se pueden comparar las prestaciones de los esquemas de comunicación reales.

Pueden ser instructivas otras consideraciones adicionales que se deducen a partir de la ecuación anterior. Para un nivel de ruido dado, podría parecer que la velocidad de transmisión se puede aumentar incrementado tanto la energía de la señal como el ancho de banda. Sin embargo, al aumentar la energía de la señal, también lo hacen las no linealidades del sistema, dando lugar a un aumento del ruido de intermodulación. Obsérvese igualmente, que como el ruido se ha supuesto blanco, cuanto mayor sea el ancho de banda, más ruido se introducirá en el sistema. Por lo tanto, cuando B aumenta, la SNR disminuye.

Ejemplo

En el siguiente ejemplo se relacionan las formulaciones de Shannon y Nyquist. Supóngase que el espectro de un canal está situado entre 3 MHz y 4 MHz y que la SNR es de 24 dB. En este caso

$$\begin{aligned} B &= 4 \text{ MHz} - 3 \text{ MHz} = 1 \text{ MHz} \\ \text{SNR}_{\text{dB}} &= 24 \text{ dB} = 10 \log_{10}(\text{SNR}) \\ \text{SNR} &= 251 \end{aligned}$$

Usando la formula de Shannon se tiene que

$$C = 10^6 \times \log_2 (1 + 251) \approx 10^6 \times 8 = 8 \text{ Mbps}$$

Éste es, como ya se ha mencionado, un límite teórico difícil de alcanzar. No obstante, supóngase que este límite se puede conseguir. Según la fórmula de Nyquist, ¿cuántos niveles de señalización se necesitarán? Se tiene que

$$\begin{aligned} C &= 2B \log_2 M \\ 8 \times 10^6 &= 2 \times (10^6) \times \log_2 M \\ 4 &= \log_2 M \\ M &= 16 \end{aligned}$$

El cociente E_b/N_0

Finalmente, en este apartado se presenta un parámetro relacionado con la SNR que es más adecuado para determinar las tasas de error y la velocidad de transmisión. Este parámetro es la fracción entre la

energía de la señal por bit y la densidad de potencia del ruido por hertzio, E_b/N_0. Sea una señal, digital o analógica, que contenga datos digitales binarios transmitidos a una determinada velocidad R. Teniendo en cuenta que 1 W = 1 J/s, la energía por bit de la señal será $E_b = ST_b$, donde S es la potencia de la señal y T_b es el tiempo necesario para enviar un bit. La velocidad de transmisión es $R = 1/T_b$. Por tanto,

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$$

o, en decibelios,

$$\left(\frac{E_b}{N_0}\right)_{dB} = S_{dBW} - 10\log R - 10\log k - 10\log T$$

$$\left(\frac{E_b}{N_0}\right)_{dB} = S_{dBW} - 10\log R + 228{,}6\,dBW - 10\log T$$

El cociente E_b/N_0 es importante ya que para datos digitales la tasa de error en un bit es una función (decreciente) de este cociente. Dado un valor de E_b/N_0, para conseguir la tasa de errores deseada, se pueden seleccionar los parámetros de acuerdo con la fórmula anterior. Nótese que cuando se aumenta la velocidad de transmisión R, la potencia de la señal transmitida, relativa al ruido, debe aumentarse para mantener el E_b/N_0 requerido.

Intentemos inferir intuitivamente este resultado a partir de la Figura 3.13. La señal aquí considerada es digital, pero el mismo razonamiento podría extenderse para el caso de una señal analógica. En algunos casos, el ruido es suficiente como para alterar el valor de un bit. Ahora, si la velocidad de transmisión se duplicase, los bits tendrían asociada una duración menor, con lo que el mismo ruido podría destruir dos bits. Por lo tanto, para una señal y ruido de energía constante, un incremento en la velocidad de transmisión aumentaría la tasa de error.

Ejemplo

En la modulación digital binaria PSK (Phase-Shift Keying) (definida en el Capítulo 5), para obtener una probabilidad de error en un bit igual a 10^{-4} (un bit erróneo cada 10.000) se necesita un $E_b/N_0 = 8{,}4$ dB. Si la temperatura efectiva es 290 °K (temperatura ambiente) y la velocidad de transmisión es 2.400 bps, ¿qué nivel de señal recibida se necesita?

En este caso se tiene que

$$\begin{aligned} 8{,}4 &= S(\text{dBW}) - 10\log 2.400 + 228{,}6\,\text{dBW} - 10\log 290 \\ &= S(\text{dBW}) - (10)(3{,}38) + 228{,}6 - (10)(2{,}46) \\ S &= -161{,}8\,\text{dBW} \end{aligned}$$

3.4. LECTURAS RECOMENDADAS

Hay muchos libros que cubren los aspectos fundamentales de la transmisión analógica y digital. [COUC97] es bastante completo. Una referencia de calidad es [FREE98], en la que se incluyen algunos de los ejemplos proporcionados a lo largo de este capítulo. Otros tratados excelentes son los tres volúmenes de [BELL90], además de [LATHI98] y [GLOV98].

[JAME95] es un tratado asequible sobre las series de Fourier y las transformadas de Fourier.

BELL90 Bellcore (Bell Communications Research). *Telecommunications Transmission Engineering, 3rd edition.* Three volumes. 1990.

COUC97 Couch, L. *Digital and Analog Communication Systems*. Upper Saddle River, NJ: Prentice Hall, 1997.

FREE98 Freeman, R. *Telecommunications Transmission Handbook*. New York: Wiley, 1998.

GLOV98 Glover, I., y Grant, P. *Digital Communications*. Upper Saddle River, NJ: Prentice Hall, 1998.

JAME95 James, J. *A Student's Guide to Fourier Transforms*. Cambridge, England: Cambridge University Press, 1995.

LATH98 Lathi, B. *Modern Digital and Analog Communication Systems*. New York: Oxford University Press, 1998.

3.5. PROBLEMAS

3.1. **a)** En una configuración multipunto, sólo un dispositivo puede trasmitir cada vez, ¿por qué?

b) Hay dos posibles aproximaciones que refuerzan la idea de que en un momento dado, sólo un dispositivo pueda transmitir. En un sistema centralizado, una estación es la responsable del control y podrá o bien transmitir, o decidir que lo haga cualquier otra. En el método descentralizado, las estaciones cooperan entre sí, estableciéndose una serie de turnos. ¿Qué ventajas y desventajas presentan ambas aproximaciones?

3.2. El sonido se puede modelar mediante funciones sinusoidales. Compare la frecuencia relativa y la longitud de onda de las notas musicales. Considere que la velocidad del sonido es igual a 330 m/s y que las frecuencias de una escala musical son:

Nota	DO	RE	MI	FA	SOL	LA	SI	DO
Frecuencia	264	297	330	352	396	440	495	528

3.3. Si la curva trazada con una línea continua en la Figura 3.14 representa al $(2\pi t)$, ¿qué función corresponde a la línea discontinua? En otras palabras, la línea discontinua se puede expresar como $A \operatorname{sen}(2\pi ft + \psi)$, ¿qué son A, f y ψ?

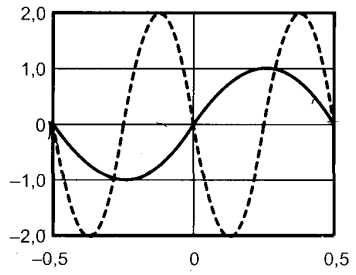


Figura 3.14. Figura del Problema 3.3.

3.4. Una señal de banda limitada con sólo tres componentes en frecuencia: dc, 100 Hz y 200 Hz, en forma de seno-coseno se puede expresar como

$$x(t) = 12 + 15\cos 200\pi t + 20\operatorname{sen} 200\pi t - 5\cos 400\,\pi t - 12\operatorname{sen} 400\pi t$$

Exprese la señal anterior en forma de amplitud/fase.

3.5. Expresar la señal $(1 + 0{,}1 \cos 5t) \cos 100t$ como combinación lineal de funciones sinusoidales, y encontrar la amplitud, frecuencia y fase de cada una de las componentes. (*Pista*: usar la expresión del $\cos a \cos b$.)

3.6. Encontrar el periodo de la función $f(t) = (10 \cos t)^2$.

3.7. La Figura 3.4 muestra el efecto resultante al eliminar las componentes de alta frecuencia de un pulso cuadrado y quedarse sólo con las componentes de baja frecuencia. ¿Cómo sería la señal resultante en el caso contrario (es decir, quedándose con todos los armónicos de frecuencia alta y eliminando los de bajas frecuencias)?

3.8. La Figura 3.5b muestra la función en el dominio de la frecuencia correspondiente a un pulso rectangular. Este pulso puede corresponder a un 1 digital en un sistema de comunicación. Obsérvese que se necesita un número infinito de frecuencias (con amplitud decreciente cuanto mayor es la frecuencia). ¿Qué implicaciones tiene este hecho en un sistema de transmisión real?

3.9. El IRA es un código de 7 bits que permite la definición de 128 caracteres. En los años 70, muchos medios de comunicación recibían las noticias a través de un servicio que usaba 6 bits denominado TTS. Este código transmitía caracteres en mayúsculas y minúsculas así como caracteres especiales y órdenes de control. Generalmente se utilizan 100 caracteres. ¿Cómo cree que se puede conseguir esto?

3.10. ¿Cuál es el incremento posible en la resolución horizontal para una señal de vídeo de ancho de banda 5 MHz? ¿Y para la resolución vertical? Respóndanse ambas cuestiones por separado; es decir, utilice el incremento de ancho de banda para aumentar la resolución horizontal o la vertical, pero no ambas.

3.11. **a)** Suponga que se transmite una imagen digitalizada de TV de 480×500 pixels, en la que cada pixel puede tomar uno de entre 32 posibles valores de intensidad. Supóngase que se envían 30 imágenes por segundo. (Esta fuente digital es aproximadamente igual que los estándares adoptados para la difusión de TV.) Determinar la velocidad de transmisión R de la fuente en bps.

b) Suponga que la fuente anterior se transmite por un canal de 4,5 MHz de ancho de banda con una relación señal-ruido de 35 dB. Encontrar la capacidad del canal en bps.

c) ¿Cómo se deberían modificar los parámetros del apartado a) para permitir la transmisión de la señal de TV en color sin incrementar el valor de R?

3.12. Dado un amplificador con una temperatura efectiva de ruido de 10.000 °K y con un ancho de banda de 10 MHz, ¿cuál será el nivel de ruido térmico a la salida?

3.13. ¿Cuál es la capacidad para un canal de un «teletipo» de 300 Hz de ancho de banda con una relación señal-ruido de 3 dB?

3.14. Para operar a 9.600 bps se usa un sistema de señalización digital:

a) Si cada elemento de señal codifica una palabra de 4 bits, ¿cuál es el ancho de banda mínimo necesario?

b) ¿Y para palabras de 8 bits?

3.15. ¿Cuál es el nivel de ruido térmico para un canal de ancho de banda de 10 kHz, 1.000 w de potencia operando a 50 °C?

3.16. Considérense los trabajos de Shannon y Nyquist sobre la capacidad del canal. Cada uno de ellos estableció un límite superior para la razón de bits del canal basándose en dos aproximaciones diferentes. ¿Cómo se pueden relacionar ambas aproximaciones?

3.17. Sea un canal con una capacidad de 20 Mbps. El ancho de banda de dicho canal es 3 MHz. ¿Cuál es la relación señal-ruido admisible para conseguir la mencionada capacidad?

3.18. La onda cuadrada de la Figura 3.7c, con $T = 1$ ms, se transmite a través de un filtro pasa-baja ideal con frecuencia de corte a 8 kHz de ganancia unidad.

a) Determinar la potencia de la señal de salida.

b) Suponiendo que a la entrada del filtro hay un ruido térmico con $N_0 = 0{,}1$ μW/Hz, encontrar la relación señal-ruido en dB a la salida.

3.19. Si el nivel recibido de una señal en un sistema digital es de -151 dBW y la temperatura efectiva del ruido en el receptor es de 1.500 °K, ¿cuál es el cociente E_b/N_0 para un enlace que transmita a 2.400 bps?

3.20. Rellenar las casillas vacías de la siguiente tabla correspondientes a distintas potencias para obtener la correspondiente relación expresada en decibelios.

Decibelios	1	2	3	4	5	6	7	8	9	10
Pérdidas			0,5							0,1
Ganancias			2							10

3.21. Si un amplificador tiene una ganancia en tensión de 30 dB, ¿cuál es su relación de tensiones de entrada y salida?

3.22. Si un amplificador proporciona a la salida 20 W, ¿cuánto proporcionará expresado en dBW?

APÉNDICE 3A. ANÁLISIS DE FOURIER

En este apéndice se presenta un resumen de los conceptos fundamentales del análisis de Fourier.

DESARROLLO EN SERIE DE FOURIER PARA SEÑALES PERIÓDICAS

La determinación del contenido en frecuencias de muchas señales se puede obtener fácilmente disponiendo de unas buenas tablas de integrales. Empezamos considerando las señales periódicas. Cualquier señal periódica se puede expresar como una suma de funciones sinusoidales, denominada serie de Fourier[7]:

$$x(t) = \frac{A_0}{2} + \sum_{n=1}^{\infty} [A_n \cos(2\pi n f_0 t) + B_n \operatorname{sen}(2\pi n f_0 t)]$$

donde f_0 es la inversa del periodo de la señal ($f_0 = 1/T$). La frecuencia f_0 se denomina *frecuencia* o *armónico fundamental*, y los múltiplos de f_0 *armónicos*. Por tanto, una señal periódica con periodo T estará compuesta por la frecuencia fundamental $f_0 = 1/T$, más los múltiplos enteros de dicha frecuencia. Si A_0 es distinto de 0, la señal $x(t)$ tendrá *componente dc* o *continua*.

[7] Los matemáticos normalmente expresan las series y la transformada de Fourier utilizando la variable w_0, con dimensiones de radianes por segundo, siendo $w_0 = 2\pi f_0$. Sin embargo, los físicos e ingenieros prefieren expresarlas en términos de f_0, ya que se simplifican las expresiones, además de que es más intuitivo tener la frecuencia expresada en hertzios en lugar de radianes por segundo.

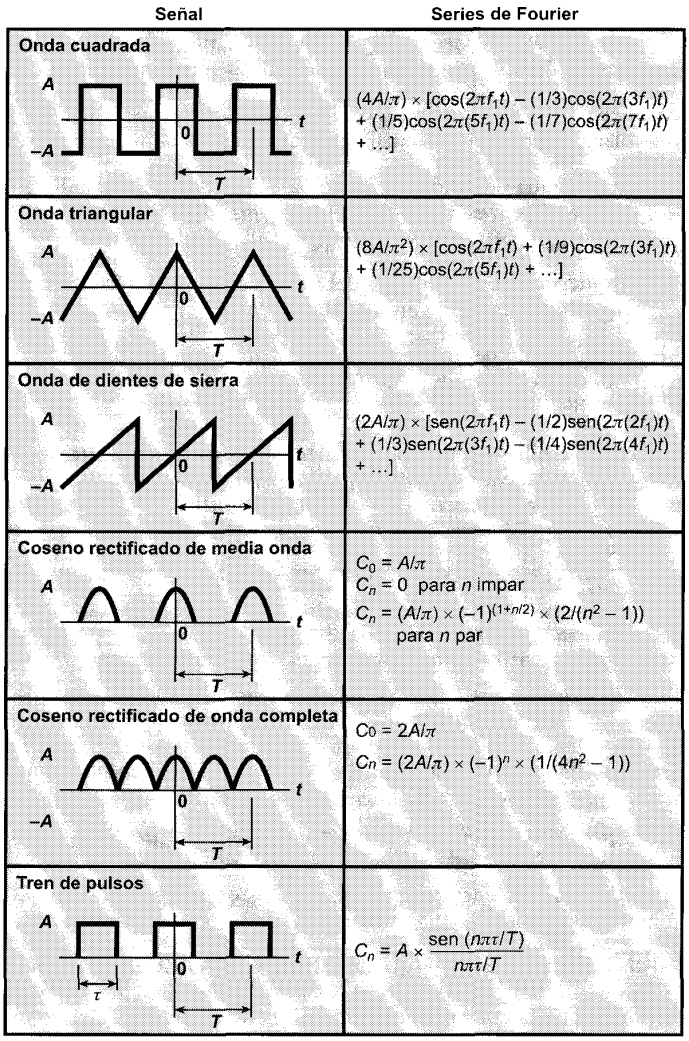


Figura 3.15. Algunos ejemplos típicos de señales periódicas y sus series de Fourier.

Los valores de los coeficientes del desarrollo en serie de Fourier se calculan mediante las siguientes expresiones:

$$A_0 = \frac{2}{T}\int_0^T x(t)\,dt$$

$$A_n = \frac{2}{T}\int_0^T x(t)\,\cos(2\pi n f_0 t)\,dt$$

$$B_n = \frac{2}{T}\int_0^T x(t)\,\text{sen}(2\pi n f_0 t)\,dt$$

Este tipo de representación, denominada representación seno-coseno, es la más sencilla de calcular, si bien, presenta el problema de tener dos componentes para cada frecuencia. Otra representación alternativa a la anterior, denominada representación módulo-fase, adopta la siguiente forma:

$$x(t) = \frac{C_0}{2} + \sum_{n=1}^{\infty} C_n \cos(2\pi n f_0 t + \theta_n)$$

que se relaciona con la representación seno-coseno mediante las expresiones siguientes:

$$C_0 = A_0$$

$$C_n = \sqrt{A_n^2 + B_n^2}$$

$$\theta_n = \tan^{-1}\left(\frac{-B_n}{A_n}\right)$$

En la Figura 3.15 se muestran ejemplos del desarrollo en serie de Fourier para algunas señales periódicas.

TRANSFORMADA DE FOURIER PARA SEÑALES NO PERIÓDICAS

El espectro de una señal periódica, consiste en un conjunto de componentes en frecuencias discretas a la frecuencia fundamental y sus armónicos. Para una señal no periódica, su espectro consiste en un continuo de frecuencias. Este espectro se puede obtener mediante la Transformada de Fourier. Para una señal $x(t)$, con espectro $X(f)$, se verifican las siguientes expresiones:

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft}\, dt$$

$$X(t) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft}\, dt$$

donde $j = \sqrt{-1}$. La aparición del número imaginario en las expresiones anteriores es por razones de comodidad. La componente imaginaria tiene una interpretación física relacionada con la fase de la forma de onda, la explicación de esta interpretación está fuera de los objetivos de este libro.

En la Figura 3.16 se representan algunas señales junto con sus correspondientes transformadas.

DENSIDAD DE POTENCIA ESPECTRAL Y ANCHO DE BANDA

Estrictamente hablando, el ancho de banda de cualquier señal limitada en el tiempo es infinito. No obstante, en la práctica, la mayor parte de la potencia de la señal se concentra en una banda finita, y en ese caso, el ancho de banda efectivo consiste en la porción del espectro que contiene la mayor parte de la potencia. Para una definición más precisa es necesario introducir el concepto de densidad de potencia espectral (PSD, Power Spectral Density). Esencialmente, la PSD describe el contenido en potencias de una señal como función de la frecuencia, tal que representa cuanta potencia hay en las distintas bandas de frecuencia.

Para comenzar, considérese la potencia de la señal en el dominio del tiempo. La función $x(t)$ alude usualmente a una señal en términos de tensión o intensidad. En cualquier caso, la potencia instantánea

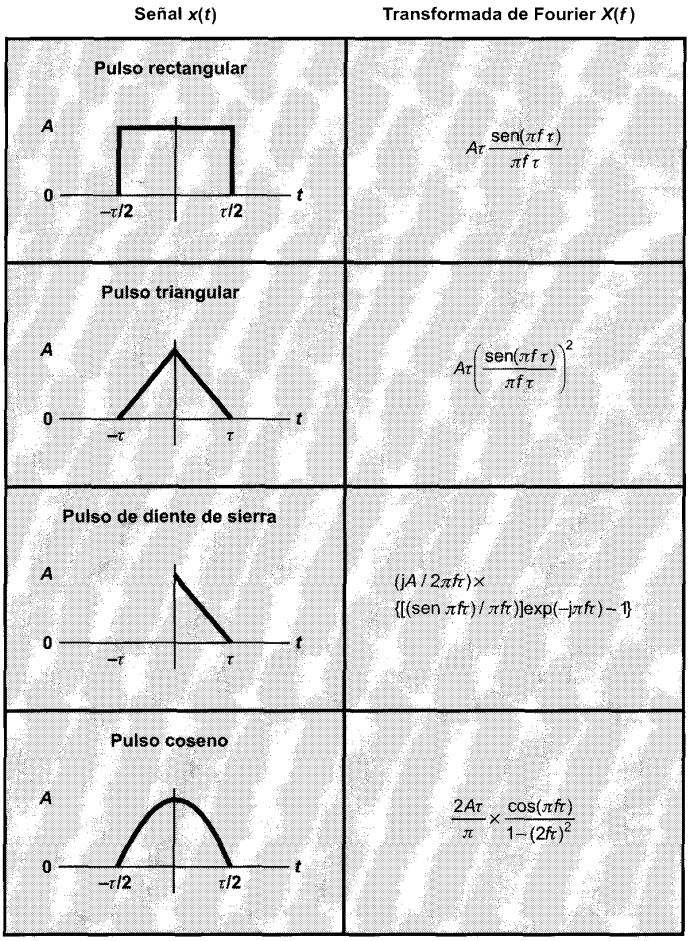


Figura 3.16. Algunas señales no periódicas típicas y sus transformadas de Fourier.

de la señal es proporcional a $|x(t)|^2$. Para una señal limitada en el tiempo se define la potencia media como

$$P = \frac{1}{t_1 - t_2}\int_{t_1}^{t_2} |x(t)|^2\,dt$$

Para el caso de una señal periódica, la potencia media en un periodo viene dada por

$$P = \frac{1}{T}\int_0^T |x(t)|^2\,dt$$

Sería ilustrativo conocer la distribución de la potencia en función de la frecuencia. Esto se puede expresar fácilmente en términos de los coeficientes del desarrollo en serie de Fourier exponencial para

el caso de señales periódicas. En ese caso, la densidad de potencia espectral $S(f)$ es

$$S(f) = \sum_{n=-\infty}^{\infty} |C_n|^2 \delta(f - nf_0)$$

donde f_0 es la inversa del periodo de la señal ($f_0 = 1/T$), C_n es el coeficiente de las series de Fourier en su representación amplitud-fase, y $\delta(t)$ es el impulso unitario o función delta, definida por

$$\delta(t) = \begin{cases} 0 & \text{si } t \neq 0 \\ \infty & \text{si } t = 0 \end{cases}$$

$$\int_{-\infty}^{\infty} \delta(t)\, dt = 1$$

La densidad de potencia espectral $S(f)$ para una señal no periódica es más difícil de definir. Esencialmente, se obtiene definiendo un «periodo» T_0, permitiendo que T_0 aumente sin límite.

Para una función continua $S(f)$, la potencia contenida en la banda de frecuencias definida por $f_1 < f < f_2$, viene dada por

$$P = 2 \int_{f_1}^{f_2} S(f)\, df$$

Si la forma de onda es periódica, la potencia contenida en los j primeros armónicos es

$$P = C_0^2 + \frac{1}{2} \sum_{n=1}^{j} C_n^2$$

Habiendo definido los conceptos anteriores, se está en disposición de definir el denominado ancho de banda de potencia mitad, que quizás sea la definición más usual de ancho de banda. El ancho de banda de potencia mitad se define como el intervalo de frecuencias en el que el valor de la potencia máxima de $S(f)$ decae a la mitad, es decir, 3 dB respecto al valor de pico.

APÉNDICE 3B. DECIBELIOS Y ENERGÍA DE LA SEÑAL

Un parámetro importante en cualquier sistema de transmisión es la energía de la señal transmitida. Al propagarse la señal en el medio, habrá una perdida, o *atenuación*, de energía de la señal. Habrá pérdidas adicionales en conectores, divisores y, en general, cualquier dispositivo pasivo atravesado por la señal. Para compensar este hecho es necesario introducir amplificadores cada cierta distancia que restituyan la energía de la señal.

Los valores de ganancias, pérdidas y en general de todas las magnitudes relativas, se suelen expresar en decibelios, ya que

- La energía de la señal decae, por lo general, logarítmicamente, por lo tanto, las pérdidas se pueden expresar cómodamente en decibelios, ya que es una unidad logarítmica.
- En un sistema de transmisión, las ganancias y pérdidas en cascada, se pueden calcular fácilmente mediante sumas o restas respectivamente.

El decibelio es una medida del cociente o proporción entre dos niveles de la señal:

$$N_{\text{dB}} = 10 \log_{10} \frac{P_2}{P_1}$$

donde

N_{dB} = número de decibelios.

P_1 = potencia de entrada.

P_2 = potencia de salida.

$\log_{10}$ = logaritmo en base 10 (a partir de ahora, se usará log en vez de $\log_{10}$).

La Tabla 3.4 muestra varias potencias de 10 expresadas en decibelios.

Tabla 3.4. Equivalencias en decibelios.

Cociente de potencias	dB	Cociente de potencias	dB
10^1	10	10^{-1}	−10
10^2	20	10^{-2}	−20
10^3	30	10^{-3}	−30
10^4	40	10^{-4}	−40
10^5	50	10^{-5}	−50
10^6	60	10^{-6}	−60

Ejemplo

Si en una línea de transmisión se inserta una señal con una potencia de 10 mW y a cierta distancia se miden 5 mW, la pérdida se puede expresar como

$$N_{dB} = 10 \log (5/10) = 10(-0{,}3) = -3 \text{ dB}$$

Obsérvese que el decibelio es una medida de una diferencia, es decir, una medida relativa, no absoluta. Una pérdida de 1.000 W a 500 W es igualmente una pérdida de 3 dB. Por tanto, una pérdida de 3 dB corresponde a dividir por dos la potencia; de igual manera, una ganancia de 3 dB corresponde a multiplicar por dos la potencia.

El decibelio también se usa para medir diferencias de tensión, ya que la potencia es proporcional al cuadrado de la tensión:

$$P = \frac{V^2}{R}$$

donde

P = potencia disipada en una resistencia R.

V = caída de tensión en la resistencia R.

Por tanto

$$N_{dB} = 10 \log \frac{P_2}{P_1} = 10 \log \frac{V_2^2/R}{V_1^2/R} = 20 \log \frac{V_2}{V_1}$$

Ejemplo

Los decibelios son útiles para determinar la ganancia o pérdida acumuladas por una serie de elementos de transmisión. Suponga un conjunto de elementos atacados por una potencia de entrada de 4 mW, sea

el primer elemento una línea de transmisión con 12 dB de atenuación (− 12 dB), el segundo elemento una amplificador con una ganancia igual a 35 dB, y por último una línea de transmisión con 10 dB de pérdida. La ganancia o atenuación neta será (− 12 + 35 − 10) = 13 dB. El cálculo de la potencia de salida P_2 es,

$$13 = 10 \log (P_2/4\,\text{mW})$$
$$P_2 = 4 \times 10^{1,3}\,\text{mW} = 79{,}8\,\text{mW}$$

Los valores en decibelios se refieren a magnitudes relativas o cambios en magnitud, no a valores absolutos. A veces, es conveniente expresar un nivel absoluto de potencia o tensión en decibelios para facilitar así el cálculo de la pérdida o ganancia. De ahí que haya varias unidades derivadas del decibelio que se usan también frecuentemente.

El dBW (decibelio-watio) se usa frecuentemente en aplicaciones de microondas. Se elige como referencia el valor de 1 W y se define esta referencia igual a 0 dBW. Se define, por tanto, el nivel absoluto de potencia en dBW como

$$\text{Potencia}_{\text{dBW}} = 10 \log \frac{\text{Potencia}_{\text{w}}}{1\,\text{W}}$$

Ejemplo

Una potencia de 1.000 W corresponde a 30 dBW y una potencia de 1 mW corresponde a − 30 dBW.

Una unidad frecuente en los sistemas de televisión por cable y en las aplicaciones LAN de banda ancha es el dBmV (decibelio-milivoltio). Ésta es una medida absoluta, donde 0 dBmV equivale a 1 mV. Por tanto

$$\text{Tensión}_{\text{dBmV}} = 20 \log \frac{\text{Tensión}_{\text{mV}}}{1\,\text{mV}}$$

En la expresión anterior, se ha supuesto que la caída de tensión se realiza en una resistencia de 75 ohmios.

CAPÍTULO 4

Medios de transmisión

- Los medios de transmisión, utilizados para transportar información, se pueden clasificar como guiados y no guiados. Los medios guiados proporcionan un camino físico a través del cual la señal se propaga; entre otros cabe citar al par trenzado, al cable coaxial y la fibra óptica. Los medios no guiados utilizan una antena para transmitir a través del aire, el vacío o el agua.
- Tradicionalmente, el par trenzado ha sido el medio por excelencia utilizado en las comunicaciones de cualquier tipo. Con el cable coaxial se pueden obtener mayores velocidades de transmisión para mayores distancias, por esta razón, el coaxial se ha utilizado en redes de área local de alta velocidad y en aplicaciones de enlaces troncales de alta capacidad. No obstante, la capacidad tremenda de la fibra óptica está desplazando al cable coaxial, copando la mayor parte del mercado de las LAN de alta velocidad y las aplicaciones a larga distancia.
- La difusión por radio, las microondas terrestres y los satélites son las técnicas que se utilizan en la transmisión no guiada. La transmisión por infrarrojos se utiliza en algunas aplicaciones LAN.

En los sistemas de transmisión de datos, el medio de transmisión es el camino físico entre el transmisor y el receptor. Los medios de transmisión se clasifican en guiados y no guiados. En ambos casos, la comunicación se lleva a cabo con ondas electromagnéticas. En los medios guiados las ondas se confinan en un medio sólido, como, por ejemplo, el par trenzado de cobre, el cable de cobre coaxial o la fibra óptica. La atmósfera o el espacio exterior son ejemplos de medios no guiados, que proporcionan un medio de transmisión de las señales pero sin confinarlas; esto se denomina *transmisión inalámbrica*.

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio en sí mismo es lo más importante en la determinación de las limitaciones de transmisión.

En medios no guiados, el ancho de banda de la señal emitida por la antena es más importante que el propio medio a la hora de determinar las características de la transmisión. Una propiedad fundamental de las señales transmitidas mediante antenas es la directividad. En general, a frecuencias bajas las señales son omnidireccionales; es decir, la señal desde la antena se emite y propaga en todas direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional.

En el diseño de sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grandes posibles. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión:

- **El ancho de banda:** si todos los otros factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión se puede incrementar.
- **Dificultades en la transmisión:** las dificultades, como, por ejemplo, la atenuación, limitan la distancia. En los medios guiados, el par trenzado sufre de mayores adversidades que el cable coaxial, que a su vez, es más vulnerable que la fibra óptica.
- **Interferencias:** las interferencias resultantes de la presencia de señales en bandas de frecuencias próximas pueden distorsionar o destruir completamente la señal. Las interferencias son especialmente relevantes en los medios no guiados, pero a la vez son un problema a considerar en los medios guiados. Por ejemplo, frecuentemente múltiples cables de pares trenzados se embuten dentro de una misma cubierta, provocando posibles interferencias, no obstante, este problema se puede reducir utilizando un apantallamiento adecuado.
- **Número de receptores:** un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido, mediante el uso de múltiples conectores. En este último caso, cada uno de los conectores utilizados puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirán.

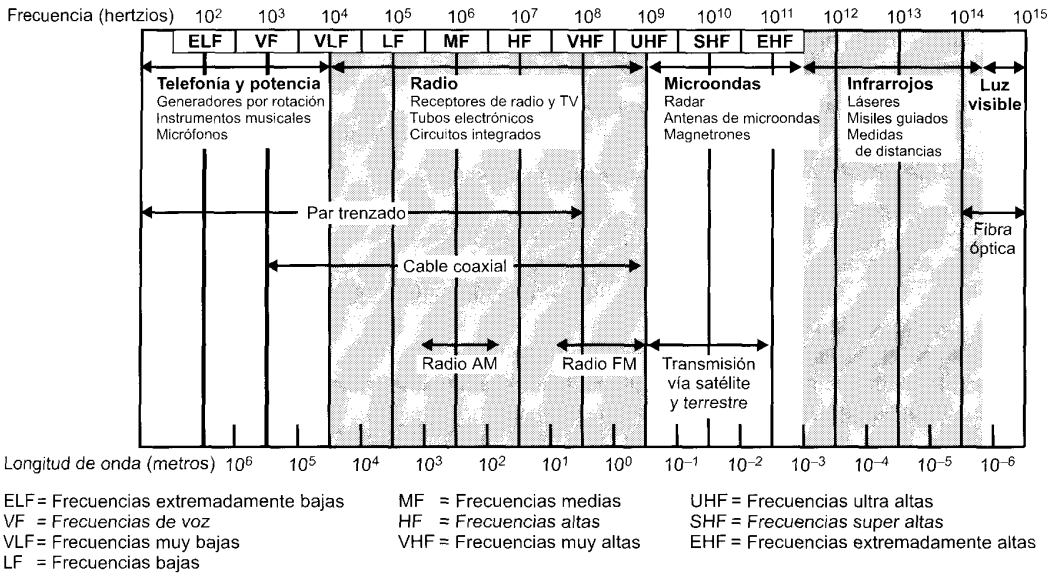


Figura 4.1. Espectro electromagnético para las telecomunicaciones.

En la Figura 4.1 se muestra el espectro electromagnético, así como la frecuencia a la que operan diferentes técnicas de transmisión sobre medios guiados y no guiados. En este capítulo se estudiarán las diferentes alternativas tanto para medios guiados como para no guiados. En todos los casos, se describirán físicamente los sistemas, se discutirán brevemente las aplicaciones y se resumirán las características principales de transmisión.

4.1. MEDIOS DE TRANSMISIÓN GUIADOS

En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia y de si el medio se usa para un enlace punto a punto o por el contrario para un enlace multipunto, como, por ejemplo, en redes de área local (LAN). En la Tabla 4.1 se indican las prestaciones típicas de los medios guiados más comunes para aplicaciones punto a punto de larga distancia. El estudio de la utilización de estos medios en LAN se aplaza para más adelante, en la Parte IV del libro.

Tabla 4.1. Características de transmisión de medios guiados punto a punto [GLOV98].

	Rango de frecuencias	Atenuación típica	Retardo típico	Separación entre repetidores
Par trenzado (con carga)	0 para 3,5 kHz	0,2 dB/km @ 1 kHz	50 μs/km	2 km
Pares trenzados (múltiples cables)	0 para 1 MHz	3 dB/km @ 1 kHz	5 μs/km	2 km
Cable coaxial	0 para 500 MHz	7 dB/km @ 10 MHz	4 μs/km	1 para 9 km
Fibra óptica	180 para 370 THz	0,2 para 0,5 dB/km	5 μs/km	40 km

Los tres medios guiados más utilizados para la transmisión de datos son el par trenzado, el cable coaxial y la fibra óptica (véase Figura 4.2). A continuación examinaremos cada uno de ellos.

PAR TRENZADO

El par trenzado es el medio guiado más económico y a la vez más usado.

Descripción física

El par trenzado consiste en dos de cables de cobre embutidos en un aislante, entrecruzados en forma de espiral. Cada par de cables constituye sólo un enlace de comunicación. Normalmente, se utilizan haces en los que se encapsulan varios pares mediante una envoltura protectora. En aplicaciones de larga distan-

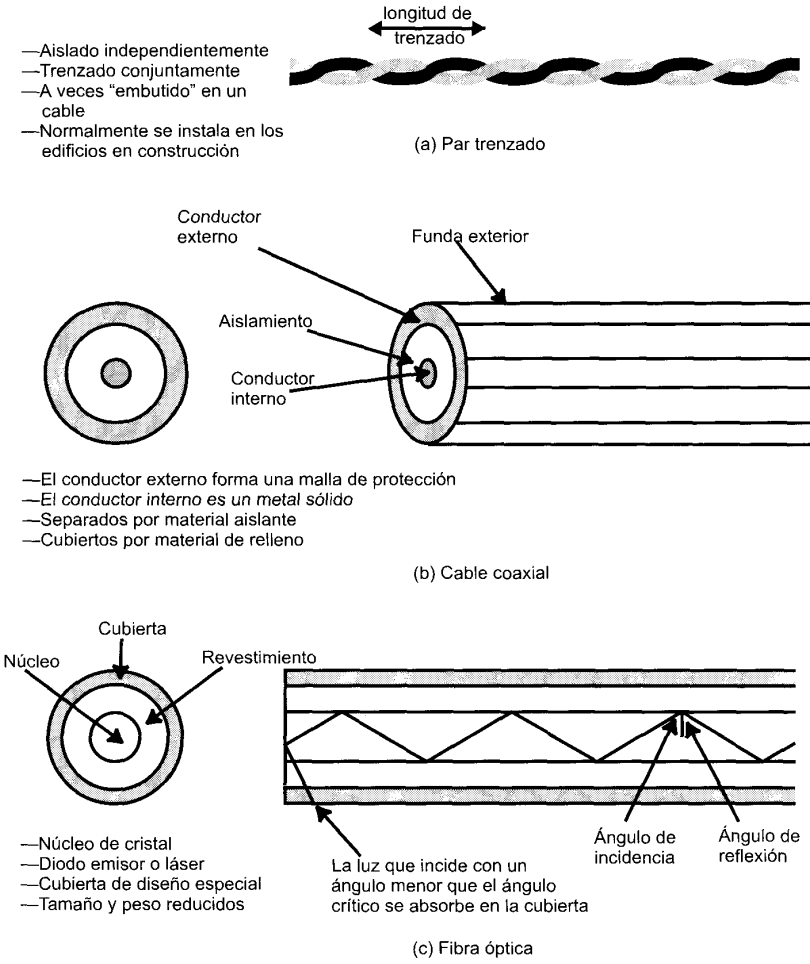


Figura 4.2. Medios de transmisión guiados.

cia, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura protectora se trenzan con pasos de torsión diferentes. Para enlaces de larga distancia, la longitud del trenzado varía entre 5 y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0,4 y 0,9 mm.

Aplicaciones

Tanto para señales analógicas como para señales digitales, el par trenzado es con diferencia el medio de transmisión más usado. Por supuesto es el medio más usado en las redes de telefonía, igualmente su uso es básico en el tendido de redes de comunicación dentro de edificios.

En telefonía, el terminal de abonado se conecta a la central local, también denominada «central final», mediante cable de par trenzado, *denominado bucle de abonado*. Igualmente, dentro de los edificios de oficinas, cada teléfono se conecta a la central privada (PBX, Private Branch Exchange) mediante un par trenzado. Estas instalaciones basadas en pares trenzados, se diseñaron para transportar tráfico de voz mediante señalización analógica. No obstante, con el uso de los modems, esta infraestructura puede utilizarse para transportar tráfico digital a velocidades de transmisión reducidas.

En señalización digital, el par trenzado es igualmente el más utilizado. Generalmente, los pares trenzados se utilizan para las conexiones al conmutador digital o a la PBX digital, con velocidades de 64 kbps. El par trenzado se utiliza también en redes de área local dentro de edificios para la conexión de computadores personales. La velocidad típica en esta configuración está en torno a los 10 Mbps. No obstante, recientemente se han desarrollado redes de área local con velocidades entre 100 Mbps y 1 Gbps mediante pares trenzados, aunque estas configuraciones están bastante limitadas por el número de posibles dispositivos conectados y extensión geográfica de la red. Para aplicaciones de larga distancia, el par trenzado se puede utilizar a velocidades de 4 Mbps o incluso mayores.

El par trenzado es mucho menos costoso que cualquier otro medio de transmisión guiado (cable coaxial y fibra óptica), y a la vez es sencillo de manejar. Ahora bien, comparado con los anteriores está más limitado en términos velocidad de transmisión y de distancia máxima.

Características de transmisión

Los cables de pares se pueden usar para transmitir tanto señales analógicas como señales digitales. Para señales analógicas, se necesitan amplificadores cada 5 o 6 km. Para transmisión digital (usando tanto señales analógicas como digitales), se requieren repetidores cada 2 o 3 km.

Comparado con otros medios guiados (cable coaxial y fibra óptica), el par trenzado permite menores distancias, menor ancho de banda y menor velocidad de transmisión. En la Figura 4.3, se muestra para el par trenzado la fuerte dependencia de la atenuación con la frecuencia. Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido, debido a su fácil acoplamiento con campos electromagnéticos externos. Así, por ejemplo, un cable conductor situado en paralelo con una línea de potencia que conduzca corriente alterna, se verá negativamente afectado por ésta. El ruido impulsivo también afecta a los pares trenzados. Para reducir estos efectos negativos es posible tomar algunas medidas. Por ejemplo, el apantallamiento del cable con una malla metálica reduce las interferencias externas. El trenzado en los cables reduce las interferencias de baja frecuencia, y el uso de distintos pasos de torsión entre pares adyacentes reduce la diafonía.

Para la señalización analógica punto a punto, un par trenzado puede ofrecer hasta 1 MHz de ancho de banda, lo que permite transportar un buen número canales de voz. En el caso de señalización digital punto a punto de larga distancia, se pueden conseguir del orden de unos pocos Mbps; para distancias cortas, actualmente ya hay disponibles productos comerciales que alcanzan los 100 Mbps e incluso 1 Gbps.

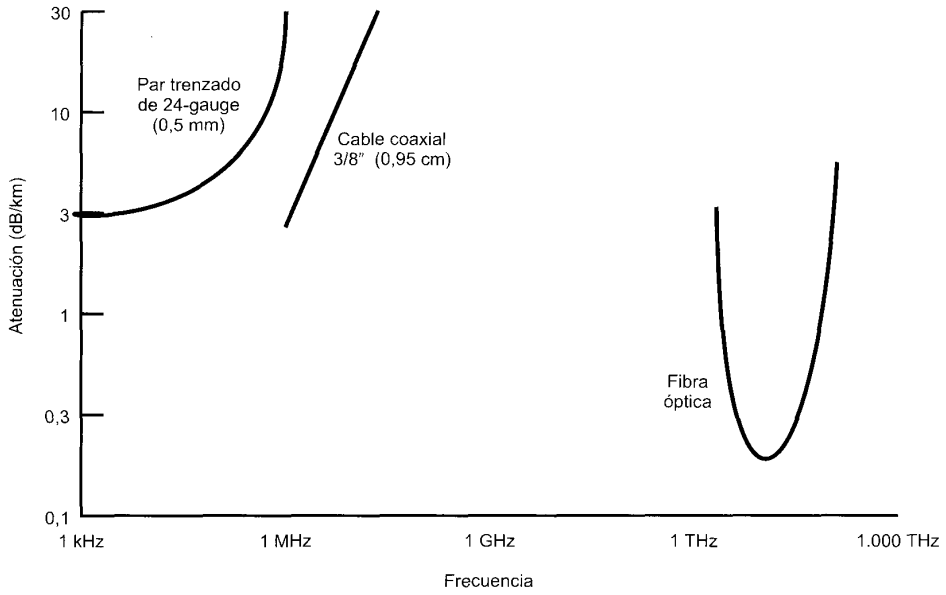


Figura 4.3. Atenuación en los medios guiados típicos.

Pares trenzados apantallados y sin apantallar

Hay dos variantes de pares trenzados: apantallado y sin apantallar. El par trenzado no apantallado (UTP, Unshielded Twisted Pair) es el medio habitual en telefonía. No obstante, actualmente es práctica habitual en el cableado de edificios, muy por encima de las necesidades reales de telefonía. Esto es así ya que hoy por hoy, el par sin apantallar es el menos caro de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y de manipular.

El par trenzado sin apantallar se puede ver afectado por interferencias electromagnéticas externas, incluyendo interferencias con pares cercanos y fuentes de ruido. Una manera de mejorar las características de transmisión de este medio es embutiéndolo dentro de una malla metálica, reduciéndose así las interferencias. El par trenzado apantallado (STP, Shielded Twisted Pair) proporciona mejores resultados a velocidades de transmisión bajas. Ahora bien, este último es más costoso y difícil de manipular que el anterior.

UTP tipo 3 y tipo 5

En la mayoría de los edificios se hace una pre-instalación con un par trenzado de 100 ohmios denominado de calidad telefónica («voice-grade»). Por tanto, este tipo de pre-instalaciones se deben considerar siempre como una alternativa bastante atractiva y poco costosa para las LAN. No obstante, hay que tener en cuenta que las velocidades de transmisión y las distancias que se pueden alcanzar con este medio no siempre cubren las necesidades típicas.

En 1991, la EIA (Electronic Industries Association) publicó el estándar EIA-568, denominado «Commercial Building Telecommunications Cabling Standard», que define el uso de pares trenzados sin apantallar de calidad telefónica y de pares apantallados como medios para aplicaciones de transmisión de datos en edificios. Nótese que por aquel tiempo, las características de dichos medios eran suficientes para el rango de frecuencias y velocidades típicas necesarias en entornos ofimáticos. Es más, en esa

época el objetivo diseño en las LAN tenía velocidades de transmisión comprendidas entre 1 y 16 Mbps. Con el tiempo, los usuarios han migrado tanto a estaciones de trabajo como a aplicaciones de mayores prestaciones. Como consecuencia, ha habido un interés creciente en las LAN que proporcionen hasta 100 Mbps sobre medios no costosos. Como respuesta a esa necesidad, en 1995 se propuso el EIA-568-A. Esta norma incorpora los más recientes avances tanto en el diseño de cables y conectores como en métodos de test. En esta especificación se consideran tanto cables de pares apantallados a 150 ohmios como pares no apantallados de 100 ohmios.

En el estándar EIA-568-A se consideran tres tipos o categorías de cables UTP:

- **Tipo 3:** consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 16 MHz.
- **Tipo 4:** consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 20 MHz.
- **Tipo 5:** consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 100 MHz.

De entre los anteriores, los tipos 3 y 5 son los más utilizados en los entornos LAN. El tipo 3 corresponde a los cables de calidad telefónica que existen en la mayoría de las edificaciones. Con un diseño apropiado y a distancias limitadas, con cables tipo 3 se pueden conseguir velocidades de hasta 16 Mbps. El tipo 5 («data-grade») es un cable de mejores características para la transmisión de datos, y cada vez se está utilizando más y más como pre-instalación en los nuevos edificios de reciente construcción. Con un diseño apropiado y a distancias limitadas, con tipo 5 se pueden alcanzar 100 Mbps.

La diferencia esencial entre los cables tipo 3 y 5 está en el número de trenzas por unidad de distancia. La longitud de la trenza en el tipo 5 es del orden de 0,6 a 0,85 cm, mientras que el tipo 3 tiene una trenza de 7,5 o 10 cm. El trenzado del tipo 5 es por supuesto más caro, ahora bien proporciona prestaciones superiores que el de tipo 3.

En la Tabla 4.2 se resumen las prestaciones de los mencionados cables: UTP tipo 3 y UTP tipo 5, así como el cable STP (Shielded Twisted Pair) especificado en el EIA-568-A. El primer parámetro para establecer la comparativa es la atenuación. Como es sabido la energía de la señal decrece con la distancia recorrida en el medio de transmisión. En medios guiados la atenuación obedece a una ley logarítmica, por tanto, se expresa como un número constante de decibelios por unidad de longitud.

La diafonía que sufren los sistemas basados en pares trenzados es debida a la inducción que provoca un conductor en otro cercano. Por conductor debe entenderse tanto los pares que forman el cable, como los «pines» (patillas metálicas) del conector. Este tipo de diafonía se denomina *cercana al extremo* porque la señal transmitida en el enlace se acopla en un conductor cercano e induce una señal en sentido contrario (es decir, la energía transmitida es capturada por un par de recepción).

Tabla 4.2. Comparación de pares trenzados apantallados y sin apantallar.

	Atenuación (dB por 100 m)			Diafonía en el extremo final (dB)		
Frecuencia (MHz)	**UTP tipo 3**	**UTP tipo 5**	**STP 150 ohmios**	**UTP tipo 3**	**UTP tipo 5**	**STP 150 ohmios**
1	2,6	2,0	1,1	41	62	58
4	5,6	4,1	2,2	32	53	58
16	13,1	8,2	4,4	23	44	50,4
25	—	10,4	6,2	—	41	47,5
100	—	22,0	12,3	—	32	38,5
300	—	—	21,4	—	—	31,3

CABLE COAXIAL

Descripción física

El cable coaxial, al igual que el par trenzado, tiene dos conductores pero está construido de forma diferente para que pueda operar sobre un rango mayor de frecuencias. Consiste en un conductor cilíndrico externo que rodea a un cable conductor (Figura 4.2b). El conductor interior se mantiene a lo largo del eje axial mediante una serie de anillos aislantes regularmente espaciados o bien mediante un material sólido dieléctrico. El conductor exterior se cubre con una cubierta o funda protectora. El cable coaxial tiene un diámetro aproximado entre 1 y 2,5 cm. Debido al tipo de apantallamiento realizado, es decir, a la disposición concéntrica de los dos conductores, el cable coaxial es mucho menos susceptible a interferencias y diafonías que el par trenzado. Comparado con éste, el cable coaxial se puede usar para cubrir mayores distancias, así como para conectar un número mayor de estaciones en una línea compartida.

Aplicaciones

El cable coaxial es quizás el medio de transmisión más versátil, por lo que cada vez más se está utilizado en una gran variedad de aplicaciones. Las más importantes son:

- Distribución de televisión.
- Telefonía a larga distancia.
- Conexión con periféricos a corta distancia.
- Redes de área local.

El cable coaxial se emplea para la distribución de *TV por cable* hasta el domicilio de los usuarios. Diseñado inicialmente para proporcionar servicio de acceso a áreas remotas (CATV, Community Antenna Television), la TV por cable en un futuro muy cercano llegará probablemente a casi tantos hogares y oficinas como el actual sistema telefónico. El sistema de TV por cable puede transportar docenas e incluso cientos de canales a decenas de kilómetros.

Tradicionalmente, el coaxial ha sido fundamental en la red de telefonía a larga distancia, aunque en la actualidad tiene una fuerte competencia en la fibra óptica, las microondas terrestres y las comunicaciones vía satélite. Cuando se usa multiplexación con división en frecuencia (FDM, Frequency Division Multiplexing, véase Capítulo 8), el cable coaxial puede transportar más de 10.000 canales de voz simultáneamente.

El cable coaxial también se usa con frecuencia para conexiones entre periféricos a corta distancias. Con señalización digital, el coaxial se puede usar como medio de transmisión en canales de entrada/salida (E/S) de alta velocidad en computadores.

Características de transmisión

El cable coaxial se usa para transmitir tanto señales analógicas como digitales. Como se puede observar en la Figura 4.3, el cable coaxial tiene una respuesta en frecuencias mejor que la del par trenzado, permitiendo por tanto mayores frecuencias y velocidades de transmisión. Como ya se ha dicho, por construcción el cable coaxial es mucho menos susceptible que el par trenzado tanto a interferencias como a diafonía. Sus principales limitaciones son la atenuación, el ruido térmico, y el ruido de intermodulación. Este último aparece sólo cuando se usan simultáneamente sobre el mismo cable varios canales (FDM) o bandas de frecuencias.

Para la transmisión de señales analógicas a larga distancia, se necesitan amplificadores separados entre sí a distancias del orden de pocos kilómetros, estando más alejados cuanto mayor es la frecuencia de trabajo. El espectro de la señalización analógica se extiende hasta aproximadamente 500 MHz. Para señalización digital, en cambio, se necesita un repetidor aproximadamente cada kilómetro, e incluso menos cuanto mayor sea la velocidad de transmisión.

FIBRA ÓPTICA

Descripción física

La fibra óptica es un medio flexible y fino capaz de confinar un haz de naturaleza óptica. Para construir la fibra se pueden usar diversos tipos de cristales y plásticos. Las pérdidas menores se han conseguido con la utilización de fibras de silicio fundido ultra-puro. Las fibras ultra-puras son muy difíciles de fabricar; las fibras de cristal multicomponente son más económicas, aunque proporcionan unas prestaciones suficientes. La fibra de plástico tiene todavía un coste menor y se pueden utilizar para enlaces de distancias cortas, para los que son aceptables pérdidas moderadamente altas.

Un cable de fibra óptica tiene forma cilíndrica y esta formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta (Figura 4.2c). El *núcleo* es la sección más interna, está constituido por una o varias hebras o fibras muy finas de cristal o plástico y tiene un diámetro entre 8 y 100 μm. Cada fibra está rodeada por su propio *revestimiento*, que no es sino otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación entre el núcleo y el revestimiento actúa como un reflector perfecto confinando el haz de luz que de otra manera escaparía del núcleo. La capa más exterior que envuelve a uno o varios revestimientos es la *cubierta*. La cubierta está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, aplastamientos y otros peligros.

Aplicaciones

Uno de los avances tecnológicos más significativos en la transmisión de datos ha sido el desarrollo de los sistemas de comunicación de fibra óptica. No en vano, la fibra disfruta de una gran aceptación para las telecomunicaciones a larga distancia, y cada vez está siendo más utilizada en aplicaciones militares. Las mejoras constantes en el diseño, junto con sus ventajas inherentes, así como la reducción en costes han contribuido decisivamente para que la fibra sea un medio atractivo en los entornos de red de área local. Las características diferenciales de la fibra óptica frente al cable coaxial y al par trenzado son:

- **Mayor capacidad:** el ancho de banda potencial, y por tanto la velocidad de transmisión, en las fibras es enorme. Experimentalmente se ha demostrado que se pueden conseguir velocidades de transmisión de cientos de Gbps para decenas de kilómetros de distancia. Compárese con el máximo que se puede conseguir en el cable coaxial de cientos de Mbps sobre aproximadamente 1 km, y con los escasos Mbps que se pueden obtener en la misma distancia o con los 100 Mbps a 1 Gbps para pocas decenas de metros en pares trenzados.
- **Menor tamaño y peso:** las fibras ópticas son apreciablemente más finas que el cable coaxial o que los pares trenzados embutidos, por lo menos en un orden de magnitud para capacidades de transmisión comparables. En las conducciones o tubos de vacío previstos para el cableado en las edificaciones, así como en las conducciones públicas subterráneas, la utilización de tamaños pequeños tiene unas ventajas evidentes. La reducción en tamaño lleva a su vez aparejada una reducción en peso que disminuye a su vez la infraestructura necesaria.
- **Atenuación menor:** la atenuación es significativamente menor en las fibras ópticas que en los cables coaxiales y pares trenzados (Figura 4.3), además es constante en un gran intervalo.
- **Aislamiento electromagnético:** los sistemas de fibra óptica no se ven afectados por los efectos de campos electromagnéticos exteriores. Estos sistemas no son vulnerables a interferencias, ruido impulsivo o diafonía. Y por la misma razón, las fibras no radian energía, produciendo interferencias despreciables con otros equipos y proporcionando a la vez un alto grado de privacidad; además, relacionado con esto la fibra es por construcción, difícil de «pinchar».
- **Mayor separación entre repetidores:** cuantos menos repetidores haya el coste será menor, además de haber menos fuentes de error. Desde este punto de vista, las prestaciones de los sistemas de fibra óptica han sido mejoradas de manera constante y progresiva. Para la fibra, es práctica

habitual necesitar repetidores separados entre sí por decenas de kilómetros, e incluso se ha demostrado experimentalmente sistemas con separación de cientos de kilómetros. Por el contrario, los sistemas basados en coaxial y en pares trenzados requieren repetidores cada pocos kilómetros.

Las cinco aplicaciones básicas en las que la fibra óptica es importante son:

- Transmisiones a larga distancia.
- Transmisiones metropolitanas.
- Acceso a áreas rurales.
- Bucles de abonado.
- Redes de área local.

La transmisión a largas distancias mediante fibras es cada vez más común en las redes de telefonía. En estas redes, las distancias medias son aproximadamente 1.500 km y tienen una gran capacidad (normalmente de 20.000 a 60.000 canales de voz). Estos sistemas son competitivos, en cuanto a coste, respecto a los enlaces de microondas y están tan por debajo, en coste, del cable coaxial que en muchos países en vías de desarrollo la fibra está desbancando al coaxial. Paralelamente, la fibra óptica cada vez se utiliza más como medio de transmisión en cables submarinos.

Los circuitos troncales de alcance metropolitano tienen una longitud media de 12 km, y pueden albergar hasta 100.000 canales de voz por cada grupo troncal. La mayoría de los servicios se están instalando usando conducciones subterráneas sin repetidores, que se usan para enlazar centrales telefónicas dentro del área metropolitana. Dentro de esta categoría pertenecen igualmente las rutas que enlazan las líneas de larga distancia de microondas, que llegan hasta las áreas perimetrales de las ciudades, con las centrales de telefonía situadas dentro del casco urbano.

Los accesos troncales a áreas rurales tienen generalmente longitudes que van desde los 40 a 160 km. En Estados Unidos, estos enlaces a su vez conectan frecuentemente centrales telefónicas pertenecientes a diferentes compañías. La mayoría de estos sistemas tienen menos de 5.000 canales de voz. Usualmente, la tecnología utilizada en estas aplicaciones compite con las microondas.

Los bucles de abonado son fibras que van directamente desde las centrales al abonado. El uso de la fibra en estos servicios está empezando a desplazar a los enlaces mediante pares trenzados y coaxiales, dado que cada vez más las redes de telefonía están evolucionando hacia redes integradas capaces de gestionar no sólo voz y datos, sino también imágenes y vídeo. El uso de la fibra en este contexto está encabezado fundamentalmente por grandes clientes (empresas), no obstante la fibra como medio de acceso desde los domicilios particulares aparecerá en un futuro a corto plazo.

Finalmente, una aplicación importante de la fibra óptica está en las redes de área local. Recientemente, se han desarrollado estándares y productos para redes de fibra óptica con capacidades que van desde 100 Mbps hasta 1 Gbps y a su vez permiten cientos, incluso miles de estaciones en grandes edificios de oficinas.

Las ventajas de la fibra óptica respecto del par trenzado o del cable coaxial serán cada vez más convincentes conforme la demanda de información multimedia vaya aumentando (voz, datos, imágenes y vídeo).

Características de transmisión

La fibra óptica propaga el haz de luz internamente de acuerdo con el principio de *reflexión total*. Este fenómeno se da en cualquier medio transparente que tenga un índice de refracción mayor que el medio que lo contenga. En efecto, la fibra óptica funciona como una guía de ondas para el rango de frecuencias que va desde 10^{14} hasta 10^{15} Hz, cubriendo parte del espectro visible e infrarrojo.

En la Figura 4.4 se muestra el principio que rige la propagación del haz de luz en la fibra óptica. La luz proveniente de la fuente penetra en el núcleo cilíndrico de cristal o plástico. Los rayos que inciden

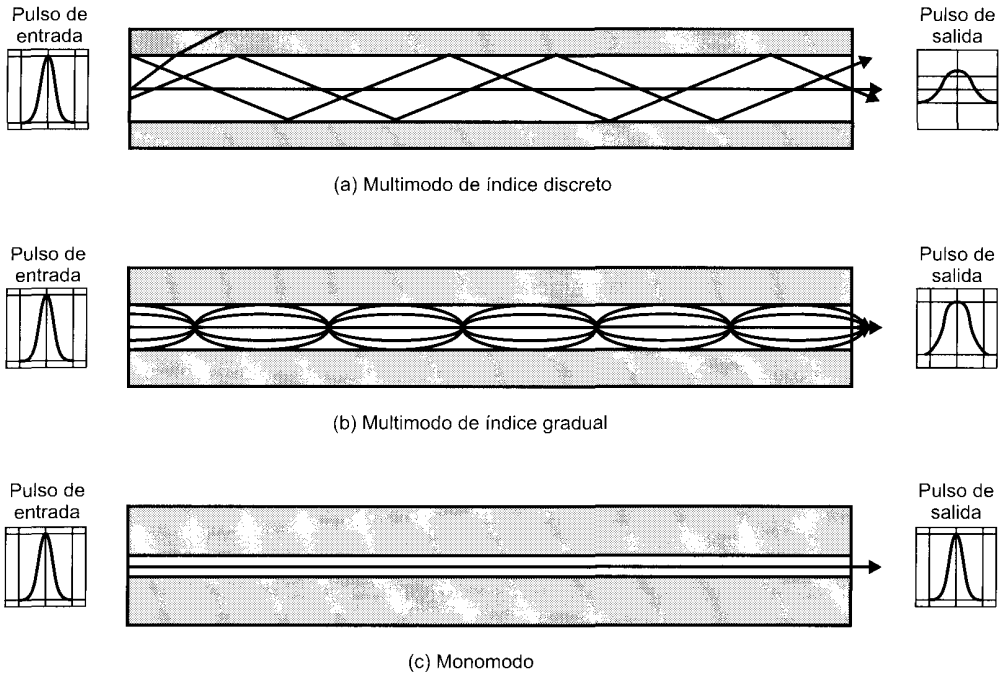


Figura 4.4. Modos de transmisión en las fibras ópticas.

con ángulos superficiales se reflejan y se propagan dentro del núcleo de la fibra, mientras que para otros ángulos, los rayos son absorbidos por el material que forma el revestimiento. Este tipo de propagación se llama **multimodal de índice discreto**, lo que alude al hecho de que hay multitud de ángulos para los que se da la reflexión total. En la transmisión multimodo, existen múltiples caminos que verifican la reflexión total, cada uno con diferente longitud y por tanto con diferente tiempo de propagación. Esto hace que los elementos de señalización que se transmitan (los pulso de luz) se dispersen en el tiempo, limitando la velocidad a la que los datos puedan ser correctamente recibidos. Dicho de otra forma, la necesidad de separar los pulsos de luz limita la velocidad de transmisión de los datos. Este tipo de fibra es más adecuada para la transmisión a distancias cortas. Cuando el radio del núcleo se reduce, la reflexión total se dará en un número menor de ángulos. Al reducir el radio del núcleo a dimensiones del orden de magnitud de la longitud de onda, un solo ángulo o modo podrá pasar: el rayo axial. Esta propagación **monomodo** proporciona prestaciones superiores por las razones que se esgrimen a continuación. Debido a la existencia de un único camino posible en la transmisión monomodo, la distorsión multimodal no puede darse. Las fibras monomodo se utilizan normalmente en aplicaciones de larga distancia, como, por ejemplo, la telefonía y la televisión por cable. Finalmente, se puede conseguir un tercer modo de transmisión variando gradualmente el índice de refracción del núcleo, denominado **multimodo de índice gradual**. Las características de este último modo están entre las de los otros dos modos comentados. Estas fibras, al disponer de un índice de refracción superior en la parte central, hace que los rayos de luz avancen más rápidamente conforme se alejan del eje axial de la fibra. En lugar de describir un zig-zag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la distorsión multimodal. El efecto de la mayor velocidad de propagación en la periferia del núcleo se traduce en que aún recorriendo distancias superiores, todos los rayos llegan aproximadamente en los mismos. Este tipo de fibras de índice gradual se utiliza en las redes de área local.

En los sistemas de fibra óptica se usan dos tipos diferentes de fuentes de luz: los diodos LED (Light Emitting Diode) y los diodos ILD (Injection Laser Diode). Ambos son dispositivos semiconductores que

emiten un haz de luz cuando se les aplica una tensión. El LED es menos costoso, opera en un rango mayor de temperaturas y tienen una vida media superior. El ILD, cuyo funcionamiento está basado en el mismo principio que los láser, es más eficaz y puede proporcionar velocidades de transmisión superiores.

Existe una relación entre la longitud de onda utilizada, el tipo de transmisión y la velocidad de transmisión que se puede conseguir. Tanto el monomodo como el multimodo pueden admitir varias longitudes de onda diferentes y pueden utilizar como fuentes tanto láseres como diodos LED. En las fibras ópticas, la luz se propaga mejor en tres regiones o «ventanas» de longitudes de onda, centradas a 850, 1.300 y 1.500 nanómetros (nm). Todas estas frecuencias están en la zona infrarroja del espectro, por debajo del espectro visible que está situado entre los 400 y 700 nm. Las pérdidas son menores cuanto mayor es la longitud de onda, permitiendo así mayores velocidades de transmisión sobre distancias superiores. En la actualidad la mayoría de las aplicaciones usan como fuentes diodos LED a 850 nm. Aunque esta elección es relativamente barata, su uso está generalmente limitado a velocidades de transmisión por debajo de 100 Mbps y a distancias de pocos kilómetros. Para conseguir mayores velocidades de transmisión y mayores distancias es necesario transmitir en la ventana centrada a 1.300 nm (usando tanto láser como diodos), y si todavía se necesitan mejores prestaciones, entonces hay que recurrir al uso de emisores láser a 1.500 nm.

Multiplexación por división en longitudes de onda

Todo el potencial de la fibra se utiliza plenamente cuando se transmiten varios haces de luz a diferentes frecuencias en la misma fibra. Esto no es sino un tipo de multiplexación por división en frecuencias (FDM), aunque se denomina multiplexación por división en longitudes de onda (Wavelength-Division Multiplexing) (WDM). En WDM, el haz de luz está constituido por multitud de colores, o longitudes de onda, cada uno de los cuales porta un canal diferente de datos. En 1997 se alcanzó un hito cuando en los laboratorios Bell se demostró la viabilidad de un sistema WDM con 100 haces cada uno operando a 10 Gbps, proporcionando una velocidad de transmisión total de un trillón de bits por segundo (también denominado 1 Terabit por segundo o 1 Tbps)[1]. Ya están disponibles en el mercado sistemas con 80 canales a 10 Gbps cada uno.

4.2. TRANSMISIÓN INALÁMBRICA

En medios no guiados, tanto la transmisión como la recepción se lleva a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), y en la recepción la antena capta las ondas electromagnéticas del medio que la rodea. Básicamente en las transmisiones inalámbricas hay dos tipos de configuraciones: direccional y omnidireccional. En la primera, la antena de transmisión emite la energía electromagnética concentrándola en un haz; por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. En el caso omnidireccional, por contra, el diagrama de radiación de la antena es más disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

En el estudio de las comunicaciones inalámbricas, se van a considerar tres rangos de frecuencias. El primer intervalo definido desde los 2 GHz (Gigahertzio = 10^9 Hertzios) hasta los 40 GHz se denomina de frecuencias microondas. En estas frecuencias de trabajo se pueden conseguir haces altamente direccionales, por lo que las microondas son adecuadas para enlaces punto a punto. Las microondas también se usan para las comunicaciones vía satélite. Las frecuencias que van desde 30 MHz a 1 GHz son adecuadas para las aplicaciones omnidireccionales. A este rango de frecuencias lo denominaremos intervalo de ondas de radio. En la Tabla 4.3 se resumen las características[2] de transmisión en medios no guiados para las distintas bandas de frecuencia. Las microondas cubren parte de la banda de UHF y cubren totalmente la banda SHF; la banda de ondas de radio cubre la VHF y parte de la banda UHF.

---

[1] *N. del T.:* Se ha optado por respetar el uso de trillón en el sentido literal del autor (habitual en U.S.A.), diferente al uso europeo.

[2] Los distintos esquemas de modulación se explicarán en el Capítulo 5.

Tabla 4.3. Características de las bandas en comunicaciones no guiadas.

Banda de frecuencia	Nombre	Datos analógicos		Datos digitales		Aplicaciones principales
		Modulación	Ancho de banda	Modulación	Velocidad de transmisión	
30-300 kKHz	LF (frecuencia baja)	Normalmente no se usa		ASK, FSK MSK	0,1 para 100 bps	Navegación
300-3.000 kHz	MF (frecuencia media)	AM	Para 4 kHz	ASK, FSK MSK	10 para 1.000 bps	Radio AM comercial
3-30 MHz	HF (frecuencia alta)	AM, SSB	Para 4 kHz	ASK, FSK MSK	10 para 3.000 bps	Radio de onda corta
30-300 MHz	VHF (frecuencia muy alta)	AM, SSB; FM	5 kHz para 5 MHz	FSK, PSK	Para 100 kbps	Televisión VHF, radio FM comercial
300-3.000 MHz	UHF (frecuencia ultra alta)	FM, SSB	Para 20 MHz	PSK	Para 10 Mbps	Televisión VHF, microondas terrestres
3-30 GHz	SHF (frecuencia súper alta)	FM	Para 500 MHz	PSK	Para 100 Mbps	Microondas terrestres, microondas por satélite
30-300 GHz	EHF (frecuencia extremadamente alta)	FM	Para 1 GHz	PSK	Para 750 Mbps	Enlaces punto a punto cercanos experimentales

Otro rango de frecuencias importante, para las aplicaciones de cobertura local, es la zona de infrarrojos del espectro definida aproximadamente por el rango de frecuencias comprendido entre los 3×10^{11} hasta los 2×10^{14} Hz. Los infrarrojos son útiles para las conexiones locales punto a punto así como para aplicaciones multipunto dentro de áreas de cobertura limitada como, por ejemplo, una habitación.

MICROONDAS TERRESTRES

Descripción física

La antena más común en las microondas es la de tipo parabólico. El tamaño típico es de un diámetro de unos 3 metros. Esta antena se fija rígidamente, y en este caso, el haz estrecho debe estar perfectamente enfocado hacia la antena receptora. Las antenas de microondas se sitúan a una altura apreciable sobre el nivel del suelo, para con ello conseguir mayores separaciones posibles entre ellas y para evitar posibles obstáculos en la transmisión. Si no hay obstáculos intermedios, la distancia máxima entre antenas, verifica

$$d = 7{,}14\sqrt{Kh}$$

donde d es la distancia de separación entre las antenas expresada en kilómetros, h es la altura de la antena en metros, y K es un factor de corrección que tiene en cuenta que las microondas se desvían o refractan con la curvatura de la tierra llegando, por lo tanto, más lejos de lo que lo harían si se propagasen en línea recta. Una buena aproximación es considerar K = 4/3. Por lo tanto, a modo de ejemplo, dos antenas de microondas con altura de 100 metros pueden separarse una distancia igual a $7{,}14 \times \sqrt{133} = 82$ km.

Para llevar a cabo transmisiones a larga distancia, se utiliza la concatenación de enlaces punto a punto entre antenas situadas en torres adyacentes, hasta cubrir la distancia deseada.

Aplicaciones

El uso principal de los sistemas de microondas terrestres son los servicios de telecomunicación de larga distancia, como alternativa al cable coaxial o a las fibras ópticas. Para una distancia dada, las microondas requieren menor número de repetidores o amplificadores que el cable coaxial, pero por contra, necesita que las antenas estén perfectamente alineadas. El uso de las microondas es frecuente en la transmisión de televisión y de voz.

Otro uso cada vez más frecuente es en enlaces punto a punto a cortas distancias entre edificios. En este último caso, aplicaciones típicas son circuitos cerrados de TV o la interconexión de redes locales. Además, las microondas a corta distancia también se utilizan en las aplicaciones denominadas de «by-pass», con las que una determinada compañía puede establecer un enlace privado hasta el centro proveedor de transmisiones a larga distancia, evitando así tener que contratar el servicio a la compañía telefónica local.

Características de transmisión

El rango de las microondas cubre una parte sustancial del espectro electromagnético. La banda de frecuencias está comprendida entre 2 y 40 GHz. Cuanto mayor sea la frecuencia utilizada, mayor es el ancho de banda potencial, y por tanto, mayor es la posible velocidad de transmisión. En la Tabla 4.4 se indican diversos valores de anchos de banda y velocidad de transmisión de datos para algunos sistemas típicos.

Al igual que en cualquier sistema de transmisión, la principal causa de pérdidas en las microondas es la atenuación. Para la microondas (y también para la banda de frecuencias de radio), las pérdidas se pueden expresar como

$$L = 10 \log \left(\frac{4\pi d}{\lambda} \right)^2 \text{ dB}$$

donde d es la distancia y λ es la longitud de onda, expresadas en las mismas unidades. Por tanto, las pérdidas varían con el cuadrado de la distancia. Por contra, en el cable coaxial y el par trenzado, las pérdidas tienen una dependencia logarítmica con la distancia (lineal en decibelios). Por lo tanto, en los sistemas que usan microondas, los amplificadores o repetidores se pueden distanciar más (de 10 a 100 km generalmente) que en coaxiales y pares trenzados. La atenuación aumenta con las lluvias, siendo este efecto especialmente significativo para frecuencias por encima de 10 GHZ. Otra dificultad adicional son las interferencias. Con la popularidad creciente de las microondas, las áreas de cobertura se pueden solapar, haciendo que las interferencias sean siempre un peligro potencial. Así pues la asignación de bandas tiene que realizarse siguiendo una regulación estricta.

Las bandas más usuales en la transmisión a larga distancia se sitúan entre 4 GHz y 6 GHz. Debido a la creciente congestión que están sufriendo estas bandas, la banda de 11 GHz se está empezando a utilizar. La banda de 12 GHz se usa para proporcionar la señal de TV a las cabeceras de distribución de TV por cable, en las que para llegar al abonado se utiliza el cable coaxial. Finalmente, cabe citar que las microondas de altas frecuencias se están utilizando para enlaces cortos punto a punto entre edificios.

Tabla 4.4. Prestaciones de microondas digitales típicos.

Banda (GHz)	Ancho de banda (MHz)	Velocidad de transmisión (Mbps)
2	7	12
6	30	90
11	40	135
18	220	274

Para tal fin, se usa generalmente la banda de 22 GHz. Las bandas de frecuencias superiores son menos útiles para distancias más largas debido a que cada vez la atenuación es mayor, ahora bien, son bastante adecuadas para distancias más cortas. Y además, a frecuencias superiores, las antenas son más pequeñas y más baratas.

MICROONDAS POR SATÉLITE

Descripción física

Un satélite de comunicaciones es esencialmente una estación que retransmite microondas. Se usa como enlace entre dos o más receptores/transmisores terrestres, denominadas estaciones base. El satélite recibe la señal en una banda de frecuencia (canal ascendente), la amplifica o repite, y posteriormente la retransmite en otra banda de frecuencia (canal descendente). Cada uno de los satélites geoestacionarios operará en una serie de bandas de frecuencias llamadas «*transponder channels*» o simplemente «*transponders*».

La Figura 4.5 muestra dos configuraciones usuales en las comunicaciones vía satélite. En la primera de ellas, el satélite se utiliza para proporcionar un enlace punto a punto entre dos antenas terrestres alejadas entre sí. En la segunda, el satélite se usa para conectar una estación base transmisora con un conjunto de receptores terrestres.

Para que un satélite de comunicaciones funcione con eficacia, generalmente se exige que se mantenga en una órbita geoestacionaria, es decir que mantenga su posición respecto de la tierra. Si no fuera así, no estaría constantemente alineado con las estaciones base. El satélite, para mantenerse geoestacionario, debe tener un periodo de rotación igual al de la tierra y esto sólo ocurre a una distancia de 35.784 km.

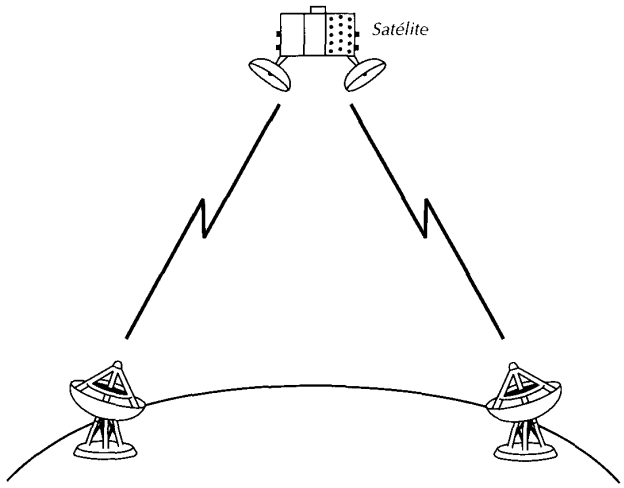
Si dos satélites utilizaran la misma banda de frecuencias y estuvieran suficientemente próximos, podrían interferir mutuamente. Para evitar esto, los estándares actuales exigen una separación mínima de 4° (desplazamiento angular medido desde la superficie terrestre) en la banda 4/6 GHz, y una separación de al menos 3° a 12/14 GHz. Por lo tanto, el número máximo de posibles satélites está bastante limitado.

Aplicaciones

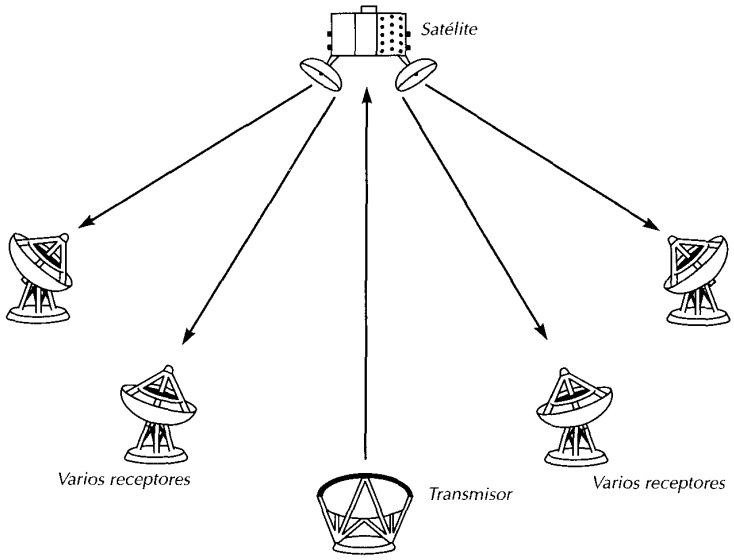
Las comunicaciones vía satélite han sido una revolución tecnológica de igual magnitud que la desencadenada por la fibra óptica. Entre las aplicaciones más importantes para los satélites cabe destacar:

- La difusión de televisión.
- La transmisión telefónica a larga distancia.
- Las redes privadas.

Debido a que los satélites son multidestino por naturaleza, su utilización es muy adecuada para la distribución de TV, por lo que están siendo ampliamente utilizados tanto en los Estados Unidos como en el resto del mundo. Tradicionalmente, en la distribución de TV una emisora local proporciona la programación a toda la red. Para lo cual los programas se transmiten al satélite que es el encargado de difundirlo a toda una serie de estaciones receptoras, las cuales redistribuyen la programación a los usuarios finales. La PBS (Public Broadcasting Service) es una red que distribuye su programación casi exclusivamente mediante el uso de los canales de satélite. Otras redes comerciales también utilizan el satélite como parte esencial de su sistema, e igualmente, cada vez más los sistemas de distribución de la TV por cable utilizan el satélite como medio de obtener su programación. La aplicación más reciente de la tecnología del satélite a la televisión es la denominada difusión directa vía satélite (DBS, Direct Broadcast Satellite), en la que la señal de vídeo se transmite directamente desde el satélite a los domicilios de los usuarios. La disminución tanto en coste como en tamaño de las antenas receptoras han hecho que esta tecnología sea factible económicamente, con lo que el número de canales disponibles es cada vez mayor.



(a) Enlaces punto a punto de microondas vía satélite



(b) Enlaces de difusión de microondas vía satélite

Figura 4.5. Distintas configuraciones de comunicaciones vía satélite.

La transmisión vía satélite se utiliza también para proporcionar enlaces punto a punto entre las centrales telefónicas en las redes públicas de telefonía. Es el medio óptimo para los enlaces internacionales que tengan un alto grado de utilización y es competitivo comparado con los sistemas terrestres en muchos enlaces internacionales de larga distancia.

Finalmente, para la tecnología vía satélite hay una gran cantidad de aplicaciones de gran interés comercial. El suministrador del servicio de transmisión vía satélite puede dividir la capacidad total dis-

ponible en una serie de canales, alquilando su uso a terceras compañías. Dichas compañías, equipadas con una serie de antenas distribuidas en diferentes localizaciones pueden utilizar un canal del satélite para establecer una red privada. Tradicionalmente, tales aplicaciones eran bastante caras, estando limitado su uso a grandes empresas. Un desarrollo reciente ha sido el sistema de terminales de pequeña abertura (VSAT, Very Small Aperture Terminal), que constituye una alternativa de bajo coste. En la Figura 4.6 se muestra una configuración VSAT típica, consistente en una serie de estaciones equipadas con una antena de VSAT de bajo coste. Mediante el uso de algún procedimiento regulador, estas estaciones compartirán la capacidad del canal del satélite para transmitir a la estación central o concentrador. Esta estación puede intercambiar información con cada uno de los abonados y puede a su vez retransmitir los mensajes a otras estaciones.

Características de transmisión

El rango de frecuencias óptimo para la transmisión vía satélite está en el intervalo comprendido entre 1 y 10 GHz. Por debajo de 1 GHZ, el ruido producido por causas naturales es apreciable, incluyendo el

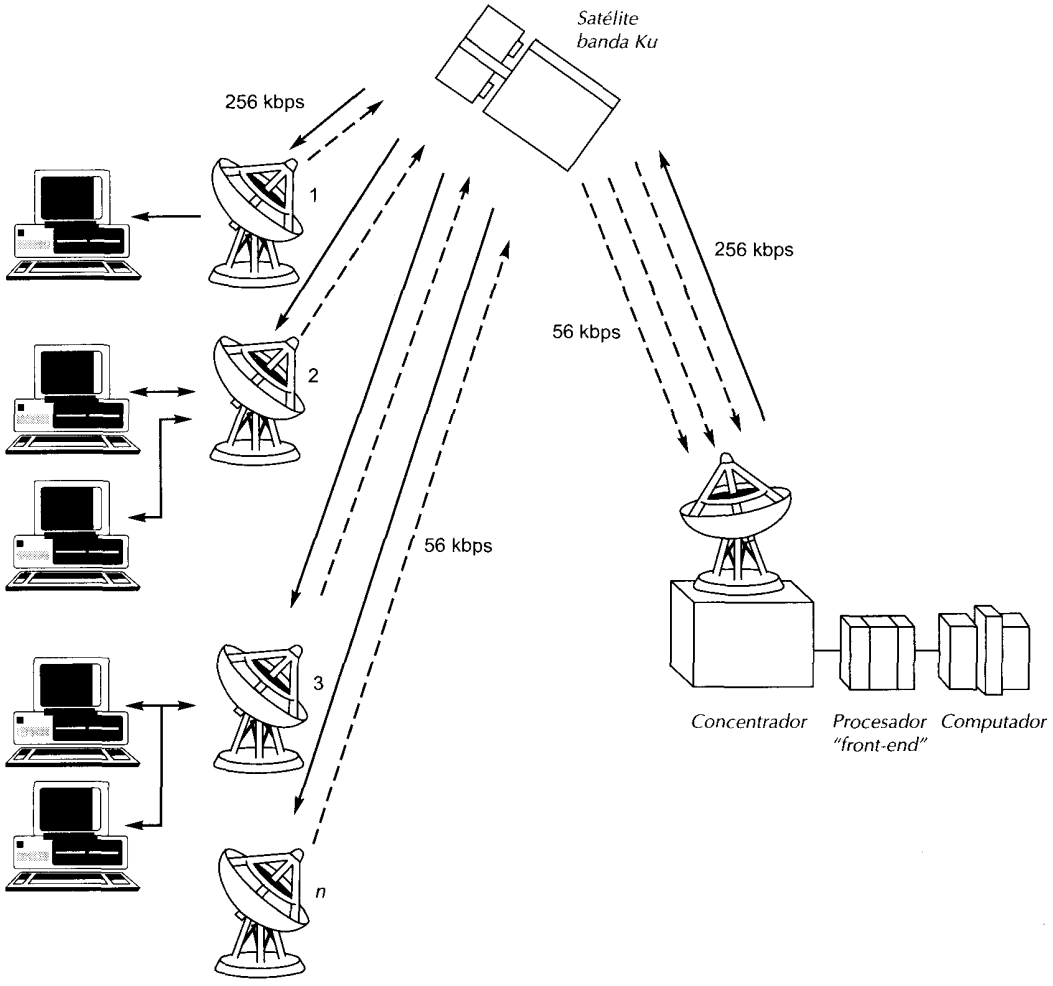


Figura 4.6. Configuración VSAT.

ruido galáctico, solar, atmosférico y el producido por interferencias con otros dispositivos electrónicos. Por encima de los 10 GHz, la señal se ve severamente afectada por la absorción atmosférica y por las precipitaciones.

La mayoría de los satélites que proporcionan servicio de enlace punto a punto operan en el intervalo entre 5,925 y 6,425 GHz para la transmisión desde las estaciones terrestres hacia el satélite (canal ascendente) y entre 3,7 y 4,2 GHz para la transmisión desde el satélite hasta la tierra (canal descendente). Esta combinación se conoce como banda 4/6 GHz. Nótese que las frecuencias ascendentes son diferentes de las descendentes. En una transmisión continua y sin interferencias, el satélite no podrá transmitir y recibir en el mismo rango de frecuencias. Así pues, las señales que se reciben desde las estaciones terrestres en una frecuencia dada se deberán devolver en otra distinta.

La banda 4/6 GHz está dentro de la zona óptima de frecuencias (de 1 a 10 GHz), ahora bien su utilización exhaustiva ha llegado a la saturación. Debido a posibles interferencias (por ejemplo, con microondas terrestres operando en ese mismo rango), las restantes frecuencias del intervalo óptimo no se pueden utilizar. Por tanto, se han desarrollado otras bandas alternativas como es la 12/14 GHz (el canal ascendente está situado entre 14 y 14,5 GHz, y la banda descendente está entre 11,7 a 14,2 Ghz). En esta banda aparecen problemas de atenuación que se deben solventar. No obstante, se pueden usar receptores terrestres más baratos y de dimensiones más reducidas. Se ha diagnosticado que esta banda también se saturará, por lo que se está proyectando la utilización de la banda 19/29 GHz (enlace ascendente: desde 27,5 a 31,0 GHz; enlace descendente: de 17,7 a 21,2 GHz). En esta banda la atenuación es incluso superior, ahora bien, por contra proporcionará un ancho de banda mayor (2.500 MHz comparados con los 500 MHz anteriores), a la vez que los receptores pueden ser todavía más pequeños y económicos.

Merecen comentarse algunas propiedades peculiares de las comunicaciones vía satélite. En primer lugar, debido a las grandes distancia involucradas, hay un retardo de propagación aproximado del orden de un cuarto de segundo para la transmisión desde una estación terrestre hasta otra pasando por el satélite. Este retardo es apreciable si se trata de una conversación telefónica ordinaria. Pero además, estos retrasos introducen problemas adicionales a la hora de controlar los errores y el flujo en la transmisión. Estos problemas serán estudiados en capítulos posteriores. En segundo lugar, los satélites con microondas son intrínsecamente un medio para aplicaciones multidestino. Varias estaciones pueden transmitir hacia el satélite, e igualmente varias estaciones pueden recibir la señal transmitida por el satélite.

ONDAS DE RADIO

Descripción física

La diferencia más apreciable entre las microondas y las ondas de radio es que estas últimas son omnidireccionales, mientras que las primeras tienen un diagrama de radiación mucho más direccional. Por lo tanto, las ondas de radio no necesitan antenas parabólicas, ni necesitan que dichas antenas estén instaladas sobre una plataforma rígida para estar alineadas.

Aplicaciones

Con el término *radio* se alude de una manera poco precisa a todas la banda de frecuencias desde 3 kHz a 300 GHz. Aquí de una manera informal se está utilizando el término *ondas de radio* para aludir a la banda VHF y parte de la UHF: de 30 MHz a 1GHz. Este rango cubre la radio comercial FM así como televisión UHF y VHF. Este rango también se utiliza para una serie de aplicaciones de redes de datos.

Características de transmisión

El rango de frecuencias comprendido entre 30 MHz y 1GHz es muy adecuado para la difusión simultánea a varios destinos. A diferencia de las ondas electromagnéticas con frecuencias menores, la ionosfera es transparente para ondas con frecuencias superiores a 30 MHz. Así pues, la transmisión es posible

cuando las antenas están alineadas, no produciéndose interferencias entre los transmisores debidas a las reflexiones con la atmósfera. A diferencia de la región de las microondas, las ondas de radio son menos sensibles a la atenuación producida por la lluvia.

Como en el caso anterior donde la transmisión sigue una línea recta, en este caso también se verifica la Ecuación (4.1); es decir, la distancia máxima entre el transmisor y el receptor es ligeramente mayor que el alcance visual, es decir, $7{,}14\sqrt{Kh}$. Al igual que en las microondas, la atenuación debida simplemente a la distancia verifica la Ecuación (4.2), es decir, $10\log\left(\frac{4\pi d}{\lambda}\right)^2$. Debido a que tienen una longitud de onda mayor, las ondas de radio sufren, en términos relativos, una atenuación menor.

Un factor determinante en las ondas de radio son las interferencias por multitrayectorias. Entre las antenas, debido a la reflexión en la superficie terrestre, el mar u otros objetos, pueden aparecer multitrayectorias. Este efecto se observa con frecuencia en el receptor de TV y consiste en que se pueden observar varias imágenes (o sombras) cuando pasa un avión por el espacio cercano.

INFRARROJOS

Las comunicaciones mediante infrarrojos se llevan a cabo mediante transmisores/receptores («transceivers») que modulan luz infrarroja no coherente. Los transceivers deben estar alineados bien directamente o mediante la reflexión en una superficie coloreada como puede ser el techo de una habitación.

Una diferencia significativa entre la transmisión de rayos infrarrojos y las microondas es que los primeros no pueden atravesar las paredes. Por tanto, los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este tipo de transmisión. Es más, no hay problemas de asignación de frecuencias, ya que en esta banda no se necesitan permisos.

4.3. LECTURAS Y SITIOS WEB RECOMENDADOS

En [FREE98] se puede encontrar una descripción detallada de las características de transmisión de los medios citados en este capítulo. En [REEV95] se realiza un excelente estudio de los pares trenzados y de las fibras ópticas. [BORE97] es un tratado completo sobre los componentes de la transmisión sobre fibra óptica. Otro artículo de calidad sobre el tema es [WILL97]. En [STAL97] se discute con más detalle las características de los medios de transmisión en LAN.

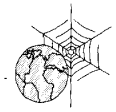
BORE97 Borella, M., *et al.* «Optical Components for WDM Lightware Networks.» *Proceeding of the IEEE*, August 1997.

FREE98 Freeman, R. *Telecommunication Transmission Handbook.* New York: Wiley, 1991.

REEV95 Reeve, W. *Subscriber Loop Signaling and Transmission Handbook.* Piscataway, NJ: IEEE Press, 1995.

STAL97 Stallings, W. *Local and Metropolitan Area Networks, Fifth Edition.* Englewood Cliffs, NJ: Prentice Hall, 1997.

WILL97 Willner, A. «Mining the Optical Bandwidth for a Terabit per Second.» *IEEE Spectrum*, April 1997.



SITIOS WEB RECOMENDADOS

- **«Mobile and Wireless Computing Index»:** información sobre las tecnologías inalámbricas, productos, congresos y publicaciones.

- **BICSI (Building Industry Consulting International) Resource Library:** incluye artículos sobre las premisas de las especificaciones de cableado, cables tipo 5 y cuestiones relacionadas.

4.4. PROBLEMAS

4.1. Supóngase que unos datos se almacenan en disquetes de 1,4 Mbytes que pesan 30 g cada uno. Supóngase que una compañía aérea transporta 10^4 kg de disquetes a una velocidad de 1.000 km/h sobre una distancia de 5.000 km. ¿Cuál es la velocidad de transmisión en bits por segundo de este sistema?

4.2. Sea una línea telefónica caracterizada por una pérdida de 20 dB. La potencia de la señal a la entrada es de 0,5 vatios, y el nivel del ruido a la salida es de 4,5 μvatios. Calcular la relación señal ruido para la línea en dB.

4.3. Dada una fuente de 100 vatios, determinar la máxima longitud alcanzable en los siguientes medios de transmisión, si la potencia a recibir es 1 vatio:

a) Un par trenzado de 24 gauges a 300 kHz.

b) Un par trenzado de 22 gauges a 1 MHz.

c) Un cable coaxial de 1 cm a 1 MHz.

d) Un cable coaxial de 1 cm a 25 MHz.

e) Una fibra óptica trabajando a su frecuencia óptima.

4.4. Un cable coaxial es un sistema de transmisión con dos conductores. ¿Qué ventaja tiene conectar la malla a tierra?

4.5. Demostrar que duplicando la frecuencia de transmisión o duplicando la distancia entre las antenas de transmisión y recepción se atenúa la potencia recibida en 6 dB.

4.6. La profundidad en el océano a la que se detectan las señales electromagnéticas aéreas, crece con la longitud de onda. Por tanto, los militares determinaron que usando longitudes de onda muy grandes, correspondientes a 30 Hz, podrían comunicarse con cualquier submarino alrededor del mundo. La longitud de las antenas es deseable que sea del orden de la mitad de la longitud de onda. ¿Cuál debería ser la longitud típica de las antenas para operar a esas frecuencias?

4.7. La potencia de la señal de voz está concentrada en torno a los 300 Hz. Las antenas para transmitir esta frecuencia deberían tener un tamaño enormemente grande, esto hace que para transmitir voz por radio, la señal debe enviarse modulando una señal de frecuencia superior (portadora) para que la antena correspondiente tenga un tamaño menor.

a) ¿Cuál sería la longitud de una antena equivalente a la mitad de la longitud de onda para enviar señal de 300 Hz?

b) Una posible alternativa es emplear un esquema de modulación, como los descritos en el Capítulo 5, de tal manera que la señal a transmitir tenga un ancho de banda estrecho centrado en torno a la frecuencia portadora. Supóngase que quisiéramos una antena de 1 metro de longitud. ¿Qué frecuencia de portadora debería utilizarse?

4.8. Hay leyendas sobre gente que es capaz de recibir la señal de radio a través de los nervios de los dientes. Supóngase que tiene un nervio de 2,5 mm (0,0025 m) de largo que actuara a modo de antena, siendo igual en longitud a la mitad de la longitud de onda. ¿Qué frecuencia recibiría?

CAPÍTULO 5

Codificación de datos

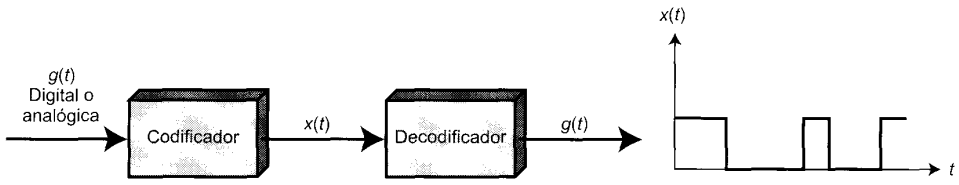
- Tanto la información analógica como la digital pueden ser codificadas mediante señales analógicas o digitales. La elección de un tipo particular de codificación dependerá de los requisitos exigidos, del medio de transmisión, así como de los recursos disponibles para la comunicación.
- Datos digitales, señales digitales: la forma más sencilla de codificar digitalmente datos digitales es asignar un nivel de tensión al uno binario y otro distinto para el cero. Para mejorar las prestaciones es posible utilizar otros códigos distintos al anterior, alterando el espectro de la señal y proporcionando capacidad de sincronización.
- Datos digitales, señales analógicas: los modems convierten los datos digitales en señales analógicas de tal manera que se puedan transmitir a través de líneas analógicas. Las técnicas básicas son desplazamiento de amplitud (ASK, Amplitude-Shift Keying), desplazamiento de frecuencia (FSK, Frecuency-Shift Keying), y desplazamiento de fase (PSK, Phase-Shift Keying). En todas ellas, para representar los datos digitales se modifican uno o más parámetros característicos de la señal portadora.
- Datos analógicos, señales digitales: los datos analógicos, como, por ejemplo, voz y vídeo, se digitalizan para ser transmitidos mediante sistemas digitales. La técnica más sencilla es la modulación por codificación de impulsos (PCM, Pulse Code Modulation), que implica un muestreo periódico de los datos analógicos y una cuantización de las muestras.
- Datos analógicos, señales analógicas: los datos analógicos se modulan mediante una portadora para generar una señal analógica en una banda de frecuencias diferente, que se puede utilizar en un sistema de transmisión analógico. Las técnicas básicas son modulación en amplitud (AM, Amplitude Modulation), modulación en frecuencia (FM, Frequency Modulation), y modulación en fase (PM, Phase Modulation).

En el Capítulo 3 se hizo una diferenciación entre lo que son datos analógicos o digitales y lo que son señales analógicas o digitales. En la Figura 3.11 se comentó que ambos tipos de datos se pueden codificar usando cualquiera de los dos tipos de señales.

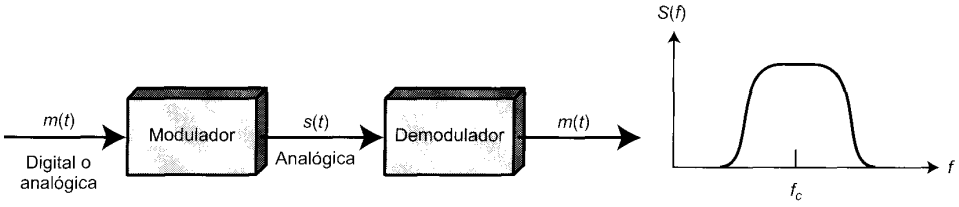
La Figura 5.1 es otro gráfico que enfatiza todos los procesos involucrados. En la **señalización digital**, una fuente de datos $g(t)$, que puede ser tanto analógica como digital, se codifica en una señal digital $x(t)$. La forma de onda en particular que adopte $x(t)$ dependerá de la técnica de codificación elegida, y se elegirá intentando optimizar el uso del medio de transmisión. Por ejemplo, la codificación se puede elegir intentando minimizar el ancho de banda o se puede elegir para minimizar la tasa de errores.

La **transmisión analógica** se basa en una señal continua de frecuencia constante denominada *portadora*. La frecuencia de la portadora se elige de forma tal que sea compatible con las características del medio que se vaya a utilizar. Los datos se pueden transmitir modulando la señal portadora. La modulación es el proceso de codificar los datos generados por la fuente, en la señal portadora de frecuencia f_c. Todas las técnicas de modulación implican la modificación de uno o más de los tres parámetros fundamentales en el dominio de la frecuencia de la portadora: amplitud, frecuencia y fase.

La señal de entrada $m(t)$ (que puede ser tanto analógica como digital) se denomina señal moduladora o también señal en banda base. A la señal resultante de la modulación de la señal portadora se denomina señal modulada $s(t)$. Como se indica en la figura 5.1b, $s(t)$ es una señal limitada en banda (pasabanda). La localización del ancho de banda asignado está relacionada con f_c, estando usualmente centrado en torno a ésta. De nuevo, el procedimiento de codificación se elegirá para optimizar algunas de las características de la transmisión.



(a) Codificación sobre una señal digital



(b) Modulación sobre una señal analógica

Figura 5.1. Técnicas de codificación y modulación.

Las cuatro posibles combinaciones, mostradas en la Figura 5.1, se utilizan con frecuencia; si bien, las razones por las que se elige una u otra pueden ser de diversa índole, como las que se indican a continuación:

- **Datos digitales, señales digitales:** en términos generales, el equipamiento para la codificación digital usando señales digitales es menos complicado y menos costoso que el equipamiento necesario para transmitir datos digitales con señales analógicas mediante modulación.
- **Datos analógicos, señales digitales:** la conversión de los datos analógicos en digital permite la utilización de las técnicas más recientes de equipos de conmutación para la transmisión digital. Las ventajas de la aproximación digital se describieron en la Sección 3.2.
- **Datos digitales, señales analógicas:** algunos medios de transmisión, como, por ejemplo, la fibra óptica y los medios no guiados, sólo permiten la propagación de señales analógicas.
- **Datos analógicos, señales analógicas:** los datos analógicos de naturaleza eléctrica se pueden transmitir fácilmente y de una forma poco costosa en banda base. Esto por ejemplo es lo que se hace para la transmisión de voz en las líneas de calidad telefónica. La modulación se usa frecuentemente para desplazar el ancho de banda de la señal en banda base hacia otra zona del espectro. De esta manera se permite que varias señales, cada una en una posición diferente del espectro, compartan el mismo medio de transmisión. Este procedimiento se denomina multiplexación por división en frecuencias.

A continuación se examinarán las técnicas involucradas en las cuatro combinaciones anteriores, y posteriormente se estudiarán las técnicas de espectro expandido.

5.1. DATOS DIGITALES, SEÑALES DIGITALES

Una señal digital es una secuencia de pulsos de tensión discretos y discontinuos, donde cada pulso es un elemento de señal. Los datos binarios se transmiten codificando cada bit de datos en cada elemento de

señal. En el caso más sencillo, habrá una correspondencia uno a uno entre los bits y dichos elementos. En la Figura 3.13 se muestra un ejemplo, en el que un 0 binario se representa mediante un nivel bajo de tensión y un 1 binario se representa por un nivel de tensión mayor. En esta sección se demostrará que hay una gran cantidad de alternativas a la codificación mostrada en la figura mencionada.

Antes de nada se va a introducir un poco de terminología. Si todos los elementos de señal tienen el mismo signo algebraico (es decir, si son todos positivos o todos negativos) la señal es unipolar. En una señal polar, por el contrario, un estado lógico se representará mediante un nivel positivo de tensión y el otro, mediante un nivel negativo. La razón de datos de una señal, o simplemente la velocidad de transmisión de una señal, es la velocidad expresada en bits por segundo, a la que se transmiten los datos. La duración o longitud de un bit se define como el tiempo empleado en el transmisor para emitir un bit; para una velocidad de transmisión R, la duración de un bit es $1/R$. La velocidad de modulación, por el contrario, es la velocidad a la que cambia el nivel de la señal, que como se explicará más adelante, dependerá del esquema de codificación elegido. La velocidad de modulación se expresa en baudios, que equivale a un elemento de señal por segundo. Para concluir, por razones históricas se usan los términos *marca* y *espacio*, aludiendo a los dígitos binarios 1 y 0 respectivamente. En la Tabla 5.1 se resume la terminología aquí introducida, que se aclarará posteriormente en esta sección mediante un ejemplo.

Las tareas involucradas al interpretar las señales digitales en el receptor se pueden resumir de nuevo considerando la Figura 3.13. En primer lugar el receptor debe conocer o determinar la duración de cada bit. Es decir, el receptor con mayor o menor precisión debe conocer cuando comienza y acaba cada bit. En segundo lugar el receptor debe determinar si el nivel para cada bit es alto (1) o bajo (0). En la Figura 3.13, estas tareas se realizan muestreando a la mitad del intervalo temporal que ocupa cada bit, y comparando el valor obtenido con un umbral. Debido a la existencia de errores y otros defectos, puede que haya errores como se mostrará posteriormente.

¿Qué factores determinan el éxito o el fracaso del receptor al interpretar la señal de entrada? Ya se vio en el Capítulo 3 que hay tres factores importantes: la relación señal ruido (o mejor E_b/N_0), la velocidad de transmisión y el ancho de banda. Si se suponen los otros factores constantes, se pueden establecer las siguientes afirmaciones:

- Un incremento de la velocidad de transmisión aumentará la tasa de errores por bit (BER, Bit Error Rate)[1].

Tabla 5.1. Terminología básica en transmisión de datos.

Término	Unidades	Definición
Datos	Bits	Un uno o cero binario
Velocidad de transición	Bits por segundo (bps)	Velocidad a la que se transmiten los datos
Elemento de señalización	Digital: un pulso de tensión de amplitud constante. Analógico: un pulso de frecuencia, fase y amplitud constantes	Aquella parte de la señal que ocupa el intervalo más corto correspondiente a un código de señalización
Velocidad de señalización o modulación	Número de elementos de señalización por segundo (baudios).	Velocidad a la que se transmiten los elementos de señalización

[1] El BER es la medida más habitual para determinar la cantidad de errores en toda línea de transmisión de datos, y se define como la probabilidad de que un bit se reciba erróneamente. También se *denomina fracción de errores por bit*. Este último término es más esclarecedor, ya que el término *tasa* se refiere típicamente a una cantidad que varía con el tiempo. Desgraciadamente, la mayoría de los libros y documentos de normalización consideran a la R de BER como *Rate (tasa)*.

- Un aumento en la relación SNR reduce la tasa de errores por bit.
- Un incremento del ancho de banda permite un aumento en la razón de datos.

Hay otro factor que se puede utilizar para mejorar las prestaciones del sistema, y éste no es otro que el propio esquema de codificación. El esquema de codificación es simplemente la correspondencia que se establece entre los bits de los datos con los elementos de señal. Se han intentado una gran diversidad de aproximaciones. En lo que sigue, se describen algunas de las más utilizadas, éstas se definen en la Tabla 5.2 y se muestran en la Figura 5.2[2].

Antes de describir las técnicas de codificación propiamente dichas, se considerarán los siguientes procedimientos a tener en cuenta para su evaluación y comparación.

- **Espectro de la señal:** hay varios aspectos del espectro de la señal que son importantes. La ausencia de componentes a altas frecuencias significa que se necesita menos ancho de banda para su transmisión. Es más, la ausencia de componente en continua (dc) es también una característica deseable. Si la señal tiene continua, para su transmisión se requiere la existencia de una conexión física directa; si la señal no contiene componente continua, es posible su transmisión mediante transformadores acoplados. Lo que proporciona un aislamiento eléctrico excelente, reduciendo las interferencias. Por último la importancia de los efectos relacionados con la distorsión de la señal y las interferencias depende de las propiedades espectrales de la señal transmitida. En la práctica es frecuente que la función de transferencia del canal sea peor cerca de los límites de la banda. Por

Tabla 5.2. Definición de los formatos de codificación digital de señales.

No retorno a cero (NRZ-L)
0 = nivel alto
1 = nivel bajo

No retorno a cero invertido (NRZI)
0 = no hay transición al comienzo del intervalo (un bit cada vez)
1 = transición al comienzo del intervalo

Bipolar-AMI
0 = no hay señal
1 = nivel positivo o negativo, alternante

Pseudoternario
0 = nivel positivo a negativo, alternante
1 = no hay señal

Manchester
0 = transición de alto a bajo en mitad del intervalo
1 = transición de bajo a alto en mitad del intervalo

Manchester diferencial
Siempre hay una transición en mitad del intervalo
0 = transición al principio del intervalo
1 = no hay transición al principio del intervalo

B8ZS
Igual que el bipolar-AMI, excepto que cualquier cadena de ceros se reemplaza por una cadena que tiene dos violaciones de código.

HDB3
Igual que el bipolar-AMI, excepto que cualquier cadena de cuatro ceros se reemplaza por una cadena que contiene una violación de código.

[2] En esta figura, se ha supuesto que en el esquema AMI el 1 (valor binario) más reciente se codificó con una tensión negativa, y para el pseudoternario, el 0 (valor binario) anterior se codificó igualmente con un nivel de tensión negativo.

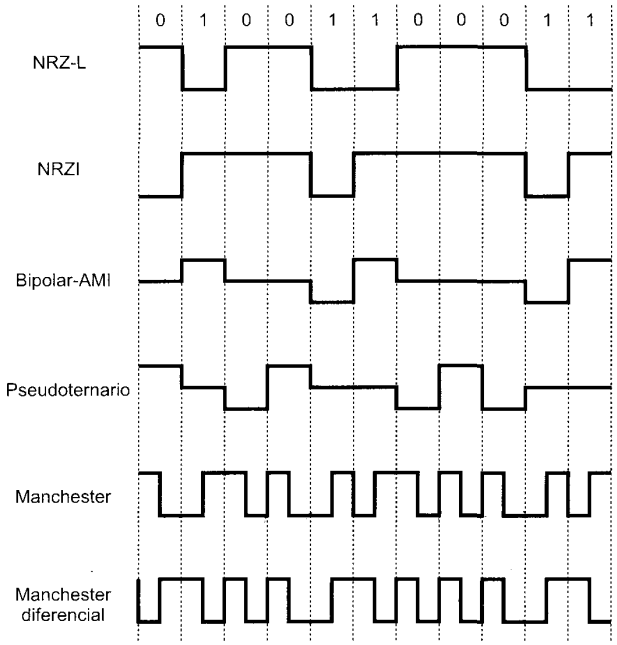


Figura 5.2. Formatos de codificación utilizando señal digital.

tanto, un buen diseño debería concentrar la potencia transmitida en la parte central del ancho de banda de la señal transmitida. En tal caso, se tendrá una distorsión menor en la señal recibida. Para conseguir este objetivo, se pueden diseñar los códigos de forma que se modele adecuadamente el espectro de la señal transmitida.

- **Sincronización:** ya se ha mencionado la necesidad de determinar el principio y fin de cada bit. Esto no es una tarea fácil. Una solución, bastante costosa, es transmitir una señal de reloj por separado para sincronizar el receptor con el transmisor. La alternativa es proporcionar la sincronización mediante la propia señal transmitida, lo que puede conseguirse si se adopta un esquema de codificación adecuado.
- **Detección de errores:** en el Capítulo 7 se discutirán algunas de las técnicas que se usan para la detección de errores, y además se mostrará que estas técnicas son responsabilidad de una capa por encima del nivel de señalización, denominada control del enlace de datos. No obstante, es útil disponer de alguna capacidad de detección de errores incorporada en el esquema de codificación situado en la capa física, permitiéndose así que los errores se detecten más rápidamente.
- **Inmunidad al ruido e interferencias:** algunos códigos exhiben un comportamiento superior que otros en presencia de ruido. Esto se expresa habitualmente mediante el BER.
- **Coste y complejidad:** aunque el coste económico de la lógica digital continúa bajando, no se debe ignorar este factor. En particular, cuanto mayor es la velocidad de elementos de señal para una velocidad de transmisión dada, mayor es el coste. En lo que sigue se describirán algunos códigos que implican una velocidad de elementos de señalización superior a la velocidad de transmisión de datos real.

Volvamos ya a la presentación y discusión de los diversos esquemas de codificación.

NO RETORNO A CERO (NRZ, NONRETURN TO ZERO)

La forma más frecuente y fácil de transmitir señales digitales es mediante la utilización de un nivel diferente de tensión para cada uno de los dos dígitos binarios. Los códigos que siguen esta estrategia comparten la propiedad de que el nivel de tensión se mantiene constante durante la duración del bit; es decir, no hay transiciones (no hay retorno al nivel cero de tensión). Por ejemplo, la ausencia de tensión se puede usar para representar un 0 binario, mientras que un nivel constante y positivo de tensión puede representar al 1. Aunque es más habitual usar un nivel negativo para representar un valor binario y una tensión positiva para representar al otro. Este último código, mostrado[3] en la Figura 5.2, se denomina código **Nivel no retorno a cero** (NRZ-L, Nonreturn-to- Zero-Level). NRZ-L se usa generalmente para generar o interpretar los datos binarios en los terminales y otros dispositivos. Si se utiliza un código diferente, éste se generará usualmente a partir de la señal NRZ-L [en los términos que se muestran en la Figura 5.1 la señal NRZ-L es $g(t)$ y la señal codificada es $s(t)$].

Una variante del NRZ se denomina **NRZI** (Noreturn to Zero, invert on ones). Al igual que NRZ-L, el NRZI mantiene constante el nivel de tensión durante la duración de un bit. Los datos se codifican mediante la presencia o ausencia de una transición de la señal al principio del intervalo de duración del bit. Un 1 se codifica mediante la transición (bajo a alto o alto a bajo) al principio del intervalo de señalización, mientras que un cero se representa por la ausencia de transición.

NRZI es un ejemplo de **codificación diferencial**. En la codificación diferencial, en lugar de determinar el valor absoluto, la señal se decodifica comparando la polaridad de los elementos de señal adyacentes. En términos generales, la codificación de cada bit se hace de la siguiente manera: si se trata del valor binario 0, se codifica con la misma señal que el bit anterior, si se trata de un valor binario 1, entonces se codifica con una señal diferente que la utilizada para el bit precedente. Una ventaja de este esquema es que en presencia de ruido puede ser más seguro detectar una transición en lugar de comparar un valor con un umbral. Otra ventaja es que en un sistema complicado de transmisión, no es difícil perder la polaridad de la señal. Por ejemplo, en una línea de par trenzado, si los cables se invierten accidentalmente, todos los 1 y 0 en el NRZ-L se invertirán. Esto no pasa en un esquema diferencial.

Los códigos NRZ son los más fáciles de implementar y además se caracterizan por hacer un uso eficaz del ancho de banda. Esta última propiedad se pone de manifiesto en la Figura 5.3, en la que se compara la densidad espectral de varios esquemas de codificación. En dicha figura, la frecuencia está normalizada a la velocidad de transmisión de los datos. Como se puede ver, en los códigos NRZ y NRZI la mayor parte de la energía está comprendida entre la componente en continua y la mitad de la velocidad de transmisión. Por ejemplo, si se usa un código NRZ para generar una señal a una velocidad de transmisión para los datos de 9.600 bps, la mayor parte de la energía estará concentrada entre la componente en continua (dc) y 4.800 Hz.

La principal limitación de las señales NRZ es la presencia de una componente dc continua y la ausencia de capacidad de sincronización. Para ilustrar esta última desventaja, téngase en cuenta que una cadena larga de unos o de ceros en un esquema NRZ-L o una cadena de ceros en el NRZI, se codificará como un nivel de tensión constante durante un largo intervalo de tiempo. En estas circunstancias, cualquier fluctuación entre los relojes del transmisor y el receptor dará lugar a una pérdida de sincronización entre ambos.

Debido a su sencillez y las características de su respuesta relativamente baja en frecuencias, los códigos NRZ se usan con frecuencia en las grabaciones magnéticas. No obstante, sus limitaciones hacen que estos códigos no sean atractivos para aplicaciones de transmisión de señales.

---

[3] En esta figura, una tensión negativa representa un 1 binario y una positiva representa un 0. Esta definición es posiblemente contraria a la definición utilizada en otros textos. La definición aquí presentada es coherente con el uso del NRZ-L en las interfaces de comunicaciones de datos y así como con las normalizaciones que controlan dichas interfaces.

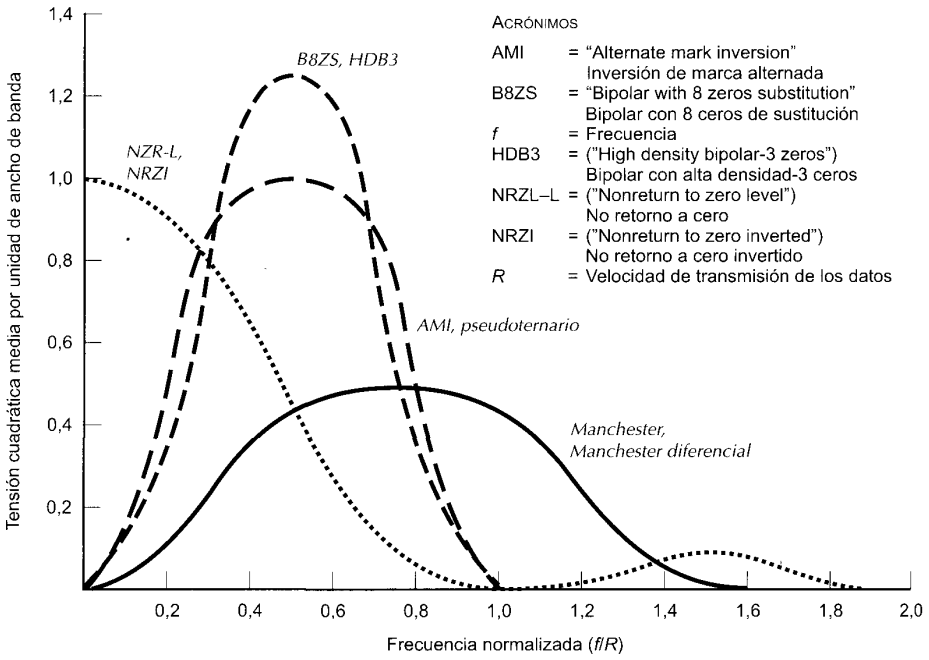


Figura 5.3. Densidad espectral de varios esquemas de codificación.

BINARIO MULTINIVEL

Las técnicas de codificación denominadas binario multinivel subsanan algunas de las deficiencias mencionadas para los códigos NRZ. Estos códigos usan más de dos niveles de señal. En la Figura 5.2 se muestran dos ejemplos, el «bipolar-AMI» (Alternate mark inversion) y el pseudoternario[4].

En el caso del esquema **bipolar-AMI**, un 0 binario se representa por ausencia de señal y el 1 binario se representa como un pulso positivo o negativo. Los pulsos correspondientes a los 1 deben tener una polaridad alternante. Este tipo de esquema tiene las siguientes ventajas. En primer lugar, no habrá problemas de sincronización en el caso de que haya una cadena larga de 1. Cada 1 fuerza una transición, por lo que el receptor se puede sincronizar en dicha transición. Una cadena larga de ceros, sigue siendo un problema. En segundo lugar, ya que los elementos de señal correspondientes a 1 alternan el nivel de tensión, no hay componente continua. Además, el ancho de banda de la señal resultante es considerablemente menor que el correspondiente a NRZ (Figura 5.3). Por último, la alternancia entre los pulsos proporciona una forma sencilla de detectar errores. Cualquier error aislado, tanto si elimina como si introduce un pulso, significa un incumplimiento de dicha propiedad.

Los comentarios del párrafo anterior son también trasladables a los códigos **pseudoternarios**. En este caso, el bit 1 se representa por la ausencia de señal, y el 0 mediante pulsos de polaridad alternante. No hay ninguna ventaja particular de esta codificación respecto de la anterior, siendo la base de muchas aplicaciones.

---

[4] Estos términos no se usan con consistencia en la literatura especializada. En algunos textos, estos dos términos se usan para esquemas de codificación diferentes a los aquí definidos, e igualmente, para los códigos mostrados en la Figura 5.2 se usa una gran diversidad de términos. La nomenclatura que se ha adoptado corresponde con la utilizada en varios documentos normalizaciones de la UIT-T.

No obstante, el grado de sincronización proporcionado por estos códigos todavía presenta algunos problemas (una cadena larga de ceros en el caso del AMI o de unos en el pseudoternario). Para solventar dichos problemas se han propuesto otra serie de códigos. Una aproximación es insertar bits que fuercen transiciones. Este procedimiento se adopta en RDSI para la transmisión a velocidades relativamente bajas. Desde luego, este esquema es costoso para velocidades de transmisión superiores, ya que significaría un aumento en la ya de por sí alta velocidad de transmisión. Para resolver este problema a altas velocidades de transmisión se utiliza una técnica que implica desordenar los datos. Posteriormente, en esta sección se proporcionarán dos ejemplos de esta técnica.

Así pues, con las modificaciones pertinentes, el esquema binario multinivel soslaya los problemas de los códigos NRZ. Por supuesto, al igual que cualquier otra decisión de ingeniería, siempre existe un compromiso. Con la codificación binaria multinivel, la señal puede tomar tres posibles valores en cada elemento de señal, lo que representaría $\log_2 3 = 1{,}58$ bits de información, aunque en realidad transporta sólo un bit de información. Por tanto, el código binario multinivel no es tan eficaz como los NRZ. Otra forma de enunciar este hecho es que el receptor de señales codificadas con binario multinivel se ve obligado a distinguir entre tres niveles ($+A$, $-A$, 0), en lugar de los dos niveles de los otros esquemas presentados anteriormente. Por tanto, para obtener la misma probabilidad de error, la señal de un código binario multinivel necesita aproximadamente 3 dB más de potencia que las señales bivaluadas. Este hecho se muestra en la Figura 5.4. Dicho de otra forma, dada una relación señal ruido, la tasa de errores por bit para los códigos NRZ es significativamente menor que la correspondiente en un código binario multinivel.

BIFASE

Bajo el término *bifase*, se engloba a otro conjunto de técnicas de codificación alternativas, diseñadas para superar las dificultades encontradas en los códigos NRZ. Dos de estas técnicas, denominadas Manchester y Manchester Diferencial, se usan frecuentemente en los sistemas de comunicación.

En el código **Manchester**, siempre hay siempre una transición en mitad del intervalo de duración del bit. Esta transición en la mitad del bit sirve como un procedimiento de sincronización a la vez que sirve para transmitir los datos: una transición de bajo a alto representa un 1, y una transición de alto a

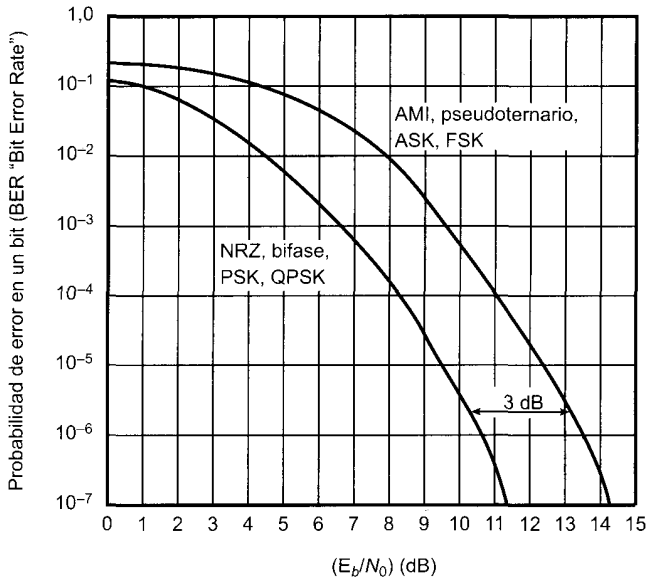


Figura 5.4. Tasa de errores por bit teórica para varios esquemas de codificación digital.

bajo representa un 0[5]. En **Manchester Diferencial**, la transición a mitad el intervalo se utiliza tan sólo para proporcionar sincronización. La codificación de un 0 se representa por la presencia de una transición al principio del intervalo del bit, y un 1 se representa mediante la ausencia de una transición al principio del intervalo. El Manchester Diferencial tiene como ventajas adicionales las derivadas de la utilización de una aproximación diferencial.

Todas las técnicas bifase fuerzan al menos una transición por cada bit pudiendo tener hasta dos en ese mismo periodo. Por tanto, la velocidad de modulación máxima es el doble que en los NRZ; esto significa que el ancho de banda necesario es por tanto mayor. No obstante, los esquemas bifase tienen las siguientes ventajas:

- **Sincronización:** debido a que la transición que ocurre durante el intervalo de duración correspondiente a un bit siempre está presente, el receptor puede sincronizarse usando dicha transición. Es ésta la razón por la que a los códigos bifase también se les denomina auto-sincronizados.
- **No tienen componente en continua:** los códigos bifase no tienen componente en continua, lo que implica todas las ventajas mencionadas anteriormente.
- **Detección de errores:** se pueden detectar errores si se observa una ausencia de la transición esperada en mitad del intervalo. Para que el ruido produjera un error no detectado tendría que invertir la señal antes y después de la transición.

Como se puede ver en la Figura 5.3, el ancho de banda en los códigos bifase es razonablemente estrecho, además de no contener componente en continua. Aún así, es más ancho que el ancho de banda de los códigos binarios multinivel.

Los códigos bifase se usan con frecuencia en los esquemas de transmisión de datos. Uno de los más conocidos es el código Manchester que se ha elegido como parte de la especificación de la normalización IEEE 802.3 para la transmisión en redes LAN con bus CSMA/CD usando cable coaxial en banda base o par trenzado. El Manchester Diferencial se ha elegido en la normalización IEEE 802.5 para redes LAN en anillo con paso de testigo, en las que se usan pares trenzados apantallados.

VELOCIDAD DE MODULACIÓN

Cuando se usan técnicas de codificación de señales, se debe hacer una diferenciación entre la velocidad de transmisión de los datos (expresada en bits por segundo) y la velocidad de modulación (expresada en baudios). La velocidad de transmisión, también denominada tasa de bits, es $1/t_B$, donde t_B = la duración de un bit. La velocidad de modulación es aquella con la que se generan los elementos de señal. Considérese por ejemplo la codificación Manchester. El elemento de señal mínimo tiene una duración igual a la mitad de la duración del intervalo correspondiente a un bit. Si se tratara de una cadena de bits todos igual a 0, o a 1, se generaría una serie de pulsos como los mencionados. Por tanto, la velocidad máxima de modulación en el código Manchester es $2/t_B$. Este caso se muestra en la Figura 5.5, correspondiente a la transmisión de una cadena de unos a una velocidad de transmisión de 1 Mbps usando NRZI y Manchester. En general,

$$D = \frac{R}{b}$$

donde

D = velocidad de modulación en baudios.

R = velocidad de transmisión en bps.

b = número de bits por elemento de señal.

---

[5] La definición del código Manchester presentada aquí es opuesta a la que se usa en muchos libros de texto que merecen respeto (por ejemplo: [TANE96], [COUC97], [FREE98] y [PETE95]) en los que un 0 binario corresponde a una transición bajo a alto, y un 1 binario corresponde a una transición alto a bajo. Aquí, la definición adoptada es coherente con la definición adoptada por la industria y con la utilizada en varios estándares para LAN, como por ejemplo, la norma IEEE 802.3.

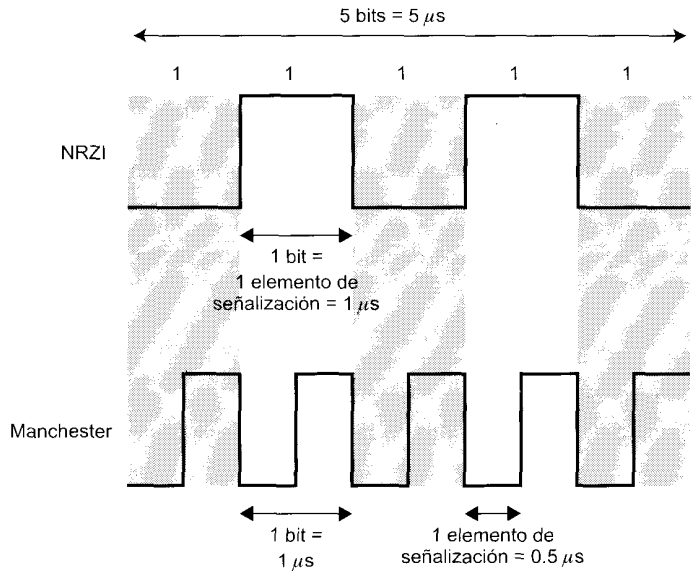


Figura 5.5. Una cadena de unos a 1 Mbps.

Una forma de caracterizar la velocidad de modulación es determinando el número medio de transiciones que se dan en el intervalo de tiempo correspondiente a la duración de un bit. En general, esto dependerá de la secuencia en particular de bits que se transmitan. En la Tabla 5.3 se comparan las velocidades de modulación para diversas técnicas. En dicha tabla se indica la razón de transiciones de la señal normalizadas para el caso de una cadena de unos y ceros alternantes, así como para las cadenas de datos correspondientes a la velocidad de modulación *máxima* y *mínima*.

TÉCNICAS DE «SCRAMBLING»

El éxito obtenido por los esquemas bifase en el entorno de las redes LAN a velocidades relativamente altas (hasta 10 Mbps), no es trasladable a las redes de larga distancia. La razón principal de esto estriba en el hecho de que bifase requiere una alta velocidad de elementos de señal comparada con la velocidad

Tabla 5.3. Velocidad de modulación normalizada de la señal para distintas velocidades de codificación de la señal digital.

	Mínimo	101010...	Máximo
NRZ-L	0 (todo 0s o 1s)	1,0	1,0
NRZI	0 (todo 0s)	0,5	1,0 (todo 1s)
bipolar-AMI	0 (todo 0s)	1,0	1,0
Pseudoternario	0 (todo 1s)	1,0	1,0
Manchester	10 (1010...)	1,0	2,0 (todo 0s o 1s)
Manchester diferencial	1,0 (todo 1s)	1,5	2,0 (todo 0s)

de transmisión obtenida para los datos. Este tipo de desventaja es más relevante, y por tanto, más costosa, en redes de larga distancia.

Otra aproximación alternativa es utilizar algún procedimiento o técnica de «scrambling». La idea subyacente en este tipo de técnicas es sencilla: reemplazar las secuencias de bits que den lugar a niveles de tensión constante por otras secuencias que proporcionen suficiente número de transiciones de forma tal que el reloj del receptor pueda mantenerse sincronizado. En el receptor se debe identificar la secuencia reemplazada y sustituirla por la secuencia original. La secuencia reemplazada tendrá la misma longitud que la original, por tanto, este procedimiento no implica cambio alguno en la velocidad de transmisión de los datos. Los objetivos en el diseño de estas técnicas se pueden resumir en:

- Evitar la componente en continua.
- Evitar las secuencias largas que correspondan a señales de tensión nula.
- No reducir la velocidad de transmisión de los datos.
- Tener cierta capacidad para detectar errores.

En la Figura 5.6 se muestran dos de las técnicas que se usan frecuentemente en las comunicaciones a larga distancia.

Un esquema de codificación que se usa habitualmente en Norteamérica se denomina **B8ZS (Bipolar with 8-Zeros Substitution)**, y se basa en un AMI bipolar. Previamente se mencionó que el inconveniente de los códigos AMI es que una secuencia larga de ceros puede dar lugar a una pérdida de sincronización. Para evitar este problema la codificación se realiza de acuerdo con las siguientes reglas:

- Si aparece un octeto con todo ceros y el último valor de tensión anterior a dicho octeto fue positivo, codificar dicho octeto como 000+−0−+.
- Si aparece un octeto con todo ceros y el último valor de tensión anterior a dicho octeto fue negativo, codificar dicho octeto como 000−+0+−.

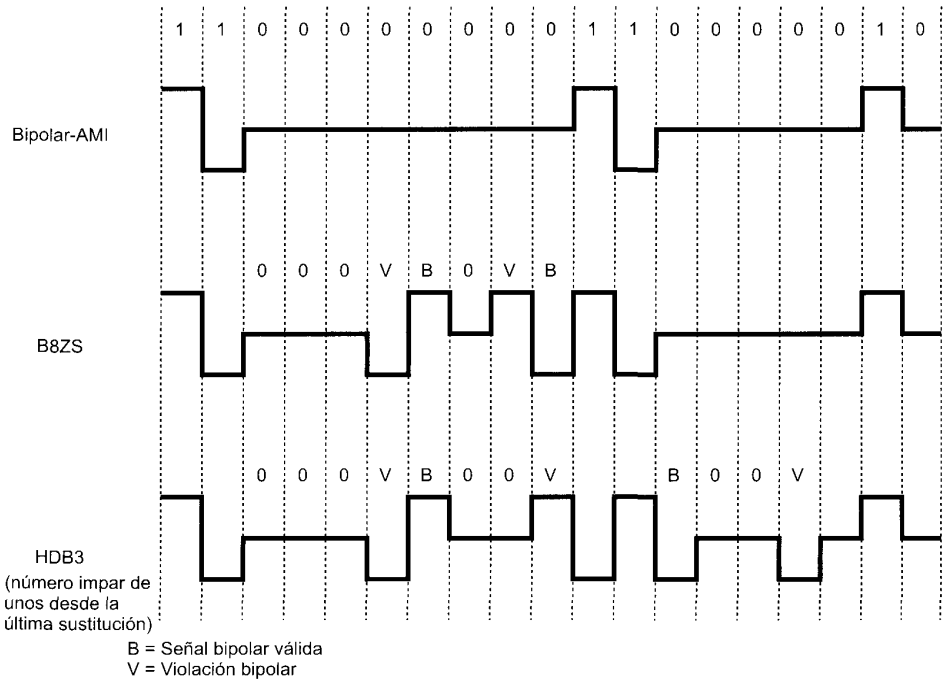


Figura 5.6. Reglas de codificación para B8ZS y HDB3.

Tabla 5.4. Reglas de sustitución en HDB3.

	Número de pulsos bipolares (unos) desde la última sustitución	
Polaridad del pulso anterior	**Impar**	**Par**
−	000 −	+ 00 +
+	000 +	− 00 −

Con este procedimiento se fuerzan dos violaciones de código del código AMI, (combinaciones de estados de señalización no permitidos por el código). Esta combinación tiene una probabilidad muy baja de haber sido causa por el ruido u otros defectos en la transmisión. El receptor identificará ese patrón y lo interpretará convenientemente como un octeto todo ceros.

Un esquema de codificación que se utiliza habitualmente en Europa y Japón es el denominado **HDB3 (High Density Bipolar-3 Zeros)**, véase Tabla 5.4. Al igual que el anterior, se basa en la codificación AMI. En este esquema, se reemplazan las cadenas de cuatro ceros por cadenas que contienen uno o dos pulsos. En este caso, el cuarto cero se sustituye una violación del código. Además, en las violaciones siguientes, se considera una regla adicional para asegurar que las mismas tengan una polaridad alternante, evitando así la introducción de componente en continua. Es decir, si la última violación fue positiva la siguiente deberá ser negativa y viceversa. En la Tabla 5.4 se indica que esta condición se determina dependiendo (1) si el número de pulsos desde la última violación es par o impar y (2) dependiendo de la polaridad del último pulso anterior a la aparición de los cuatro ceros.

En la Figura 5.4 se muestran las propiedades espectrales de los dos códigos mencionados. Como se puede observar, ninguno de los dos contiene componente en continua. La mayor parte de la energía se concentra en una región estrecha en torno a la frecuencia correspondiente a la mitad de la velocidad de transmisión de los datos. Por tanto, estos códigos son adecuados para la transmisión a altas velocidades.

5.2. DATOS DIGITALES, SEÑALES ANALÓGICAS

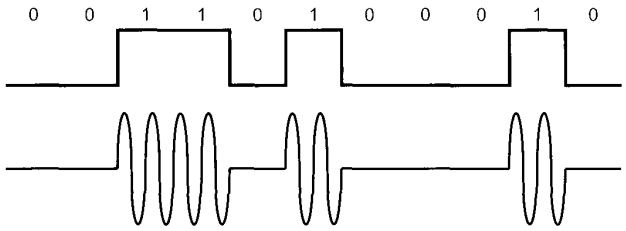
Consideremos ahora el caso de la transmisión de datos digitales usando señales analógicas. La situación más habitual para este tipo de situaciones es la transmisión de datos digitales a través de la red telefónica. Esta red se diseñó para recibir, conmutar y transmitir señales analógicas en el rango de frecuencias de voz entre 300 y 3.400 Hz. No es, por tanto, adecuada para la transmisión de señales digitales desde el terminal de abonado (aunque esto está progresivamente cambiando). No obstante, se pueden conectar dispositivos digitales a través de la red mediante el uso de dispositivos modem (modulador-demodulador), que convierten los datos digitales en señales analógicas y viceversa.

En la red telefónica se usan los modems para producir señales en el rango de frecuencias de voz, si bien, las mismas técnicas se pueden usar para modems a frecuencias más altas (por ejemplo microondas). En esta sección se presentan estas técnicas y se proporciona una breve discusión de las prestaciones de las distintas posibles alternativas.

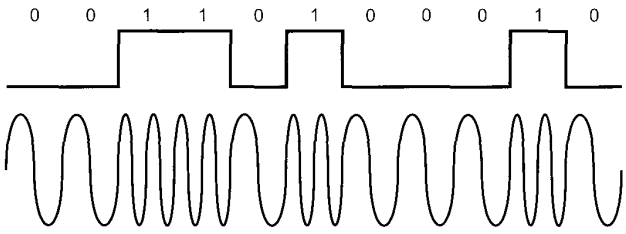
TÉCNICAS DE CODIFICACIÓN

Se ha mencionado que la modulación involucra a uno o más de los parámetros característicos de la señal portadora: la amplitud, la frecuencia y la fase. Por consiguiente, como se muestra en la Figura 5.7, hay tres técnicas básicas de codificación o de modulación, que transforman los datos digitales en señales analógicas:

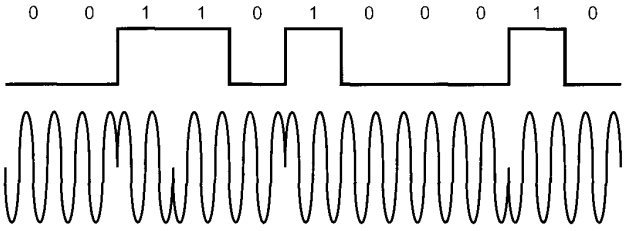
- Desplazamiento de amplitud (ASK, Amplitudes-Shift Keying).
- Desplazamiento de frecuencia (FSK, Frequency-Shift Keying).
- Desplazamiento de fase (PSK, Phase-Shift Keying).



(a) Desplazamiento de amplitud (ASK)



(b) Desplazamiento de frecuencia (FSK)



(c) Desplazamiento de fase (PSK)

Figura 5.7. Modulación de datos digitales.

En todos los casos, la señal resultante ocupa un ancho de banda centrado en torno a la frecuencia de la portadora.

En **ASK**, los dos valores binarios se representan mediante dos amplitudes diferentes de la portadora. Es usual que una de las amplitudes sea cero; es decir, uno de los dígitos binarios se representa mediante la presencia de la portadora a amplitud constante, y el otro mediante la ausencia de portadora. La señal resultante es

$$\textbf{ASK} \qquad s(t) = \begin{cases} A\cos(2\pi f_c t) & 1 \text{ binario} \\ 0 & 0 \text{ binario} \end{cases}$$

en el que la portadora es $A\cos(2\pi f_c t)$. ASK es sensible a cambios repentinos de la ganancia, además es una técnica de modulación bastante ineficaz. En líneas de calidad telefónica, ASK se usa típicamente a 1.200 bps como mucho.

La técnica ASK se usa para la transmisión de datos digitales en fibras ópticas. En los transmisores con LED, la expresión anterior sigue siendo válida. Es decir, un elemento de señal se representa mediante un pulso de luz, mientras que el otro elemento se representa mediante la ausencia de luz. Los transmisores láser tienen normalmente un valor de desplazamiento («bias») que hace que el dispositivo emita para el último caso una señal de baja intensidad. Este pequeño nivel será uno de los elementos de señalización, mientras que el otro será un haz de luz de mayor amplitud.

En **FSK**, los dos valores binarios se representan mediante dos frecuencias diferentes próximas a la frecuencia de la portadora. La señal resultante es

$$\textbf{FSK} \qquad s(t) = \begin{cases} A\cos(2\pi f_1 t) & 1 \text{ binario} \\ A\cos(2\pi f_2 t) & 0 \text{ binario} \end{cases}$$

donde típicamente f_1 y f_2 corresponden a desplazamientos de la frecuencia portadora f_c, de igual magnitud pero en sentidos opuestos.

En la Figura 5.8 se muestra un ejemplo del uso de FSK en una transmisión full-duplex en una línea de calidad telefónica. Dicha figura corresponde a la serie de modems Bell System 108. Recuérdese que una línea de calidad telefónica deja aproximadamente pasar frecuencias en el rango de 300 a 3.400 Hz, y que *full-duplex* significa que la señales se transmiten simultáneamente en ambos sentidos. Para transmitir full-duplex, el ancho de banda anterior se parte en torno a los 1.700 Hz. En uno de los sentidos (correspondiente a la transmisión o a la recepción) las frecuencias utilizadas para representar al 1 o 0 están centradas en torno a los 1.170 Hz, desplazándose 100 Hz a cada lado. El efecto de usar estas dos frecuencias se muestra en la Figura 5.8, y corresponde a la transmisión de una señal cuyo espectro corresponde con la zona sombreada de la izquierda de la figura. De igual manera, para el otro sentido (recepción o transmisión) el modem utilizará señales correspondientes a desplazamientos de 100 Hz en torno a la frecuencia central de 2.125 Hz. Estas señales corresponden con el área sombreada a la derecha en la Figura 5.8. Obsérvese que hay un pequeño solapamiento entre las bandas, es decir, hay una pequeña interferencia.

FSK es menos sensible a errores que ASK. En líneas de calidad telefónica, se utiliza típicamente a velocidades de hasta 1.200 bps. También se usa frecuentemente en transmisión de radio a más altas frecuencias (desde 3 hasta 30 MHz). También se puede usar incluso a frecuencias superiores en redes de área local que utilicen cable coaxial.

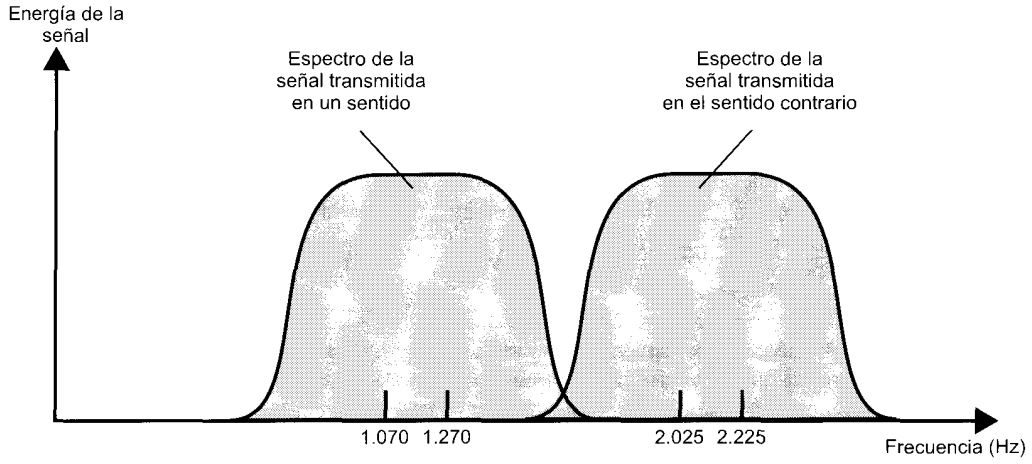


Figura 5.8. Transmisión «full-duplex» en una línea de calidad telefónica.

En el esquema **PSK**, la fase de la señal portadora se desplaza para representar con ello a los datos digitales. En la parte inferior de la Figura 5.7 se muestra un ejemplo de un sistema que utiliza dos fases. En este sistema, un 0 binario se representa mediante la transmisión de una señal con la misma fase que la fase de la señal anteriormente enviada. Mientras que un 1 se representa mediante la transmisión de una señal cuya fase está en oposición de fase respecto a la señal precedente. Esta técnica se conoce como PSK diferencial, ya que el desplazamiento en fase es relativo a la fase correspondiente al último símbolo transmitido, en vez de ser relativo a algún valor constante de referencia. La señal resultante es

$$\textbf{PSK} \qquad s(t) = \begin{cases} A\cos(2\pi f_c t + \pi) & 1 \text{ binario} \\ A\cos(2\pi f_c t) & 0 \text{ binario} \end{cases}$$

siendo la fase relativa a la correspondiente del bit anterior.

Se puede conseguir una utilización más eficaz del ancho de banda si cada elemento de señalización representa a más de un bit. Por ejemplo, en lugar de usar un desplazamiento de fase de 180°, como el que se hace en PSK, otra técnica de codificación frecuente denominada desplazamiento de fase en cuadratura (QPSK, Quadrature phase-shift keying), considera desplazamientos de fase correspondientes a múltiplos de $\pi/2$ (90°).

$$\textbf{QPSK} \qquad s(t) = \begin{cases} A\cos\left(2\pi f_c t + \frac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t + \frac{3\pi}{4}\right) & 10 \\ A\cos\left(2\pi f_c t + \frac{5\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t + \frac{7\pi}{4}\right) & 01 \end{cases}$$

Por lo que cada elemento de señal representa dos bits en lugar de uno.

Este esquema se puede ampliar, ya que se pueden transmitir tres bits cada vez si se usan ocho ángulos de fase diferentes. Es más, cada ángulo puede tener varias amplitudes. Por ejemplo, en un modem estándar a 9.600 bps se utilizan 12 ángulos de fase diferentes, cuatro de los cuales tienen dos posibles amplitudes.

En este último ejemplo se puede establecer claramente la diferencia entre la velocidad de transmisión R (en bps) y la velocidad de modulación D de la señal (en baudios). Supongamos que este esquema se emplea con una entrada digital codificada en NRZ-L. La velocidad de transmisión será $R = 1/t_B$, donde t_B es igual a la anchura de cada bit codificado con NRZ-L. No obstante, la señal codificada contiene $b = 4$ bits en cada elemento de señal, ya que se usan $L = 16$ combinaciones diferentes de amplitudes y fases. La velocidad de modulación será $R/4$, ya que cada elemento de señalización transporta cuatro bits. Por tanto, la velocidad de modulación de la línea es igual a 2.400 baudios, mientras que la velocidad de transmisión es igual a 9.600 bps. Esencialmente, ésta es la explicación de cómo en líneas de calidad telefónica se puede transmitir a velocidades de transmisión superiores utilizando esquemas de modulación más complejos.

En general,

$$D = \frac{R}{b} = \frac{R}{\log_2 L}$$

donde

D = velocidad de modulación en baudios.

R = velocidad de transmisión en bps.

L = número de elementos de señalización diferentes.

b = número de bits por elemento de señalización.

El procedimiento anterior se complica cuando se utiliza una técnica de codificación distinta al NRZ. Por ejemplo, ya se vio que la velocidad de modulación máxima para las señales bifase es $2/t_B$. Por tanto, D es mayor en bifase que en NRZ, por lo que en cierta manera se está contrarrestando la reducción en D conseguida con las técnicas de modulación multinivel.

PRESTACIONES

El primer parámetro que se debe considerar para comparar las prestaciones de los distintos esquemas de modulación digital a analógico es el ancho de banda de la señal modulada. Éste dependerá de diversos factores, entre otros de la propia definición que se haga de ancho de banda así como de la técnica de filtrado que se use para obtener la señal pasabanda. Aquí se utilizarán los resultados obtenidos en [COUC97].

El ancho de banda B_T para ASK es de la forma

$$B_T = (1 + r)R$$

donde R es la velocidad de transmisión y r está relacionado con la técnica de filtrado de la señal aplicada para limitar el ancho de banda de la misma, permitiendo así su posterior transmisión, típicamente se verifica que $0 < r < 1$. Así el ancho de banda está directamente relacionado con velocidad de transmisión. La expresión anterior es también válida para PSK.

Para FSK, el ancho de banda se puede expresar como

$$B_T = 2\Delta F + (1 + r)R$$

donde $\Delta F = f_2 - f_c = f_c - f_1$ es el desplazamiento de la frecuencia de la señal modulada respecto de la frecuencia de la portadora. Cuando se usan frecuencias muy altas, el término ΔF es el dominante. Por ejemplo, uno de los estándares que utiliza FSK en redes locales multipunto sobre cable coaxial usa $\Delta F = 1{,}25$ MHz, $f_c = 5$ MHz, y $R = 1$ Mbps. En este caso $2\Delta F = 2{,}5$ MHz. En el ejemplo anteriormente mencionado del modem Bell 108, $\Delta F = 100$ Hz, $f_c = 1.170$ Hz (en un sentido), y $R = 300$ bps. En este caso el término $(1 + r)R$ domina.

Utilizando señalización multinivel, se pueden conseguir mejoras significativas en el ancho de banda. En general,

$$B_T = \left(\frac{1 + r}{b}\right)R = \left(\frac{1 + r}{\log_2 L}\right)R$$

donde b es el número de bits codificados en cada elemento de señalización y L es el número de elementos de señalización diferentes.

En la Tabla 5.5 se muestra el cociente entre las velocidades de transmisión R y el ancho de banda necesario para distintos esquemas de modulación. Este cociente también se denomina eficiencia del ancho de banda. Como su nombre indica, este parámetro es una medida de la eficiencia en la utilización del ancho de banda al transmitir los datos. Por tanto, las mejoras introducidas por la utilización de un esquema de señalización multinivel, ahora son ya evidentes.

Por supuesto, la discusión anterior hace referencia al espectro de la señal de entrada a la línea de transmisión. Nótese, que todavía no se ha mencionado nada relacionado con la presencia de ruido. En la Figura 5.4 se resumen algunos resultados relevantes basados en ciertas suposiciones relativas a los sistemas de transmisión [COUC97]. Aquí se representa la tasa de errores por bit en función del cociente E_b/N_0, definido en el Capítulo 3. Por supuesto, cuando este cociente aumenta, la tasa de errores disminuye. Es más, PSK y QPSK mejoran a ASK y a FSK en aproximadamente 3 dB.

Tabla 5.5. Relación entre la razón de datos y el ancho de banda de transmisión para varios esquemas de codificación digital-analógico.

	$r = 0$	$r = 0{,}5$	$r = 1$
ASK	1,0	0,67	0,5
FSK			
Banda ancha ($\Delta F \gg R$)	~0	~0	~0
Banda estrecha ($\Delta F \approx f_c$)	1,0	0,67	0,5
PSK	1,0	0,67	0,5
Señalización multinivel			
$L = 4$, $b = 2$	2,00	1,33	1,00
$L = 8$, $b = 3$	3,00	2,00	1,50
$L = 16$, $b = 4$	4,00	2,67	2,00
$L = 32$, $b = 5$	5,00	3,33	2,50

Este concepto se puede ya relacionar con la eficiencia del ancho de banda. Recuérdese que

$$\frac{E_b}{N_0} = \frac{S}{N_0 R}$$

El parámetro N_0 es la densidad de potencia del ruido, en vatios/hertzios. Por tanto, el ruido en una señal con ancho de banda B_T es $N = N_0 B_T$. Sustituyendo, se tiene que

$$\frac{E_b}{N_0} = \frac{S}{N}\frac{B_T}{R}$$

En un esquema de señalización dado, la tasa de errores por bit se puede reducir incrementando E_b/N_0, lo que se puede conseguir incrementando el ancho de banda o reduciendo la velocidad de transmisión de los datos; en otras palabras, reduciendo la eficiencia del ancho de banda.

Ejemplo

¿Cuál es la eficiencia del ancho de banda para FSK, ASK, PSK, y QPSK si la tasa de errores por bit es 10^{-7} en un canal con una SNR igual a 12 dB?

Se tiene que

$$\frac{E_b}{N_0} = 12\,\text{dB} - \left(\frac{R}{B_T}\right)_{\text{dB}}$$

A partir de la Figura 5.4, para FSK y ASK se tiene que

$$\frac{E_b}{N_0} = 14{,}2\,\text{dB}$$

$$\left(\frac{R}{B_T}\right)_{\text{dB}} = -2{,}2\,\text{dB}$$

$$\frac{R}{B_T} = 0{,}6$$

De la misma figura, para PSK

$$\frac{E_b}{N_0} = 11{,}2\,\text{dB}$$

$$\left(\frac{R}{B_T}\right)_{\text{dB}} = 0{,}8\,\text{dB}$$

$$\frac{R}{B_T} = 1{,}2$$

Para QPSK se debe tener en cuenta que $D = R/2$. Por tanto

$$\frac{R}{B_T} = 2{,}4$$

Como se muestra en el ejemplo anterior, los esquemas ASK y FSK proporcionan la misma eficiencia del ancho de banda, PSK es mejor, y todavía se consigue mayor eficiencia si se utiliza una señalización multinivel.

Es conveniente hacer una comparación de estas necesidades de ancho de banda con las correspondientes a la señalización digital. Una buena aproximación es

$$B_T = 0{,}5(1 + r)D$$

donde D es la velocidad de modulación. En NRZ se cumple que $D = R$, luego

$$\frac{R}{B_T} = \frac{2}{1 + r}$$

Por tanto, la señalización digital es comparable en cuanto a la eficiencia del ancho de banda con ASK, FSK y PSK. Si bien se puede observar una mejora significativa en la señalización analógica al utilizar técnicas multinivel.

5.3. DATOS ANALÓGICOS, SEÑALES DIGITALES

En esta sección se estudia el proceso de la transformación de datos analógicos en señales digitales. Estrictamente hablando, es más correcto referirse a este proceso como la conversión de datos analógicos a datos digitales; este proceso es también denominado digitalización. Una vez que los datos analógicos se convierten a digitales, puede ocurrir lo siguiente:

1. Los datos digitales se transmiten usando NRZ-L. En este caso, se habrá realizado directamente una conversión de datos analógicos a señales digitales.
2. Los datos digitales se codifican usando un código diferente al NRZ-L. Por tanto, en este caso se necesitaría un paso adicional.
3. Los datos digitales se convierten en señales analógicas, usando una de las técnicas de modulación presentadas en la Sección 5.2.

Este último procedimiento, aparentemente curioso, se muestra en la Figura 5.9, en la que se representan datos de voz tras ser digitalizados, se han convertido posteriormente en señales analógicas tipo ASK. Este procedimiento permite la transmisión digital, en el sentido definido en el Capítulo 3. Los datos de voz, al haber sido digitalizados, se pueden procesar como si fueran digitales, incluso cuando los requisitos de la transmisión (por ejemplo la utilización de microondas) fuercen la utilización de señales analógicas.

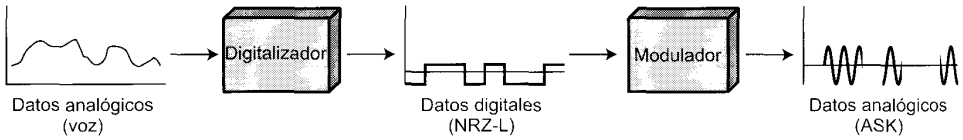


Figura 5.9. Digitalización de datos analógicos.

El dispositivo que se utiliza para la conversión de los datos analógicos en digitales, y que posteriormente recupera los datos analógicos iniciales de los digitales se denomina codec (codificador-decodificador). En esta sección se examinarán las dos técnicas más importantes que se usan en los codecs, es decir, la modulación por impulsos codificados y la modulación delta. La sección concluye comparando sus prestaciones.

MODULACIÓN POR CODIFICACIÓN DE IMPULSOS

La modulación por codificación de impulsos (PCM, Pulse Code Modulation) se basa en el teorema de muestreo, que dice:

> Si una señal $f(t)$ se muestrea a intervalos regulares de tiempo con una frecuencia mayor que el doble de la frecuencia más alta de la señal, entonces las muestras así obtenidas contienen toda la información de la señal original. La función $f(t)$ se puede reconstruir a partir de estas muestras mediante la utilización de un filtro pasa baja.

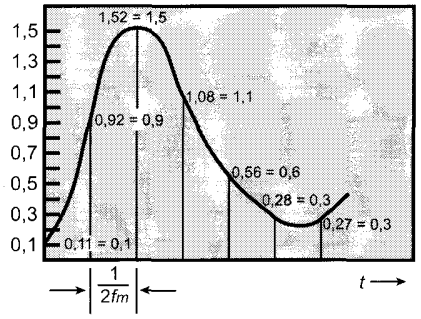
Para el lector interesado, en el Apéndice 5A se desarrolla la demostración del teorema anterior. Si los datos de voz se limitan a frecuencias por debajo de 4.000 Hz, lo que significa que la inteligibilidad se conserva, para caracterizar completamente la señal de voz serían suficientes obtener 8.000 muestras por segundo. Obsérvese que aún se trata de muestras analógicas, denominadas muestras PAM (Pulse Amplitude Modulation). Para convertir las muestras PAM a digital, se les debe asignar un código digital a cada una de ellas. En la Figura 5.10 se muestra un ejemplo en el que cada muestra se aproxima mediante su cuantización en uno de 16 posibles niveles. Por lo tanto, cada una de las muestras se puede representar por 4 bits. Pero, ya que los niveles cuantizados son sólo aproximaciones, es imposible recuperar completamente la señal original. Utilizando muestras de 8 bits, lo que permite 256 niveles de cuantización, la calidad de la señal de voz resultante es comparable a la que se consigue mediante transmisión analógica. Nótese que esto implica que para una única señal de voz se necesitan 8.000 muestras por segundo × 8 bits por muestra = 64 kbps.

Así pues, la técnica PCM genera la señal digital tomando como entrada la señal analógica continua en el tiempo y amplitud. La señal digital resultante consiste en bloques de n bits, donde cada número de n bits corresponde a la amplitud de un impulso PCM. En el receptor este procedimiento se invierte para obtener así la señal analógica. Obsérvese, no obstante, que este proceso viola las condiciones exigidas por el teorema de muestreo. Al cuantificar los impulsos PAM, la señal original sólo se aproxima, por lo que no podrá ser recuperada con exactitud. Este efecto se denomina error de cuantización o ruido de cuantización. La razón señal-ruido para el ruido de cuantización se puede expresar como [GIBS93]:

$$\text{SNR} = 20 \log 2^n + 1{,}76\,\text{dB} = 6{,}02n + 1{,}76\,\text{dB}$$

Por tanto, cada bit adicional que se use en la cuantización aumentará la razón señal-ruido en 6 dB, es decir un factor 4.

Generalmente, el esquema PCM se refina mediante técnicas denominadas de codificación no lineal, en las que los niveles de cuantización no están igualmente separados. El problema que surge al considerar separaciones entre niveles iguales es que el valor medio del valor absoluto del error para cada muestra es el mismo, independientemente del nivel de la señal. Por consiguiente, los niveles de señal



(a)

Dígitos	Equivalentes en binario	Forma de onda PCM
0	0000	
1	0001	
2	0010	
3	0011	
4	0100	
5	0101	
6	0110	
7	0111	
8	1000	
9	1001	
10	1010	
11	1011	
12	1100	
13	1101	
14	1110	
15	1111	

(b)

Figura 5.10. Modulación por codificación de impulsos.

más pequeños estarán en términos relativos más distorsionados. Al usar un número mayor de niveles de cuantización para señales de poca amplitud, y un número menor para las señales de mayor amplitud, se consigue una reducción en la distorsión media de la señal (por ejemplo, véase la Figura 5.11).

El mismo efecto se puede conseguir usando cuantización uniforme pero ahora, comprimiendo y posteriormente expandiendo la señal analógica de entrada. Este procedimiento consiste en comprimir a la entrada el rango de intensidades de la señal, asignando a las señales de baja amplitud una ganancia superior que a las señales de amplitud mayor. En la salida se realiza la operación contraria. En la Figura 5.12 se representa una función típica de compresión-expansión.

La codificación no lineal puede conseguir una mejora significativa de la SNR de un sistema PCM. Para las señales de voz se han conseguido mejoras de 24 a 30 dB.

MODULACIÓN DELTA (DM, DELTA MODULATION)

Para mejorar las prestaciones de la codificación PCM, o para reducir su complejidad, se ha desarrollado un gran número de técnicas. Una de las alternativas de mayor aceptación es la modulación delta (DM).

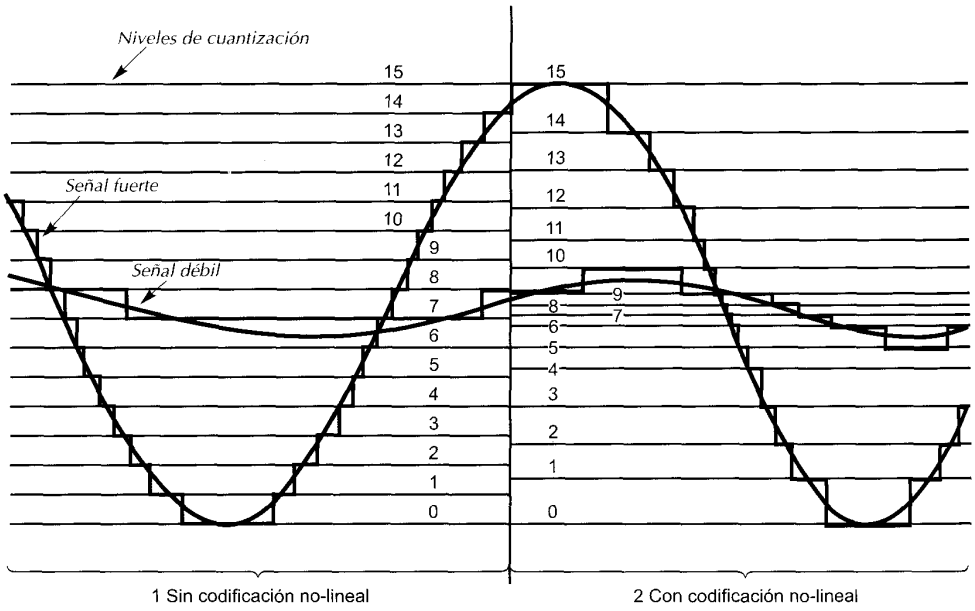


Figura 5.11. Efecto de la codificación no-lineal.

En la modulación delta, la entrada analógica se aproxima mediante una función escalera que en cada intervalo de muestreo (T_S) sube o baja un nivel de cuantización (δ). En la Figura 5.13 se muestra un ejemplo, en el que la función escalera está superpuesta a la señal original. La característica principal de la función escalera es que su comportamiento es binario: en cada instante de muestreo la función sube o baja una cantidad constante [δ]. Por tanto, la salida del modulador delta se puede representar mediante un único bit para cada muestra. Resumiendo, se obtiene una cadena de bits que aproxima a la derivada de la señal analógica de entrada en lugar de a la propia amplitud: se genera un 1 si la función escalera sube en el siguiente intervalo, o un 0 en cualquier otro caso.

La transición (hacia arriba o hacia abajo) que ocurre en cada intervalo de muestreo se elige de tal manera que la función escalera aproxime tanto como sea posible a la forma de onda de la señal original. La Figura 5.14 muestra este procedimiento, que básicamente consiste en un mecanismo de realimen-

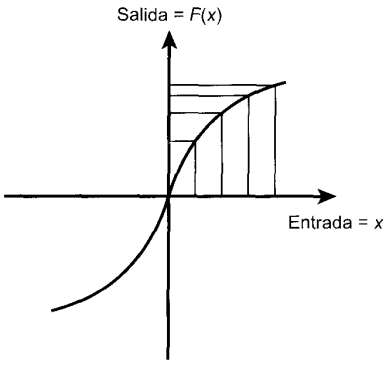


Figura 5.12. Función de compresión típica.

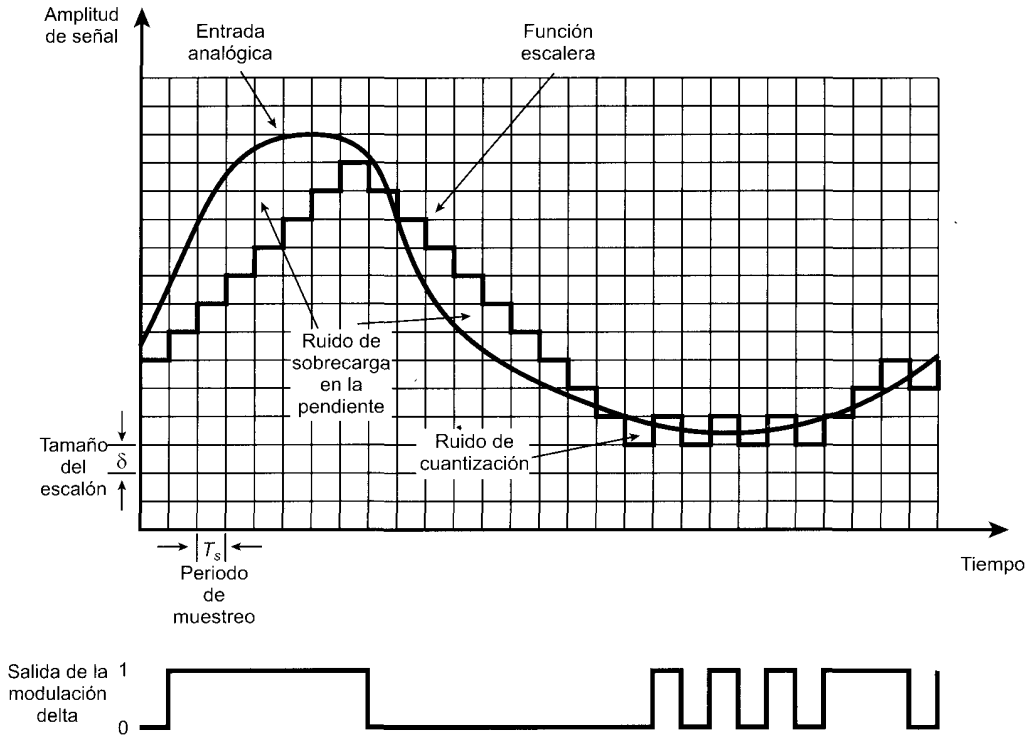


Figura 5.13. Ejemplo de modulación delta.

tación. Al transmitir ocurre lo siguiente: por cada intervalo de muestreo, la señal analógica de entrada se compara con el valor más reciente de la función escalera. Si el valor de la forma de onda muestreada supera el de la función escalera, se genera un 1, en otro caso se generará un 0. Por tanto, la función escalera siempre se modifica en la dirección de la señal de entrada. La salida del proceso DM es por tanto una secuencia binaria que se puede usar en el receptor para reconstruir la función escalera. Esta función reconstruida, se podrá suavizar mediante algún procedimiento de integración o mediante un filtro pasa baja que genere una aproximación analógica a la señal analógica de entrada.

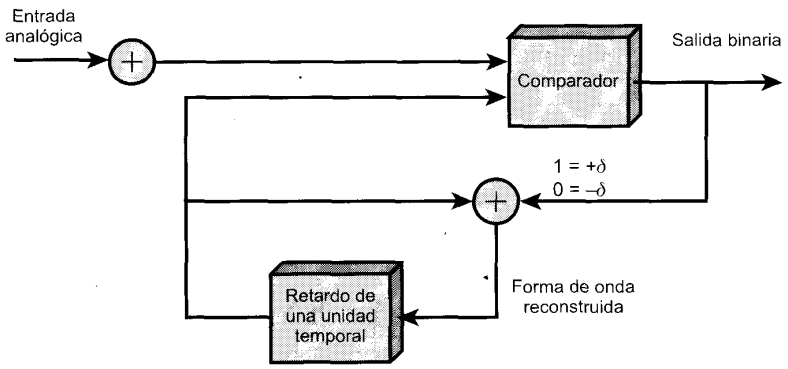
Hay dos parámetros importantes en el esquema DM: el tamaño del cuanto asignado a cada dígito binario, δ, y la frecuencia de muestreo. Como se muestra en la Figura 5.13, δ se debe elegir tal que se consiga un compromiso entre los dos tipos de error o ruido. Cuando la señal analógica varíe muy lentamente, habrá ruido de cuantización, siendo este ruido tanto mayor cuanto mayor sea δ. Por contra, cuando la señal de entrada cambie tan rápidamente que la función escalera no la pueda seguir, se producirá un ruido de sobrecarga en la pendiente. Este ruido aumenta al disminuir δ.

Debe quedar claro que la precisión de este esquema se puede mejorar aumentando la frecuencia de muestreo. No obstante, esto incrementará la velocidad de transmisión de los datos a la salida.

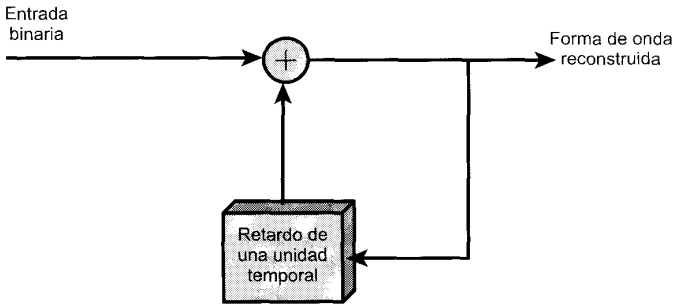
La principal ventaja de la DM respecto a la PCM es su sencillez de implementación. No obstante, PCM consigue, en general, una mejor SNR para la misma velocidad de transmisión.

PRESTACIONES

Se puede conseguir una buena calidad de reproducción de voz con 128 niveles, es decir con 7 bits ($2^7 = 128$). La señal de voz, siendo conservador, ocupa un ancho de banda de 4 kHz. Por tanto, de



(a) Transmisión



(b) Recepción

Figura 5.14. Modulación delta.

acuerdo con el teorema de muestreo, las muestras se deben tomar a una razón de 8.000 muestras por segundo. Esto implica que para los datos digitales codificados en PCM se obtiene una velocidad de transmisión igual a $8.000 \times 7 = 56$ kbps.

Veamos que significa esto desde el punto de vista del ancho de banda necesario. Una señal analógica de voz ocupa 4 kHz. Esta señal analógica de 4 kHz se convierte mediante PCM en una señal digital a 56 kbps. De acuerdo con el criterio de Nyquist (véase Capítulo 3) esta señal digital necesitaría aproximadamente 28 kHz de ancho de banda. Este hecho será tanto más evidente cuanto mayor sea el ancho de banda de la señal. Por ejemplo, un esquema típico de PCM para la televisión en color utiliza código de 10 bits, que se transmite a 92 Mbps para señales de 5,66 MHz de ancho de banda. A pesar de lo elevado de estas cifras, las técnicas de transmisión digital se utilizan cada vez más en la transmisión de datos analógicos. Este hecho está justificado por las siguientes razones:

- No hay ruido aditivo debido a que se usan repetidores en lugar de amplificadores.
- Como posteriormente se verá, para señales digitales en lugar de utilizar multiplexación por división en frecuencias (FDM, Frecuency-division multiplexing), se usa la multiplexación por división en el tiempo (TDM, Time-division multiplexing). En TDM no hay ruido de intermodulación, característico de la FDM.
- La conversión a señales digitales permite el uso de técnicas más eficaces de conmutación.

Es más, se han desarrollando técnicas que proporcionen códigos más eficaces. Para el caso de la voz, un objetivo que parece razonable está en torno a los 4 kbps. Para la codificación de señales de vídeo, se puede usar el hecho de que la mayor parte de los elementos de la imagen no cambian cuadro a cuadro. Las técnicas de codificación que aprovechan las dependencias existentes entre cuadros adyacentes, permiten reducir la velocidad de transmisión para la señal de vídeo hasta 15 Mbps; y, para las secuencias que varíen poco, como, por ejemplo, una teleconferencia, se puede reducir hasta 64 kbps o incluso menos.

Finalmente, hay que decir que el uso de un sistema de telecomunicación dará lugar tanto a una conversión de digital a analógico como de analógico a digital. La mayoría de los terminales en las redes de telecomunicación son analógicos, y las redes en sí utilizan una mezcla de técnicas y dispositivos analógicos y digitales. Por tanto, los datos digitales en el terminal del usuario se deberán convertir a analógicos mediante un modem, posteriormente se deberán digitalizar mediante un codec y posiblemente todavía sufran conversiones adicionales antes de alcanzar su destino final.

Debido a esto, los servicios de telecomunicación gestionan señales analógicas que representan tanto voz como datos digitales. Las características de las formas de las ondas respectivas son bastante diferentes. Mientras que la señal de voz tiende a estar concentrada en la parte baja del ancho de banda (véase Figura 3.9), la codificación analógica de señales digitales tiene una distribución espectral más plana, conteniendo por tanto más componentes a altas frecuencias. Algunos estudios han demostrado que, debido a la presencia de estas altas frecuencias, en la digitalización de señales analógicas que representan datos digitales, es preferible el uso de técnicas tipo PCM, en lugar de optar por procedimientos similares a la DM.

5.4. DATOS ANALÓGICOS, SEÑALES ANALÓGICAS

La modulación se ha definido como el proceso de combinar una señal de entrada $m(t)$ y una portadora a frecuencia f_c para producir una señal $s(t)$ cuyo ancho de banda esté (normalmente) centrado en torno a f_c. Para el caso de datos digitales, la justificación de la modulación es evidente: será necesaria cuando exista sólo la posibilidad de transmisión analógica, permitiendo así convertir los datos digitales en analógicos. Sin embargo, cuando los datos son analógicos la justificación no es tan evidente. Después de todo, las señales de voz se transmiten a través de líneas telefónicas usando su espectro original (esto se denomina transmisión en banda base). Para la transmisión de señales analógicas mediante modulación analógica, existen fundamentalmente dos razones:

- Para llevar a cabo una transmisión más efectiva puede que se necesite una frecuencia mayor. En los medios no guiados es prácticamente imposible transmitir señales en banda-base ya que el tamaño de las antenas tendría que ser de varios kilómetros de diámetro.
- La modulación permite la multiplexación por división en frecuencias, técnica muy importante que se estudiará en el Capítulo 8.

En esta sección consideraremos las técnicas más importantes para la modulación de datos analógicos: la modulación en amplitud (AM, Amplitude Modulation), la modulación en frecuencias (FM, Frecuency Modulation) y la modulación en fase (PM, Phase Modulation). Al igual que antes, los tres parámetros básicos de la portadora se utilizan para llevar a cabo la modulación.

MODULACIÓN EN AMPLITUD

La modulación en amplitud (AM), mostrada en la Figura 5.15, es la técnica más sencilla de modulación. Matemáticamente el proceso se puede expresar como

$$s(t) = [1 + n_a x(t)] \cos 2\pi f_c t$$

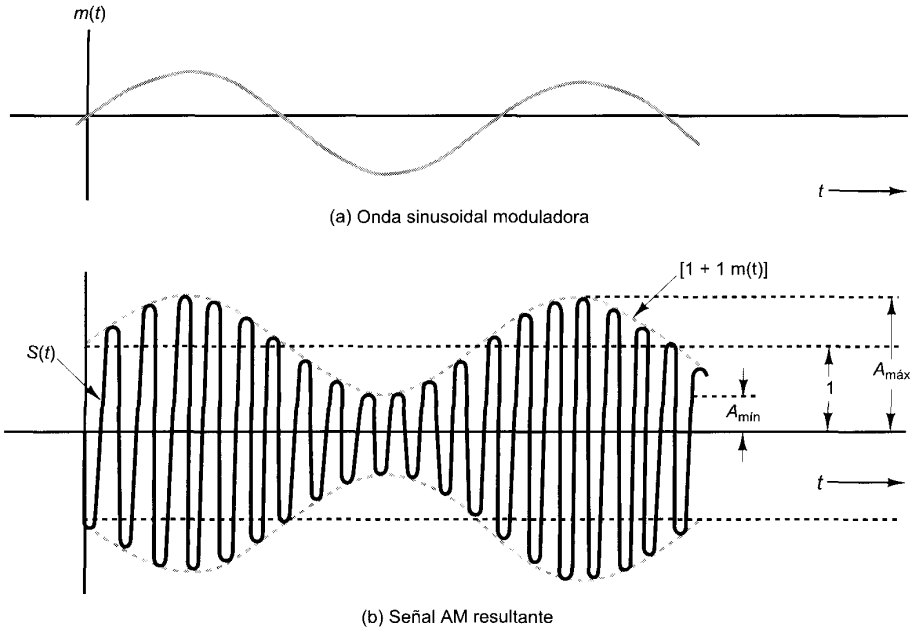


Figura 5.15. Modulación en amplitud.

donde $\cos 2\pi f_c t$ es la portadora y $x(t)$ es la señal de entrada, ambas normalizadas a la amplitud unidad. El parámetro n_a, denominado índice de modulación, es el cociente entre la amplitud de la señal de entrada y la amplitud de la portadora. De acuerdo con la notación previa, la señal de entrada será $m(t) = n_a x(t)$. El «1» en la expresión anterior es una componente de continua que evita pérdidas de información, como se explica a continuación. Este esquema también se denomina transmisión de portadora con doble banda lateral (DSBTC, double sideband transmitted carrier).

Ejemplo

Obtener la expresión de $s(t)$ si $x(t)$ es la señal moduladora en amplitudes $\cos 2\pi f_m t$.

Se tiene que

$$s(t) = [1 + n_a \cos 2\pi f_m t] \cos 2\pi f_c t$$

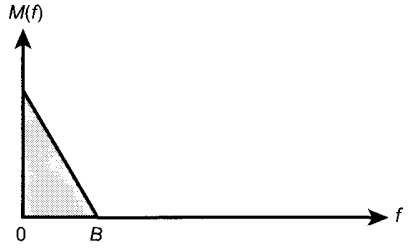
Utilizando la identidad trigonométrica, la expresión anterior se puede desarrollar, obteniéndose

$$s(t) = \cos 2\pi f_c t + \frac{n_a}{2} \cos 2\pi (f_c - f_m) t + \frac{n_a}{2} \cos 2\pi (f_c + f_m) t$$

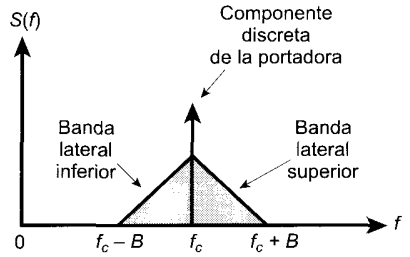
La señal resultante tiene una componente a la frecuencia original de la portadora, más un par de componentes adicionales separadas f_m hertzios de la frecuencia de la portadora.

A partir de la expresión anterior y de la Figura 5.15, se puede observar que AM implica la multiplicación de la señal de entrada por la portadora. La envolvente de la señal resultante es $[1 + n_a x(t)]$ y, mientras que $n_a < 1$, la envolvente será una reproducción exacta de la señal original. Si $n_a > 1$, la envolvente cruzará el eje del tiempo perdiéndose así información.

Es instructivo observar el espectro de la señal AM. En la Figura 5.16, se muestra un ejemplo. El espectro está formado por la portadora original más el espectro de la señal de entrada trasladada a f_c. La



(a) Espectro de la señal moduladora



(b) Espectro de una señal AM con portadora a f_C

Figura 5.16. Espectro de una señal AM.

parte del espectro para la que $|f| > |f_c|$ es la *banda lateral superior*, y la porción del espectro para la que $|f| > |f_c|$ es la *banda lateral inferior*. Tanto la banda superior como la inferior son réplicas exactas del espectro original $M(f)$, estando la banda inferior invertida en frecuencias. A modo de ejemplo, considérese la modulación de la señal de voz, con un espectro comprendido entre 300 y 3.000 Hz, sobre una portadora de 60 kHz. La señal resultante estará constituida por la banda superior, entre 60,3 y 63 kHz, y la banda inferior entre 57 y 59,7 kHz, además de la portadora de 60 Hz. Una relación importante es

$$P_t = P_c\left(1 + \frac{n_a^2}{2}\right)$$

donde P_t es la potencia total transmitida en $s(t)$, y P_c es la potencia transmitida en la portadora. Es deseable hacer n_a tan grande como sea posible de tal manera que la mayor parte de la potencia de la señal transmitida se use para transportar información. Ahora bien, n_a debe mantenerse menor que 1.

Debería estar claro que $s(t)$ contiene componentes innecesarias, ya que cada una de las bandas laterales contiene todo el espectro de $m(t)$. Una variante de AM, denominada AM de banda lateral única (SSB, single sideband), aprovecha este hecho, transmitiendo sólo una de las bandas laterales, eliminando la otra y la portadora. Las principales ventajas de esta aproximación son:

- Solamente se necesita la mitad del ancho de banda, es decir $B_T = B$, donde B es el ancho de banda de la señal original. En DSBTC, $B_T = 2B$.
- Se necesita menos potencia ya que se ahorra la potencia correspondiente a la portadora y a la otra banda lateral. Otra variante es la doble banda lateral con portadora suprimida (DSBSC, double sideband supressed carrier), en la que se elimina la frecuencia portadora y se transmiten las dos bandas laterales. Con este procedimiento se ahorra algo de potencia, pero se utiliza igual ancho de banda que en DSBTC.

La desventaja de suprimir la portadora es que dicha componente se puede usar para la sincronización. Por ejemplo, supóngase que la señal analógica original es una forma de onda ASK que codifica datos digitales. El receptor necesitará conocer dónde comienza cada bit para así interpretar correctamente los datos. Una portadora constante proporciona un mecanismo de sincronización con el que se puede temporizar la llegada de los bits. Una aproximación que implica un compromiso es la denominada banda lateral vestigial (VSB, vestigial sideband), en la que se usa una de las bandas laterales y una portadora de potencia reducida.

MODULACIÓN EN ÁNGULO

La modulación en frecuencias (FM, frecuency modulation) y la modulación en fase (PM, Phase modulation) son casos particulares de la denominada modulación en ángulo. La señal modulada se expresa como

$$s(t) = A_c \cos [2\pi f_c t + \phi(t)]$$

En la modulación en fase, la fase es proporcional a la señal moduladora:

$$\phi(t) = n_p m(t)$$

donde n_p es el índice de modulación en fase.

En la modulación en frecuencias, la derivada de la fase es proporcional a la señal moduladora:

$$\phi'(t) = n_f m(t)$$

donde n_f es el índice de modulación en frecuencias.

Las anteriores definiciones se pueden clarificar mediante la siguiente argumentación matemática. La fase de $s(t)$ en cualquier instante dado es $2\pi f_c t + \phi(t)$. La desviación de la fase instantánea respecto de la señal portadora es $\phi(t)$. En la modulación en fase (PM), esta desviación instantánea de fase es proporcional a $m(t)$. Debido a que la frecuencia se puede definir como la velocidad de cambio de la fase de una señal, la frecuencia instantánea de $s(t)$ viene dada por

$$2\pi f_i(t) = \frac{d}{dt}[2\pi f_c t + \phi(t)]$$

$$f_i(t) = f_c + \frac{1}{2\pi}\phi'(t)$$

y la desviación de la frecuencia instantánea respecto a la frecuencia de la portadora es $\phi'(t)$, que en FM es proporcional a $m(t)$.

En la Figura 5.17 se muestra la modulación en amplitud, frecuencia y fase de una señal seno. El aspecto de las señales FM y PM son muy parecidas. De hecho, es imposible diferenciarlas sin tener un conocimiento previo de la función de modulación.

Con relación a FM se pueden realizar las siguientes observaciones. La desviación de pico ΔF se puede obtener como

$$\Delta F = \frac{1}{2\pi} n_f A_m \text{ Hz}$$

donde A_m es al valor máximo de $m(t)$. Por tanto, un incremento en la amplitud de $m(t)$ aumentará ΔF, lo que, intuitivamente, debería aumentar el ancho de banda transmitido B_T. Sin embargo, como se evidencia a partir de la Figura 5.17, esto no incrementa el nivel de potencia medio de la señal FM, igual a $A_c^2/2$. Esto es diferente a lo que ocurre en AM, ya que el nivel de modulación afecta a la potencia de la señal AM pero no afecta a su ancho de banda.

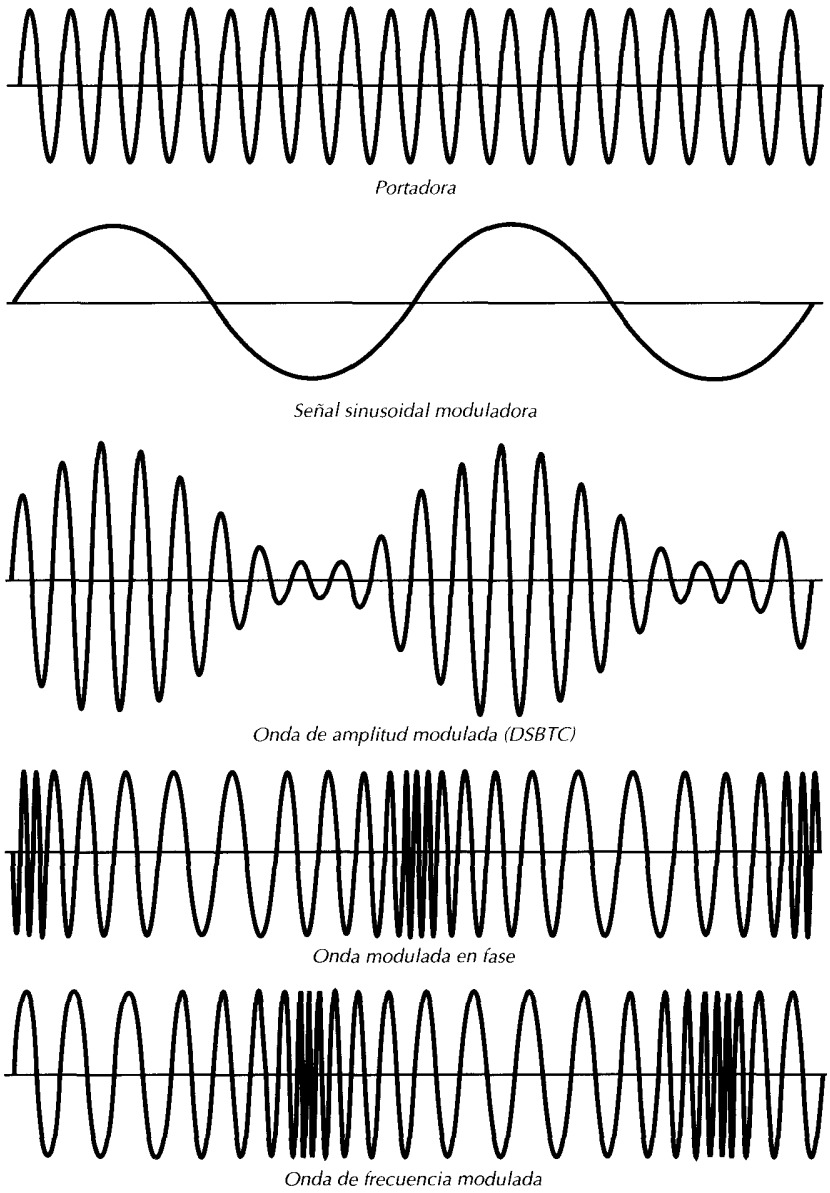


Figura 5.17. Modulación en amplitud, fase y frecuencia de una portadora sinusoidal mediante una señal sinusoidal.

Ejemplo

Obtener la expresión de $s(t)$ si $\phi(t)$ la señal modulada en fase, es $n_p \cos 2\pi f_m t$. Supóngase que $A_c = 1$. Entonces, se obtiene directamente que

$$s(t) = \cos [2\pi f_c t + n_p \cos 2\pi f_m t]$$

La desviación instantánea de fase respecto a la señal portadora es $n_p \cos \pi f_m t$. El ángulo de fase de la señal varía respecto de su valor no modulado como una sencilla señal sinusoidal, siendo el valor de pico de la desviación en fase igual a n_p.

La expresión anterior se puede desarrollar teniendo en cuenta las identidades trigonométricas de Bessel, es decir:

$$s(t) = \sum_{n=-\infty}^{\infty} J_n(n_p) \cos\left(2\pi f_c t + 2\pi f_m t + \frac{n\pi}{2}\right)$$

donde $J_n(n_p)$ es la n-ésima función de Bessel de primera clase. Usando la propiedad

$$J_{-n}(x) = (-1)nJ_n(x)$$

se puede reescribir como

$$s(t) = J_0(n_p) \cos 2\pi f_c t + \sum_{n=-\infty}^{\infty} J_n(n_p)\left[\cos\left(2\pi(f_c + nf_m)t + \frac{n\pi}{2}\right) + \cos\left(2\pi(f_c - nf_m)t + \frac{(n+2)\pi}{2}\right)\right]$$

La señal resultante tiene una componente a la frecuencia de la portadora original más un conjunto de bandas laterales desplazadas respecto de f_c por todos los posibles múltiplos de f_m. Para $n_p \ll 1$, los términos de orden superior caen rápidamente.

Ejemplo

Obtener la expresión de $s(t)$ si $\phi'(t)$, la señal moduladora en frecuencias, es de la forma $-n_f \operatorname{sen}(2\pi f_m t)$. La expresión de $\phi'(t)$ se ha elegido por cuestiones de sencillez. Se tiene que

$$\phi(t) = -\int n_f \operatorname{sen} 2\pi f_m t \, dt = \frac{n_f}{2\pi f_m} \cos 2\pi f_m t$$

por tanto

$$s(t) = \cos\left[2\pi f_c t + \frac{n_f}{2\pi f_m} \cos 2\pi f_m t\right]$$

$$s(t) = \cos\left[2\pi f_c t + \frac{\Delta F}{f_m} \cos 2\pi f_m t\right]$$

La desviación de la frecuencia instantánea respecto de la frecuencia de la portadora es $-n_f \operatorname{sen}(2\pi f_m t)$. La frecuencia de la señal varía sinusoidalmente en torno a su valor no modulado, siendo su desviación máxima igual a n_f radianes/segundo.

Sustituyendo $\Delta F/f_m$ por n_p la expresión para la señal FM es idéntica a la correspondiente señal PM, es decir, el desarrollo de Bessel es el mismo.

Al igual que en AM, tanto FM como PM dan lugar a una señal cuyo ancho de banda está centrado en torno a f_c. Sin embargo, a continuación se verá que la amplitud de sus anchos de banda son muy diferentes. La modulación en amplitud es un proceso lineal que produce frecuencias iguales a la suma y a la diferencia de la portadora y las componentes de la señal moduladora. Por tanto para AM, se tiene que

$$B_T = 2B$$

No obstante, la modulación en ángulo incluye un término de la forma $\cos(\phi(t))$, que evidentemente no es lineal y generará un gran rango de frecuencias. En definitiva, para una señal moduladora sinusoidal

de frecuencia f_m, $s(t)$ contendrá componentes en $f_c + f_m$, $f_c + 2f_m$, y así sucesivamente. En el caso más general, para la transmisión de una señal FM o PM se necesitará un ancho de banda infinito. En la práctica una buena aproximación nemotécnica es la denominada ley de Carson [COUC97], dada por

$$B_T = 2(\beta + 1)B$$

donde

$$\beta = \begin{cases} n_p A_m & \text{para PM} \\ \dfrac{\Delta F}{B} = \dfrac{n_f A_m}{2\pi B} & \text{para FM} \end{cases}$$

La expresión para FM se puede reescribir de la siguiente manera

$$B_T = 2\Delta F + 2B$$

Luego tanto FM como PM necesitan un ancho de banda mayor que AM.

MODULACIÓN EN AMPLITUD EN CUADRATURA, QAM (QUADRATURE AMPLITUDE MODULATION)

QAM es una técnica habitual de señalización analógica que se utiliza en ADSL (Línea de abonado digital y asimétrica) (Asymmetric Digital Subscriber Line), técnica que se explicará en el Capítulo 8. Esta técnica de modulación es una combinación de modulación en fase y en amplitud. En QAM se aprovecha el hecho de que es posible enviar simultáneamente dos señales diferentes sobre la misma portadora, utilizando dos réplicas de la misma desplazadas entre sí 90°. En QAM cada una de las dos portadoras es modulada usando ASK. Las dos señales independientes se transmiten sobre el mismo medio. En el receptor, las dos señales se demodulan, combinándose para reproducir la señal binaria de entrada.

En la Figura 5.18 se muestra en términos generales el esquema de modulación QAM. La entrada al sistema es una cadena de bits con velocidad igual a R bps. Esta cadena se separa en dos secuencias de $R/2$ bps cada una, tomando bits alternativamente. En el diagrama, la secuencia de arriba se modula mediante ASK sobre una portadora de frecuencia f_c; este procedimiento se lleva a cabo sin más que multiplicar cada bit por la portadora. Por tanto, un cero binario será representado mediante la ausencia de portadora, mientras que un uno binario se representará mediante la presencia de una señal portadora de amplitud constante. Esta misma portadora se desplaza en 90° y a su vez se usa para la modulación

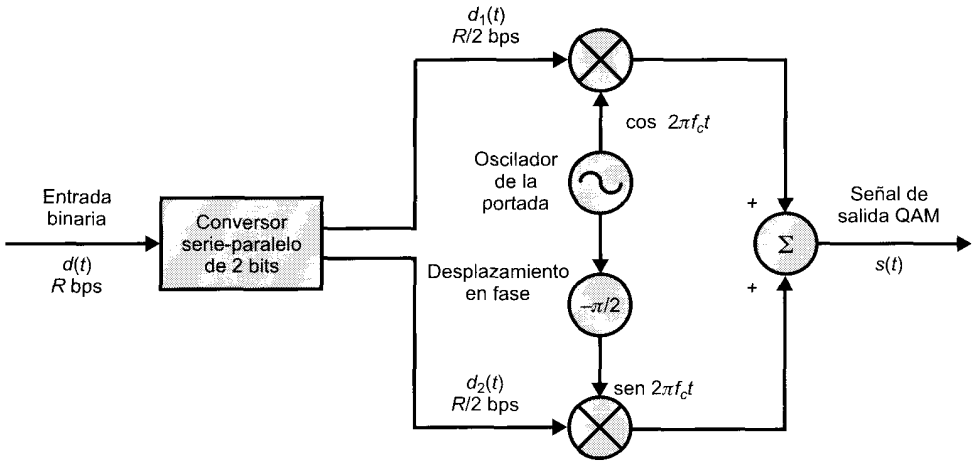


Figura 5.18. Modulador QAM.

ASK de la secuencia binaria de abajo. Las dos señales moduladas se suman y posteriormente se transmiten. La señal transmitida, por tanto, se puede expresar como

$$s(t) = d_1(t) \cos 2\pi f_c t + d_2(t) \operatorname{sen} 2\pi f_c t$$

Si se utiliza un esquema ASK con dos niveles, entonces cada una de las dos secuencias binarias podrá representarse mediante dos estados, que combinadas dan lugar a una señal con 4 (2 × 2) posibles estados de señalización. Si se usa ASK con cuatro niveles (esto es, cuatro niveles diferentes de amplitud), entonces la secuencia combinada podrá tomar uno de entre 16 (4 × 4) estados. En la práctica se implementan sistemas con 64 e incluso 256 niveles. Para un ancho de banda dado, cuanto mayor sea el número de niveles, mayor será la velocidad de transmisión posible. Desde luego, como ya se ha comentado previamente, cuanto mayor sea el número de estados mayor será la tasa potencial de errores por bit debida al ruido y a la atenuación.

5.5. ESPECTRO EXPANDIDO (SPREAD SPECTRUM)

Una técnica de transmisión que cada vez es más popular es la que se conoce por espectro expandido. Siendo rigurosos, esta técnica en realidad no se puede encuadrar en ninguna de las técnicas estudiadas en este capítulo, ya que se puede usar para transmitir tanto señales analógicas como digitales, utilizando una señal analógica.

La técnica del espectro expandido se desarrolló inicialmente para aplicaciones militares y para servicios de inteligencia. La idea básica consiste en expandir la información de la señal sobre un ancho de banda mayor, para con ello dificultar las interferencias y su posible intercepción. Dentro de éstas, el primer tipo se denomina salto en frecuencias[6]. Una versión más reciente es la denominada espectro expandido con secuencia directa. Estas dos técnicas se utilizan en la actualidad en las redes de datos inalámbricas, además de en otras aplicaciones como, por ejemplo, en los teléfonos inalámbricos.

En la Figura 5.19 se resaltan los puntos clave de cualquier sistema de espectro expandido. A partir de los datos de entrada, el codificador del canal genera una señal analógica con un ancho de banda relativamente estrecho en torno a su frecuencia central. Esta señal se modula posteriormente usando una secuencia de dígitos aparentemente aleatorios denominada secuencia pseudoaleatoria. Con esta modulación lo que se pretende es aumentar drásticamente el ancho de banda (expandir el espectro) de la señal a transmitir. En el receptor, se usa la misma secuencia de dígitos para demodular la señal de espectro expandido. Y por último, la señal demodulada se decodifica para recuperar los datos originales.

Llegados a este punto, es pertinente comentar algo sobre la secuencia pseudoaleatoria. Esta secuencia de números se genera mediante un algoritmo a partir de un valor inicial denominado semilla. El

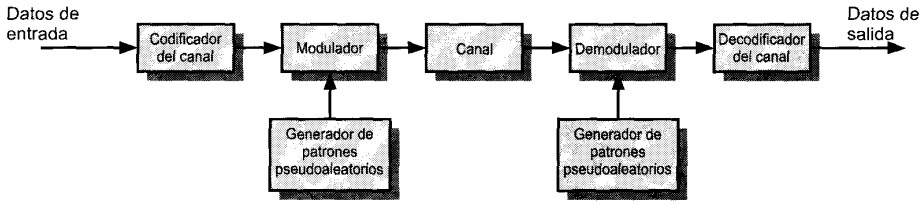


Figura 5.19. Modelo genérico para un sistema de comunicación digital con espectro expandido.

[6] Por increíble que parezca, la técnica del espectro expandido (usando saltos de frecuencia) fue inventada por la estrella de Holywood Hedy Lamarr en 1940 a los 26 años de edad. Ella, junto con un socio, consiguieron una patente en 1942 («U.S. patent 2,292,387» el 11 de agosto de 1942). Lamarr consideró que ésa iba a ser su contribución a la causa de la guerra, por lo que nunca obtuvo beneficios por su invención. Esta interesante historia se puede completar en [MEEK90].

algoritmo es determinista, por lo que la secuencia de números que genera no es estadísticamente aleatoria. No obstante, si el algoritmo es suficientemente bueno, las secuencias resultantes superarán un buen número de tests de aleatoriedad. Estos números se denominan con frecuencia números pseudoaleatorios[7]. La clave aquí reside en el hecho de que a menos que se conozca tanto el algoritmo como la semilla, es casi imposible predecir la secuencia. Por tanto, sólo los receptores que conozcan esta información serán capaces de decodificar adecuadamente la señal.

SALTO EN FRECUENCIA

En este esquema, la señal se emite sobre una serie de radio-frecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia por cada fracción de segundo transcurrida. El receptor captará el mensaje saltando de frecuencia en frecuencia síncronamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits.

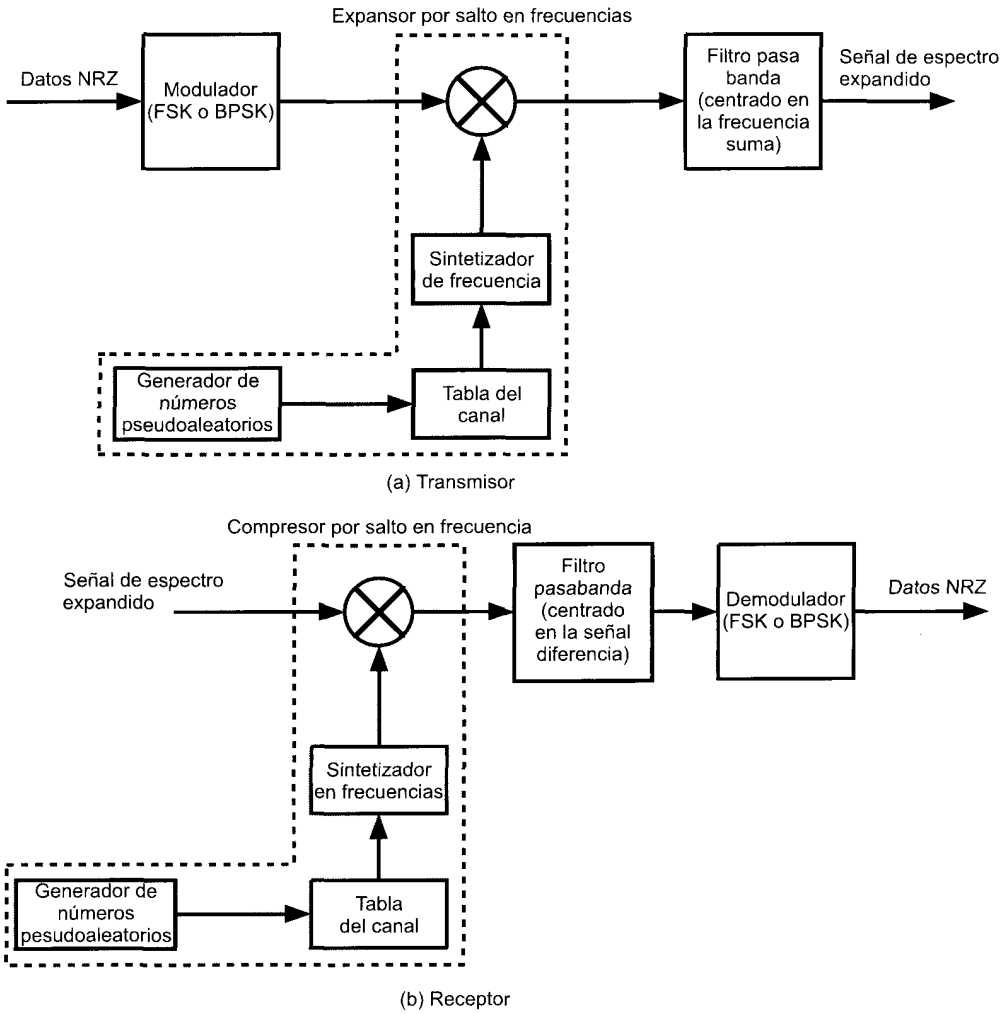


Figura 5.20. Sistema de espectro expandido mediante salto en frecuencias.

[7] Para obtener más información sobre los números pseudoaleatorios véase [STAL99].

El diagrama típico de un sistema con salto de frecuencias se muestra en la Figura 5.20. En la transmisión, los datos digitales constituyen la entrada del modulador usando algún tipo de esquema de codificación digital a analógico, como, por ejemplo, desplazamiento en frecuencias (FSK, Frequency-Shift Keying) o desplazamiento en fase binario (BPSK, Binary Phase Shift Keying). La señal resultante estará centrada en torno a alguna frecuencia base. Se utiliza un generador de números pseudoaleatorios que servirá como puntero a una tabla de frecuencias. A partir de dicha tabla se selecciona una frecuencia en cada uno de los intervalos considerados. Esta frecuencia es modulada por la señal generada en el modulador inicial, dando lugar a una señal nueva con la misma forma pero ahora centrada en torno a la frecuencia elegida según la tabla anterior.

En el receptor, la señal de espectro expandido se demodula usando la misma secuencia de frecuencias obtenidas a través de la tabla y posteriormente se demodula la señal resultante para producir los datos de salida.

Por ejemplo, si se emplea FSK, el modulador selecciona una de entre dos frecuencias, digamos f_0 o f_1, de acuerdo con el símbolo binario a transmitir (0 o 1). La señal binaria FSK resultante se traslada en frecuencias una cantidad que se determina a partir de la secuencia de salida del generador de números pseudoaleatorios. Así, si en el instante i se selecciona la frecuencia f_i, la señal en ese instante será $f_i + f_0$ o $f_i + f_1$.

SECUENCIA DIRECTA

En este esquema, cada bit de la señal original se representa mediante varios bits de la señal transmitida; a este procedimiento se le denomina código de compartición. Este código expande la señal a una banda de frecuencias más ancha, directamente proporcional al número de bits que se usen. Es decir, un código de compartición de 10 bits expande la señal a una banda de frecuencias de anchura 10 veces mayor que un código de compartición de 1 bit.

Una técnica de espectro expandido por secuencia directa consiste en combinar la secuencia de dígitos de entrada con la cadena de bits pseudoaleatorios utilizando la función OR-exclusiva. En la Figura 5.21

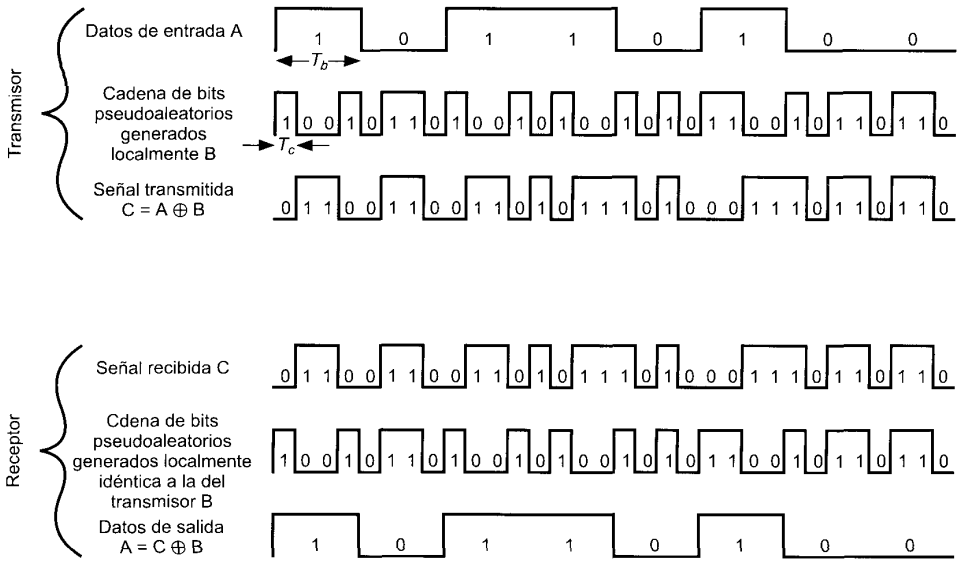
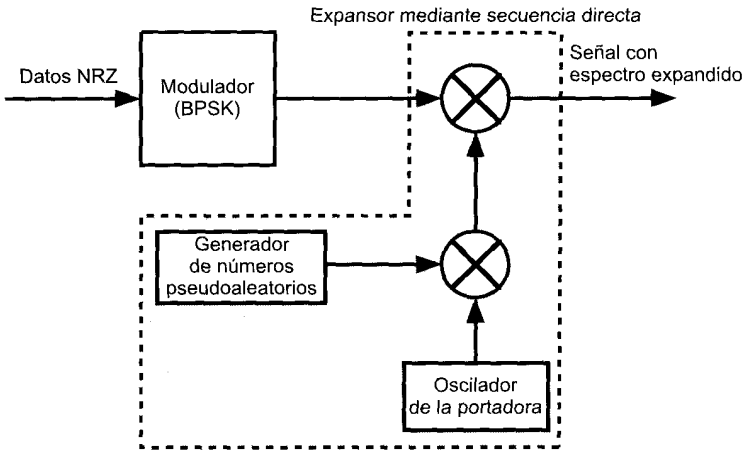


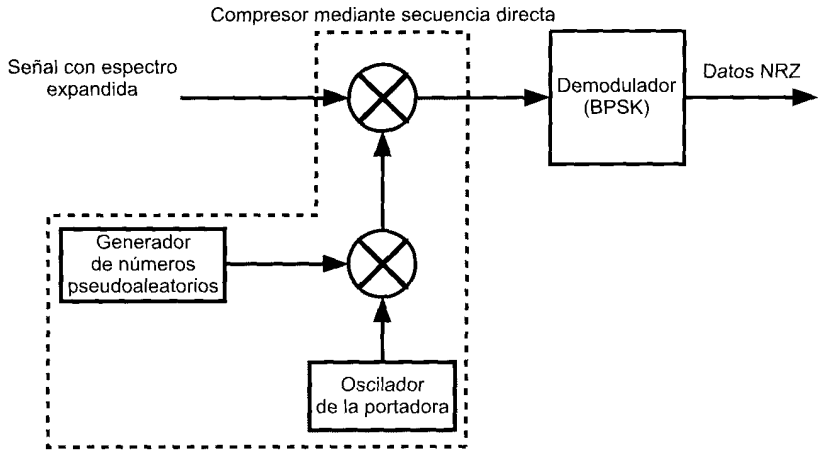
Figura 5.21. Ejemplo de un espectro expandido mediante secuencia directa.

se muestra un ejemplo. Obsérvese que un uno de información invierte los bits pseudoaleatorios, mientras que un bit de información igual a cero hace que los bits pseudoaleatorios se transmitan sin ser invertidos. La cadena resultante tendrá la misma velocidad de transmisión que la secuencia original pseudoaleatoria, por tanto tendrá un ancho de banda mayor que la secuencia de información. En el ejemplo, la cadena de bits pseudoaleatorios tiene una frecuencia de reloj igual a cuatro veces la frecuencia de los bits de información.

En la Figura 5.22 se muestra un ejemplo de la realización de un sistema típico de secuencia directa. En este caso, en lugar de realizar la función OR-exclusiva entre los bits de información y los pseudoaleatorios, para posteriormente ser modulados, dichos bits se convierten primero a señales analógicas y posteriormente se combinan.



(a) Transmisor



(b) Receptor

Figura 5.22. Sistema de espectro expandido mediante secuencia directa.

La expansión del espectro llevada a cabo mediante la técnica de secuencia directa se determina fácilmente. Por ejemplo, supóngase que los bits de la señal de información tienen una anchura t_b, lo que equivale a una velocidad de transmisión $1/t_b$. En ese caso, el ancho de banda de la señal, dependiendo de la técnica de codificación, es aproximadamente $2/t_b$. Igualmente, el ancho de banda de la señal pseudoaleatoria es $2/T_c$, donde T_c es la anchura de los bits de la entrada pseudoaleatoria. El ancho de banda de la señal combinada es aproximadamente igual a la suma de los dos anchos de banda. El grado de la expansión conseguido está directamente relacionado con la velocidad de transmisión de la cadena pseudoaleatoria: cuanto mayor sea dicha velocidad de transmisión, mayor será la expansión obtenida.

5.6. LECTURAS RECOMENDADAS

Por diversos motivos es difícil encontrar manuales que presenten un tratamiento riguroso sobre los esquemas de codificación digital a digital. [PEEB87] incluye uno de los mejores análisis. Las referencias [SKLA88] y [BERG87] son también recomendables. Por el contrario, hay un gran número de buenas referencias sobre los esquemas de modulación analógica de datos digitales. Una buena elección sería [COUC97], [HAYK94] y [PROA94]; estos tres también proporcionan un buen tratamiento de la modulación analógica y digital de datos analógicos.

[PEAR92] contiene una exposición excepcionalmente clara que cubre las técnicas de digital a analógico, de analógico a digital y de analógico a analógico.

Para las técnicas de espectro expandido se pueden usar [PETE95] y [DIXO94].

[FREE98] es un texto instructivo que abarca conceptos tales como la velocidad de transmisión, la velocidad de modulación y el ancho de banda. [SKLA93] es un «tutorial» recomendable que explica más ampliamente los conceptos abordados en los capítulos precedentes relacionados con la eficiencia del ancho de banda y los esquemas de codificación.

BERG96 Bergmans, J. *Digital Baseband Transmission and Recording*. Boston: Kluwer, 1996.

COUC97 Couch, L. *Digital and Analog Communication Systems*. Upper Saddle River, NJ: Prentice Hall, 1997.

FREE98 Freeman, R. «Bits, Symbols, Baud, and Bandwidth.» *IEEE Communications Magazine*, April 1998.

HAYK94 Haykin, S. *Communication Systems*. New York: Wiley, 1995.

PEAR92 Pearson, J. *Basic Communication Theory*. Englewood Cliffs, NJ: Prentice Hall, 1992.

PEEB87 Peebles, P. *Digital Communication Systems*. Englewood Cliffs, NJ: Prentice Hall, 1987.

PETE95 Peterson, R.; Ziemer, R.; y Borth, D. *Introduction to Spread Spectrum Communications*. Englewood Cliffs, NJ: Prentice Hall, 1995.

PROA94 Proakis, J., y Salehi, M. *Coomunication Systems Engineering*. Englewood Cliffs, NJ: Prentice Hall, 1995.

SKLA88 Sklar, B. *Digital Communications: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1988.

SKLA93 Sklar, B. «Defining, Designinf, and Evaluating Digital Communication Systems.» *IEEE Communications Magazine*, November 1993.

5.7. PROBLEMAS

5.1. ¿Cuál de las señales de la Tabla 5.2 usa codificación diferencial?

5.2. Obtener los algoritmos que implementen cada uno de los códigos de la Tabla 5.2 a partir de la señal en NRZ-L.

5.3. Una versión modificada del código NRZ denominada NRZ-mejorado (E-NRZ, enhanced NRZ) se usa a veces para las grabaciones en cintas magnéticas de alta densidad. El E-NRZ implica la separación de la cadena de datos NRZ-L en palabras de 7 bits; se invierten los bits 2, 3, 6 y 7 y se añade un bit de paridad a cada palabra. El bit de paridad se elige para que el número total de unos en la palabra de 8 bits sea impar. ¿Qué ventajas tiene E-NRZ respecto NRZ-L? ¿Tiene desventajas?

5.4. Desarrollar el diagrama de estados (máquina de estados finitos) de una codificación pseudoternaria.

5.5. Considérese el siguiente esquema de codificación. A la entrada se tienen datos binarios, a_m, con $m = 1,2,3...$ Supóngase que se realiza un procesamiento en dos niveles. En primer lugar, se genera un conjunto de números binarios de acuerdo con la siguiente expresión

$$b_0 = 0$$

$$b_m = (a_m + b_{m-1}) \bmod 2$$

que se codifican de acuerdo con

$$c_m = b_m - b_{m-1}$$

En el receptor, los datos originales se recuperan mediante

$$a_m = c_m \bmod 2$$

a) Verificar que los valores recibidos de a_m son igual a los valores transmitidos.

b) ¿Qué tipo de codificación es ésta?

5.6. Para la cadena de bits 01001110, representar las formas de onda de cada uno de los códigos mostrados en la Tabla 5.2. Supóngase que en el NRZI el nivel de la señal para codificar el bit anterior fue alto; que el bit 1 precedente en el esquema AMI correspondió a un nivel de tensión negativa; y que para el código pseudoternario el bit 0 más reciente se codificó con una tensión negativa.

5.7. La forma de onda de la Figura 5.23, corresponde a una cadena de bits codificada con código Manchester. Determinar el principio y el final de los bits (es decir, extraer la señal de reloj) y obtener la secuencia de datos.

Figura 5.23. Una cadena Manchester.

5.8. Supóngase una secuencia de datos binarios formada por una serie larga de 1 consecutivos, seguida de un cero al que le siguen otra una serie larga de 1; si se suponen las mismas condiciones que las del Problema 5.6, dibujar la forma de onda correspondiente a esta secuencia si se codifica con

a) NRZ-L.

b) Bipolar-AMI.

c) Pseudoternario.

5.9. La forma de onda de un código bipolar-AMI correspondiente a la secuencia 0100101011 se transmite por un canal ruidoso. La forma de onda recibida se muestra en la Figura 5.24, en la que se ha incluido un error en un bit. Localice dónde está el error y justifique la respuesta.

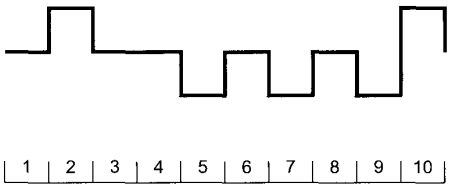


Figura 5.24. Una onda bipolar-AMI recibida.

5.10. En la Figura 5.25 se muestra el demodulador QAM correspondiente al modulador QAM de la Figura 5.18. Muestre que este sistema efectivamente recupera las dos señales $d1(t)$ y $d2(t)$, las cuales, si se combinaran darían lugar a la señal de entrada.

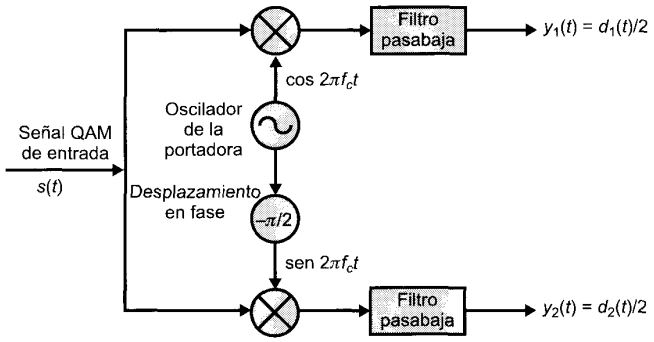


Figura 5.25. Demodulador QAM.

5.11. En los dos esquemas siguientes de señalización a) PSK y b) QPSK se utiliza una onda seno. La duración del elemento de señalización es 10^{-5} segundos. Si la señal recibida es

$$s(t) = 0{,}005 \operatorname{sen}(2\pi 10^6 t + 0) \text{ voltios}$$

y el ruido en el receptor es $2{,}5 \times 10^{-8}$ vatios, determinar E_b/N_0 (en dB) para cada caso.

5.12. Obténgase la expresión de la velocidad de modulación D (en baudios) en función de la velocidad de transmisión R para una modulación QPSK en la que se utilizan las técnicas de codificación digital mostradas en la Tabla 5.2.

5.13. ¿Qué SNR se necesita para conseguir una eficiencia del ancho de banda de 1,0 en los esquemas ASK, FSK, PSK y QPSK? Suponer que la tasa de errores por bit es 10^{-6}.

5.14. Una señal NRZ-L se pasa a través de un filtro con $r = 0{,}5$ y posteriormente se modula sobre una portadora. La velocidad de transmisión es 2.400 bps. Calcular el ancho de banda para ASK y FSK. Para FSK suponer que las frecuencias utilizadas son 50 kHz y 55 kHz.

5.15. Supóngase que el canal de una línea telefónica se ecualiza para permitir la transmisión de datos en un rango de frecuencias de 600 hasta 3.000 Hz. El ancho de banda disponible es de 2.400 Hz. Para $r = 1$, calcular el ancho de banda necesario para QPSK a 2.400 bps, y para 4.800 bps•ambas con ocho bits de señalización multinivel. ¿Es dicho ancho de banda adecuado?

5.16. ¿Por qué PCM es preferible a DM en la codificación de señales analógicas que representen datos digitales?

5.17. ¿Es el modem un dispositivo que realiza las funciones inversas de un codec? (es decir, ¿podría un modem funcionar como un codec invertido y viceversa?).

5.18. Una señal se cuantiza utilizando 10 bits PCM. Calcular la relación señal-ruido de cuantización.

5.19. Considérese una señal de audio cuyas componentes espectrales están comprendidas en el rango de 300 a 3.000 Hz. Suponer que se usa una frecuencia de muestreo de 7.000 muestras por segundo para generar la señal PCM.

a) Para una SNR = 30 dB, ¿cuántos niveles se necesitan en un cuantizador uniforme?

b) ¿Cuál es la velocidad de transmisión necesaria?

5.20. Determinar el tamaño del escalón δ que se necesita para evitar el ruido de sobrecarga en la pendiente en función de la componente máxima en frecuencias de la señal. Supóngase que todas las componentes tienen amplitud A.

5.21. Un codificador PCM acepta señales con un fondo de escala de 10 voltios de tensión, y genera códigos de 8 bits usando cuantización uniforme. La tensión máxima normalizada cuantizada es $1 - 2^{-8}$. Determinar a) el tamaño del escalón normalizado, b) el tamaño del escalón real en voltios, c) el máximo nivel cuantizado real en voltios, d) la resolución normalizada, e) la resolución real, f) el porcentaje de resolución.

5.22. La forma de onda analógica que se muestra en la Figura 5.26 se va a codificar usando modulación delta. El periodo de muestreo y el tamaño del escalón se muestran en la figura. En la misma figura se muestran la primera salida DM y la correspondiente función escalera. Obtener el resto de la función escalera y la salida DM. Indicar las regiones donde haya distorsión de sobrecarga en la pendiente.

5.23. Supóngase la señal modulada en ángulo, correspondiente a la siguiente presión

$$s(t) = 10\cos[(10^8)\pi t + 5\,\text{sen}\,2\pi(10^3)t]$$

Encontrar la máxima desviación de fase y la máxima desviación en frecuencia.

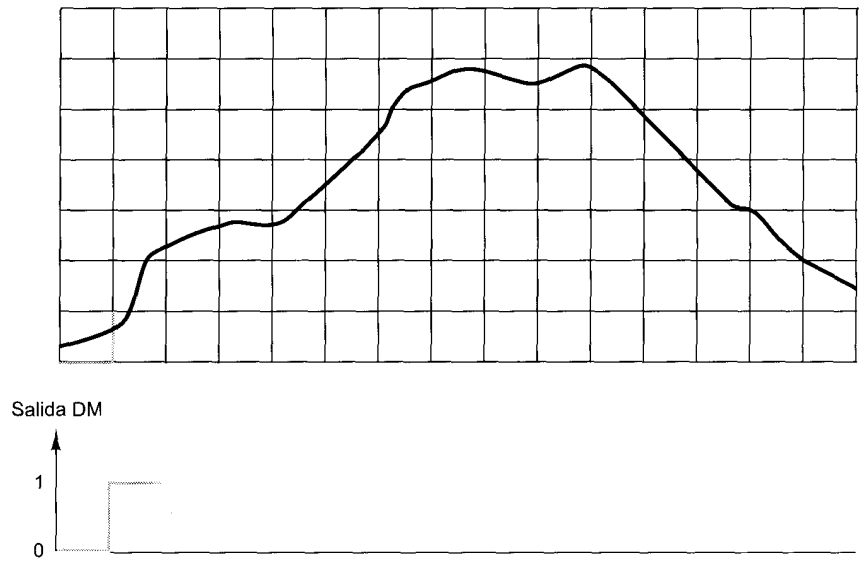


Figura 5.26. Ejemplo de modulación delta.

5.24. Supóngase la señal modulada en ángulo, correspondiente a la siguiente expresión

$$s(t) = 10\cos[2\pi(10^6)t + 0{,}1\,\text{sen}\,(10^3)\pi t]$$

a) Expresar $s(t)$ como una señal PM siendo $n_p = 10$.

b) Expresar $s(t)$ como una señal FM siendo $n_f = 10\pi$.

5.25. Sean $m_1(t)$ y $m_2(t)$ dos señales que contienen mensajes y sean $s_1(t)$ y $s_2(t)$ las correspondientes señales moduladas, en las que se ha utilizado una portadora de frecuencia f_c.

a) Demostrar que si se utiliza un simple esquema AM, $m_1(t) + m_2(t)$ genera una señal modulada igual a la combinación lineal de $s_1(t)$ y $s_2(t)$. Esto justifica el porqué a veces a AM se le denomina modulación lineal.

b) Demostrar que si se utiliza un esquema simple PM, entonces $m_1(t) + m_2(t)$ genera una señal modulada no igual a la combinación lineal de $s_1(t)$ y $s_2(t)$. Esto justifica el porqué a veces a la PM se le denomina modulación nolineal.

APÉNDICE 5A. DEMOSTRACIÓN DEL TEOREMA DE MUESTREO

El teorema de muestreo establece que dadas

- $x(t)$ una señal limitada en banda , con ancho de banda f_h.
- $p(t)$ una señal de pulsos de muestreo en instantes de tiempo $T_S = 1/f_s$, donde f_S es la frecuencia de muestreo.
- $x_S(t) = x(t)p(t)$ la señal muestreada.

$x(t)$ se puede recuperar exactamente a partir de $x_s(t)$ si y solamente si $f_S \geqslant 2f_h$.

DEMOSTRACIÓN

Si $p(t)$ es una serie de pulsos uniformes, es por tanto una señal periódica, por lo que se puede aproximar mediante su desarrollo en serie de Fourier:

$$p(t) = \sum_{n=-\infty}^{\infty} P_n e^{j2\pi n f_s t}$$

Se tiene que

$$x_S(t) = x(t)p(t) = \sum_{n=-\infty}^{\infty} P_n x(t) e^{j2\pi n f_s t}$$

Ahora, considérese la transformada de Fourier de $x_S(t)$:

$$X_S(f) = \int_{-\infty}^{\infty} x_S(t) e^{j2\pi n f t}\, dt$$

Sustituyendo $x_S(t)$,

$$X_S(f) = \int_{-\infty}^{\infty} \sum_{n=-\infty}^{\infty} P_n x(t) e^{j2\pi n f_s t} e^{-j2\pi n f t}\, dt$$

Reordenando términos

$$X_S(f) = \sum_{n=-\infty}^{\infty} P_n \int_{-\infty}^{\infty} x(t) e^{-j2\pi(f - nf_s)t}\, dt$$

De la definición de la transformada de Fourier, se puede escribir que

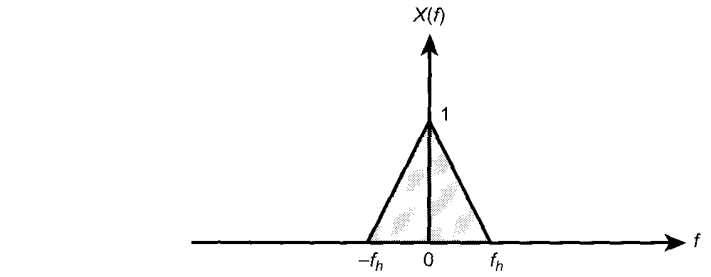
$$X(f - nf_S) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi(f - nf_S)t}\,dt$$

donde $X(f)$ es la transformada de Fourier de $x(t)$. Sustituyendo en la expresión anterior, se tiene que

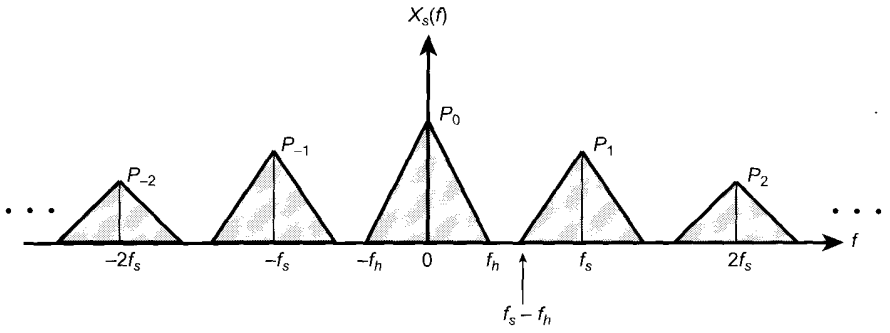
$$X_S(f) = \sum_{n=-\infty}^{\infty} P_n X(f - nf_S)$$

Esta última expresión tiene una interpretación diferente, la cual se muestra en la Figura 5.27, en la que se supone sin pérdida de generalidad que el ancho de banda de $x(t)$ está dentro del intervalo definido entre 0 y f_h. El espectro de $x_S(t)$ está formado por el espectro de $x(t)$ más el espectro de $x(t)$ trasladado sobre cada armónico de la frecuencia de muestreo. Cada uno de los espectros desplazados se multiplica por el correspondiente coeficiente de la serie de Fourier de $p(t)$. Ahora, si $f_S \geq 2f_h$, los espectros desplazados no se solaparán, y el espectro de $x(t)$ multiplicado por P_0 aparece en $X_S(f)$. El espectro de $x(t)$ se recupera filtrando $X_S(f)$ con un filtro pasabanda en el que $f \leq f_S$. Es decir,

$$X_S(f) = P_0 X(f) \qquad \frac{-f_S}{2} \leq f \leq \frac{f_S}{2}$$



(a) Espectro de $x(t)$



(b) Espectro de $x_S(t)$

Figura 5.27. Demostración del teorema de muestreo.

CAPÍTULO 6

La interfaz en las comunicaciones de datos

- La transmisión de una cadena de bits desde un dispositivo a otro a través de una línea de transmisión implica un alto grado de cooperación entre ambos extremos. Uno de los requisitos esenciales es la **sincronización.** El receptor debe saber la velocidad a la que se están recibiendo los datos de tal manera que pueda muestrear la línea a intervalos constantes de tiempo para así determinar cada uno de los bits recibidos. Para este fin, se utilizan habitualmente dos técnicas. En la **transmisión asíncrona**, cada carácter se trata independientemente. El primer bit de cada carácter es un bit de comienzo, que alerta al receptor sobre la llegada del carácter. El receptor muestrea cada bit del carácter y busca el comienzo del siguiente. Esta técnica puede no funcionar correctamente para bloques de datos excesivamente largos debido a que el reloj del receptor podría desincronizarse del reloj del emisor. No obstante, la transmisión de datos en bloques grandes es más eficaz que la transmisión carácter a carácter. Para el envío de bloques grandes se utiliza **la transmisión síncrona**. Cada bloque de datos forma una trama, que incluirá entre otros campos los delimitadores de principio y de fin. En la transmisión de la trama se empleará alguna técnica de sincronización, como, por ejemplo, la que se obtiene con el código Manchester.
- Para transmitir a través de un medio, todo dispositivo lo hará mediante alguna **interfaz**. La interfaz no sólo define las características eléctricas de la señal sino que además especifica la conexión física, así como los procedimientos para transmitir y recibir bits.

En los capítulos anteriores, se han estudiado fundamentalmente los aspectos principales de la transmisión de datos, tales como la caracterización de las señales de datos y los medios de transmisión, la codificación de señales y las medidas de las prestaciones. En este capítulo centraremos la atención en la interfaz entre los dispositivos de comunicación de datos y los sistemas de transmisión.

Para que dos dispositivos conectados por un medio de transmisión intercambien datos es necesario un alto grado de cooperación. Generalmente, los datos se transmiten bit a bit a través del medio; la temporización (es decir: la velocidad de transmisión, la duración y la separación entre bits) de estos bits debe ser común en el receptor y en el transmisor. En la Sección 6.1 se estudian dos técnicas que son habituales para el control de la temporización: la transmisión síncrona y la asíncrona. En la sección siguiente se revisan las configuraciones más habituales en las líneas de transmisión. Finalmente, se estudia la interfaz física entre los dispositivos transmisores-receptores y la línea de transmisión. Usualmente, los dispositivos de transmisión digital no se conectan directamente a través del medio. En su lugar, la conexión se realiza con una interfaz normalizada que controla la interacción de los dispositivos de recepción/emisión con la línea de transmisión.

6.1 TRANSMISIÓN ASÍNCRONA Y SÍNCRONA

Este libro estudia fundamentalmente la transmisión de datos serie; es decir, la transmisión de datos a través de un único camino, en lugar utilizar un conjunto de líneas en paralelo, como es habitual en los dispositivos de E/S y en los buses internos de los computadores. En la transmisión serie, los elementos de señalización se envían a través de la línea de transmisión de uno en uno. Cada elemento puede ser:

- **Menos de un bit:** como, por ejemplo, en la codificación Manchester.
- **Un bit:** NRZ-L y FSK son un ejemplo digital y otro analógico, respectivamente.
- **Más de un bit:** como, por ejemplo, en QPSK.

Para simplificar, en el razonamiento que sigue, mientras no se especifique lo contrario, supondremos que se usa un bit por elemento de señalización. Esta simplificación no va a influir en el tratamiento llevado a cabo.

Recuérdese que (véase Figura 3.13) para determinar el valor binario en la recepción de los datos digitales, se realiza un muestreo de la señal por cada bit recibido. En este caso, los defectos en la transmisión pueden corromper la señal de tal manera que se cometan errores ocasionales. El problema anterior se agrava por la dificultad adicional de la temporización: para que el receptor muestree los bits recibidos correctamente, debe conocer el instante de llegada así como la duración de cada bit.

Supóngase que el emisor emite una cadena de bits. Esto se hará de acuerdo con el reloj del transmisor. Por ejemplo, si los datos se transmiten a un millón de bits por segundo (1 Mbps), significará que se transmite un bit cada $1/10^6 = 0{,}1$ microsegundos (μs), medidos con el reloj del emisor. Generalmente, el receptor intentará muestrear el medio en la parte central de cada bit, obteniendo una muestra por cada intervalo de duración de un bit. En el ejemplo, el muestreo se hará cada 1 μs. Si el receptor delimita las duraciones basándose en su propio reloj, potencialmente se puede presentar un problema si los dos relojes (el del emisor y el del receptor) no están sincronizados con precisión. Si hay una desincronización del 1 por ciento (el reloj del receptor es un 1 por ciento más rápido o lento que el reloj del transmisor), entonces el primer muestreo estará desplazado 0,01 veces la duración del bit (0,01 μs) del instante central del intervalo (es decir, a 0,5 μs del principio o del final del intervalo). Tras 50 muestras o más, el receptor puede obtener un error debido a que el muestreo lo realizará en un instante incorrecto ($50 \times 0{,}01 = 0{,}5$ μs). Si la desincronización fuera menor el error ocurriría más tarde, en cualquier caso, si se emite un número suficiente de bits dicho error aparecerá irremediablemente si no se adoptan medidas para sincronizar al transmisor y al receptor.

TRANSMISIÓN ASÍNCRONA

Hay dos enfoques habituales para resolver el problema de la sincronización. El primero se denomina, de una manera no muy acertada, transmisión asíncrona. La estrategia seguida aquí consiste en evitar el problema de la temporización mediante el envío ininterrumpido de cadenas de bits que no sean muy largas. En su lugar, los datos se transmiten enviándolos carácter a carácter, normalmente cada carácter tiene una longitud de 5 a 8 bits[1]. La temporización o sincronización se debe mantener durante la duración del carácter, ya que el receptor tiene la oportunidad de resincronizarse al principio de cada carácter nuevo.

Esta técnica se va a explicar haciendo referencia a la Figura 6.1. Cuando no se transmite ningún carácter, la línea entre el emisor y el receptor estará en estado de *reposo*. La definición de *reposo* es equivalente al elemento de señalización correspondiente al 1 binario. Así, en la señalización NRZ-L (veáse Figura 5.2), que es habitual en la transmisión asíncrona, el estado de reposo correspondería con la presencia de una tensión negativa en la línea. El principio de cada carácter se indica mediante un *bit de comienzo* que corresponde al valor binario 0. A continuación se transmite el carácter, comenzando por el bit menos significativo, que tendrá entre cinco y ocho bits. En la Tabla 3.1, para los caracteres IRA el primer bit transmitido se ha etiquetado b_1. Normalmente, los bits correspondientes al carácter van seguidos de un bit de paridad, que ocupará por tanto la posición del bit más significativo. El bit de paridad se determina en el emisor de tal manera que el número de unos dentro del carácter, incluyendo el bit de paridad, sea par (paridad par) o impar (paridad impar), dependiendo del criterio que se elija. Este bit se usa en el receptor para la detección de errores, como así se explica en el Capítulo 7. Por último está el denominado *elemento de parada*, que corresponde a un 1 binario. Se debe especificar la longitud mínima del elemento de parada, y normalmente coincide con 1, 1,5 ó 2 veces la duración de un bit convencional. No se especifica un valor máximo. Debido a que el elemento de parada es igual que el estado de reposo, el transmisor transmitirá la señal de parada hasta que se vaya a transmitir el siguiente carácter.

[1] El número de bits correspondiente a cada carácter depende del código que se utilice. Ya se ha mencionado un ejemplo, el código IRA, en el que se usan siete bits por carácter (Tabla 3.1). Otro ejemplo es el EBCDIC («Extended Binary Coded Decimal Interchange Code»), que es el código de 8 bits que se utiliza en todas las máquinas de IBM, excepto en los computadores personales y estaciones de trabajo.

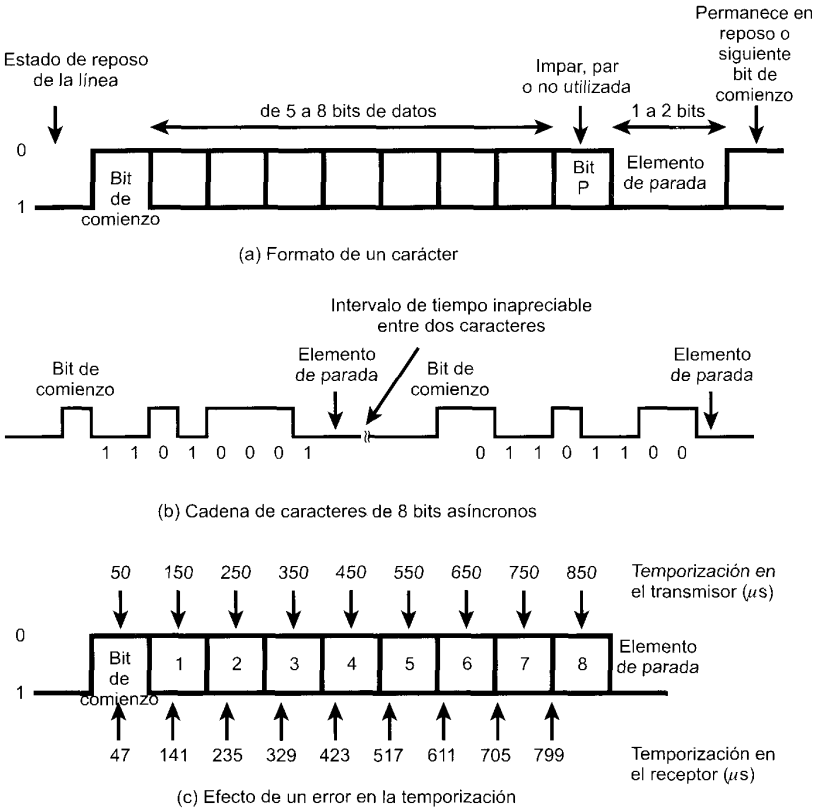


Figura 6.1. Transmisión asíncrona.

Si se envía una cadena estacionaria de caracteres, la separación entre cada dos caracteres será uniforme e igual a la duración del elemento de parada. Por ejemplo, si el elemento de parada corresponde a 1 bit y se envía los caracteres ABC en IRA (con paridad par) el patrón de bits será[2] 0100000101001000010101100001111 1...111. El bit de comienzo (0) determinará la secuencia de temporización para los siguientes 9 elementos, que corresponden con un código IRA de 7 bits, el bit de paridad y el bit de parada. En el estado de reposo, el receptor buscará una transición de 1 a 0 que indicará el comienzo del siguiente carácter y entonces muestreará, siete veces la señal de entrada, una vez por cada intervalo. A continuación buscará la siguiente transición de 1 a 0, lo que no ocurrirá antes del intervalo correspondiente a la duración de un bit.

Este esquema no es muy exigente en cuanto a los requisitos de temporización. Por ejemplo, generalmente los caracteres IRA se envían como unidades de 8 bits, incluyendo el bit de paridad. Si el receptor es un 5 por ciento más rápido o más lento que el emisor, el octavo muestreo estará desplazado un 45 por ciento, lo que significa que todavía es aceptable. En la Figura 6.1c se muestra el efecto de un error de temporización lo suficientemente grande como para provocar un error en la recepción. En este ejemplo supondremos una velocidad de transmisión de 10.000 bits por segundo (10 kbps); por tanto, se transmite un bit cada 0,1 milisegundos (ms), es decir tiene una duración de 100 μs. Supongamos que el receptor está desincronizado al 6 por ciento, es decir en 6 μs cada intervalo de duración de un bit. Por tanto, el

[2] En el texto, la transmisión se muestra de izquierda (el primer bit transmitido) a derecha (último bit transmitido).

receptor muestrea el carácter de entrada cada 94 μs (medidos con el reloj del transmisor). Como se puede observar, la *última muestra será errónea.*

Un error como el anterior en realidad dará lugar a dos errores. Primero, el último bit muestreado será incorrecto, y segundo, la cuenta de bits puede estar desalineada. Si el bit 7 es un 1 y el bit 8 es un 0, el bit 8 se puede interpretar erróneamente como un bit de comienzo. Este tipo de error se denomina *error de delimitación de trama*, ya que a la unidad constituida por el carácter más el bit de comienzo y el elemento de parada se le denomina trama. Se puede dar igualmente un error de delimitación de trama si el ruido hace que se detecte un bit de comienzo erróneamente durante el estado de reposo.

La transmisión asíncrona es sencilla y barata, si bien requiere 2 o 3 bits suplementarios por cada carácter. Por ejemplo, en un código de 8 bits sin bit de paridad y con un elemento de parada de duración 1 bit, de cada 10 bits, 2 no contendrán información ya que se dedicarán a la sincronización; por tanto, los bits suplementarios llegan a un 20 por ciento. Por descontado que el porcentaje de bits suplementarios se podría reducir mediante la transmisión de bloques con más bits entre el bit de comienzo y el de parada. No obstante, como se muestra en la Figura 6.1c, cuanto mayor sea el bloque de bits, mayor será el error de temporización acumulativo. Para conseguir un mejor rendimiento se puede usar una estrategia diferente para la sincronización denominada transmisión síncrona.

TRANSMISIÓN SÍNCRONA

En la transmisión síncrona, se transmite un bloque de bits como una cadena estacionaria sin utilizar códigos de comienzo o parada. El bloque puede tener una longitud de muchos bits. Para prevenir la desincronización entre el emisor y el receptor, sus relojes se deberán sincronizar de alguna manera. Una posibilidad puede ser proporcionar la señal de reloj a través de una línea independiente. Uno de los extremos (el receptor o el transmisor) enviará regularmente un pulso de corta duración. El otro extremo utilizará esta señal a modo de reloj. Esta técnica funciona bien a distancias cortas, sin embargo a distancias superiores, los pulsos de reloj son susceptibles de las mismas dificultades y defectos que las propias señales de datos, por lo que pueden aparecer errores de sincronización. La otra alternativa consiste en incluir la información relativa a la sincronización en la propia señal de datos. Para la señalización digital, esto se puede llevar a cabo mediante la codificación Manchester o Manchester Diferencial. Para señales analógicas se han desarrollado a su vez diversas técnicas; por ejemplo, se puede utilizar la propia portadora para sincronizar al receptor usando la fase.

En la transmisión síncrona se requiere además un nivel de sincronización adicional para que el receptor pueda determinar dónde está el comienzo y el final de cada bloque de datos. Para llevar a cabo esto, cada bloque comienza con un patrón de bits denominado *preámbulo* y generalmente termina con un patrón de bits de *final*. Además de los anteriores, se añaden otros bits que se utilizan en los procedimientos de control del enlace estudiados en el Capítulo 7. Los datos, más el preámbulo, más los bits de final junto con la información de control se denomina **trama**. El formato en particular de la trama dependerá del procedimiento de control del enlace que se utilice.

En la Figura 6.2 se muestra, en términos generales, un formato típico para una trama de una transmisión síncrona. Normalmente, la trama comienza con un preámbulo denominado delimitador de 8 bits. El mismo delimitador se utiliza igualmente como indicador del final de la trama. El receptor buscará la aparición del delimitador que determina el comienzo de la trama. Este delimitador estará seguido por algunos campos de control, el campo de datos (de longitud variable para la mayoría de los protocolos), más campos de control y por último, se repetirá el delimitador indicando el final de la trama.

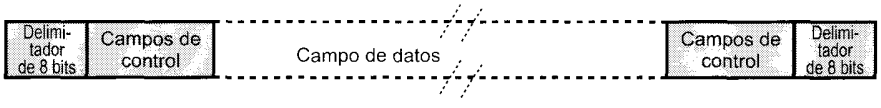


Figura 6.2. Formato de una trama síncrona.

Para los bloques de datos que sean de suficiente tamaño, la transmisión síncrona es mucho más eficiente que la asíncrona. La transmisión asíncrona requiere un 20 por ciento o más de bits suplementarios. La información de control, el preámbulo y el final son normalmente menos de 100 bits. Por ejemplo, el HDLC, uno de los esquemas más utilizados (estudiado en el Capítulo 7), contiene 48 bits de control, preámbulo y final. Por tanto, para bloques de datos de 1.000 caracteres, cada trama contiene 48 bits de bits suplementarios y $1.000 \times 8 = 8.000$ bits de datos, lo que corresponde a un porcentaje de bits suplementarios igual a $48/8048 \times 100\% = 0{,}6\%$ solamente.

6.2. CONFIGURACIONES DE LA LÍNEA

Las dos características que distinguen a las posibles configuraciones del enlace de datos son la topología y su funcionamiento en «semi-duplex» o «full-duplex».

TOPOLOGÍA

Con el término topología se hace referencia a la disposición física de las estaciones en el medio de transmisión. Si hay sólo dos estaciones (es decir, un terminal y un computador, o dos computadores), el enlace es punto a punto. Si hay más de dos estaciones, entonces se trata de una topología multipunto. Históricamente, los enlaces multipunto se han utilizado cuando se disponía de un computador (estación principal) y un conjunto de terminales (estaciones secundarias). Actualmente, las topologías multipunto son típicas de las redes de área local.

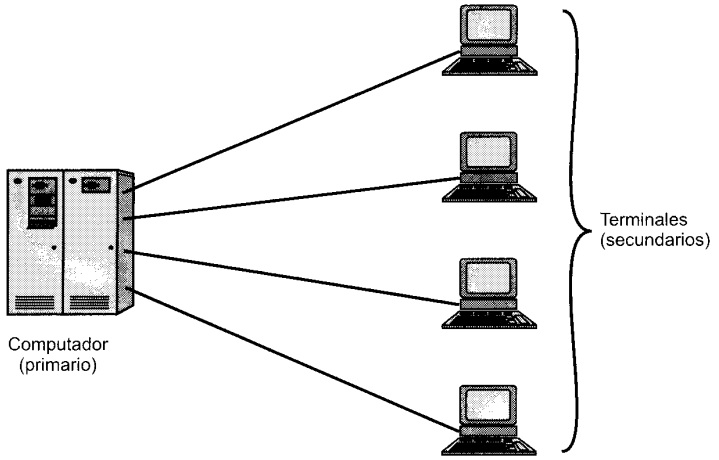
Las topologías tradicionales multipunto son sólo útiles cuando los terminales transmiten durante una fracción del tiempo. En la Figura 6.3 se muestran las ventajas de la configuración multipunto. Si cada terminal tuviera un enlace punto a punto hasta su computador central, éste debería tener un puerto de E/S para cada terminal conectado. También se necesitaría una línea desde cada uno de los terminales al computador central. En una configuración multipunto, el computador central sólo necesita un puerto de E/S y una única línea de transmisión, ahorrando así los correspondientes costes.

FULL-DUPLEX Y SEMI-DUPLEX

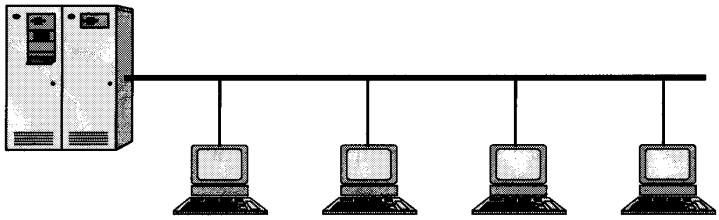
El intercambio de datos a través de una línea de transmisión se puede clasificar como full-duplex o semi-duplex. En la *transmisión semi-duplex* cada vez sólo una de las dos estaciones del enlace punto a punto puede transmitir. Este modo también se denomina *en dos sentidos alternos*, aludiendo al hecho de que las dos estaciones pueden transmitir alternativamente. Esto es comparable a un puente que tuviera un solo carril y con circulación en los dos sentidos. Este tipo de transmisión se usa a menudo en la interacción entre los terminales y el computador central. Mientras que el usuario introduce y transmite datos, el computador central no podrá enviar datos al terminal, ya que si no, éstos aparecerían en la pantalla del terminal provocando confusión.

En la *transmisión full-duplex* las dos estaciones pueden simultáneamente enviar y recibir datos. Este modo se denomina *dos sentidos simultáneos* y es comparable a un puente que tuviera dos carriles con tráfico en ambos sentidos. Para el intercambio de datos entre computadores, este tipo de transmisión es más eficiente que la transmisión semi-duplex.

Para la señalización digital, en la que se requiere un medio guiado, la transmisión full-duplex normalmente exige dos caminos separados (por ejemplo, dos pares trenzados), mientras que la transmisión semi-duplex necesita solamente uno. Para la señalización analógica, dependerá de la frecuencia: si una estación transmite y recibe a la misma frecuencia, utilizando transmisión inalámbrica se deberá operar en modo semi-duplex, aunque para medios guiados se puede operar en full-duplex utilizando dos líneas de transmisión distintas. Si una estación emite en una frecuencia y recibe a otra, para la transmisión inalámbrica se deberá operar en full-duplex. Para medios guiados se deberá optar por full-duplex usando una sola línea.



(a) Punto a punto



(b) Multipunto

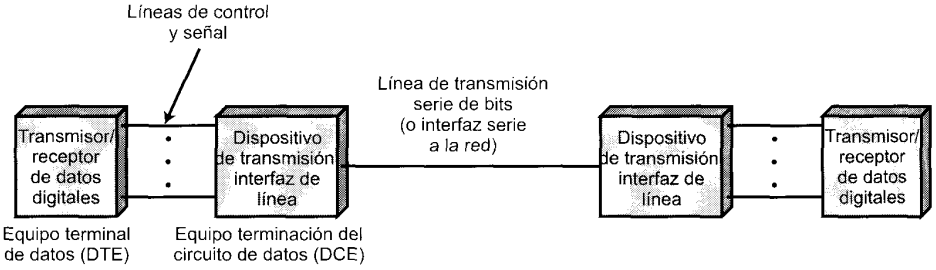
Figura 6.3. Configuraciones tradicionales computador/terminal.

En realidad es factible transmitir simultáneamente en ambas direcciones sobre una única línea de transmisión utilizando la técnica denominada cancelación de eco. Es ésta una técnica de procesamiento de señales cuya explicación está fuera del alcance de este texto.

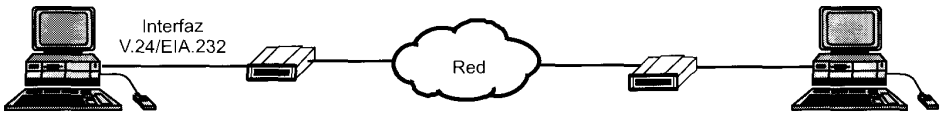
6.3. INTERFACES

La mayoría de los dispositivos utilizados para el procesamiento de datos tienen una capacidad limitada de transmisión. Generalmente, generan una señal digital, como, por ejemplo, NRZ-L, pudiendo transmitir a una distancia limitada. Consecuentemente, es extraño que dichos dispositivos (terminales y computadores) se conecten directamente a la red de transmisión. En la Figura 6.4 se muestra la configuración más habitual. Los dispositivos finales, normalmente terminales y computadores, se denominan generalmente *equipo terminal de datos (DTE, Data Terminal Equipmen).* Un DTE hace uso del medio de transmisión mediante la utilización de un *equipo terminación del circuito de datos (DCE, Data Circuit-Terminating Equipment),* como, por ejemplo, un modem.

Por un lado el DCE es responsable de transmitir y recibir bits, de uno en uno, a través del medio de transmisión o red. Por el otro, el DCE debe interaccionar con el DTE. En general, esto exige que se intercambien tanto datos como información de control. Esto se lleva a cabo a través de un conjunto



(a) Interfaz genérica al medio de transmisión



(b) Configuración típica

Figura 6.4. Interfaces para las comunicaciones de datos.

de cables que se denominan *circuitos de intercambio*. Para que este esquema funcione, se necesita un alto grado de cooperación. Los dos DCEs que se intercambian señales a través de la línea de transmisión o red, deben entenderse el uno al otro. Es decir, el receptor de cada DCE debe usar el mismo esquema de codificación (por ejemplo Manchester o PSK) y la misma velocidad de transmisión que el transmisor del otro extremo. Además, cada pareja DTE-DCE se debe diseñar para que funcionen cooperativamente. Para facilitar las cosas tanto a los usuarios como a los fabricantes de los equipos para el procesamiento de datos, se han desarrollado normalizaciones que especifican exactamente la naturaleza de la interfaz entre el DTE y el DCE. La interfaz tiene cuatro características importantes o especificaciones:

- Mecánicas.
- Eléctricas.
- Funcionales.
- De procedimiento.

Las *características mecánicas* tratan de la conexión física entre el DTE y el DCE. Generalmente, los circuitos de intercambio de control y de datos se embuten en un cable con un conector, macho o hembra, a cada extremo. El DTE y el DCE deben tener conectores de distinto género a cada extremo del cable. Esta configuración es análoga a los cables de suministro de energía eléctrica. La energía se facilita a través de una toma de corriente o enchufe, y el dispositivo que se conecte debe tener el conector macho (con dos polos, dos polos con polaridad o tres polos) que corresponda a la toma.

Las *características eléctricas* están relacionadas con los niveles de tensión y su temporización. Tanto el DTE como el DCE deben usar el mismo código (por ejemplo NRZ-L), deben usar los mismos niveles de tensión y deben utilizar la misma duración para los elementos de señal. Estas características determinan la velocidad de transmisión así como las máximas distancias que se puedan conseguir.

Las *características funcionales* especifican las funciones que se realizan a través de cada uno de los circuitos de intercambio. Las funciones a realizar se pueden clasificar en cuatro grandes categorías: datos, control, temporización y masa o tierra.

Las *características de procedimiento* especifican la secuencia de eventos que se deben dar en la transmisión de los datos, basándose en las características funcionales de la interfaz. Los ejemplos que se dan a continuación pueden clarificar este concepto.

Existen varias normalizaciones para la interfaz. En esta sección se presentan dos de las más significativas: V.24/EIA-232-F y la interfaz física de RDSI.

V.24/EIA-232-F

La interfaz que más se utiliza es la especificada en el estándar V.24 de la UIT-T. De hecho, este estándar especifica sólo los aspectos funcionales y de procedimiento de la interfaz; V.24 hace referencia a otros estándares para los aspectos eléctricos y mecánicos. En los Estados Unidos está publicada la EIA-232-F: una especificación prácticamente idéntica a V.24 que cubre las cuatro características mencionadas:

- Mecánicas: ISO 2110
- Eléctricas: V.28
- Funcionales: V.24
- De procedimiento: V.24

EIA-232 fue establecida inicialmente como RS-232 por la EIA (Electronic Industries Association) en 1962. Actualmente está en su sexta versión EIA-232-F de 1997. Las versiones actuales de V.24 y V.28 se establecieron en 1996 y 1993 respectivamente. Esta interfaz se utiliza para la conexión de dispositivos DTE a modems, que a su vez están conectados a líneas de calidad telefónica en sistemas analógicos y públicos de telecomunicación. También se utiliza en otras muchas aplicaciones de interconexión.

Especificaciones mecánicas

En la Figura 6.5 se muestran las especificaciones mecánicas del EIA-232-F, en la que se usa un conector de 25 contactos metálicos distribuidos de una manera específica según se define en el ISO 2110. Este conector es el terminador del cable que va desde el DTE (el terminal) al DCE (por ejemplo, el modem). Por tanto, en teoría habría que utilizar un cable que tuviera 25 conductores, aunque en la mayoría de las aplicaciones prácticas se usa un número menor de circuitos y, por tanto, de conductores.

Especificaciones eléctricas

Aquí se definen la señalización entre el DTE y el DCE. Se utiliza señalización digital en todos los circuitos de intercambio. Los valores eléctricos se interpretarán como binarios o como señales de control, dependiendo de la función del circuito de intercambio. Esta normalización especifica que, respecto a una referencia de tierra común, una tensión más negativa que 3 voltios se interprete como un binario, mientras que una tensión mayor de 3 voltios se interprete como un 0 binario. Esto corresponde al código NRZ-L mostrado en la Figura 5.2. La interfaz se utiliza a una velocidad de transmisión <20 kbps para cubrir distancias menores que 15 metros. Con un diseño adecuado se pueden conseguir distancias y velocidades mayores, pero es prudente suponer que estos límites deben respetarse tanto en teoría como en la práctica.

Para las señales de control se aplican los mismos niveles de tensión: una tensión menor de -3 voltios se interpreta como OFF y una tensión mayor de $+3$ voltios se interpreta como ON.

Especificaciones funcionales

En la Tabla 6.1 se resumen las especificaciones funcionales de los circuitos de intercambio, y en la Figura 6.5 se muestran la localización de estos circuitos en el conector. Los circuitos se pueden clasifi-

Tabla 6.1. Circuitos de intercambio en V.24/EIA-232-F.

V.24	EIA-232	Nombre	Dirección hacia:	Función
		SEÑALES DE DATOS		
103	BA	Transmisión de datos	DCE	Transmitidos por DTE
104	BB	Recepción de datos	DTE	Recibidos por el DTE
118	SBA	Transmisión de datos secundario	DCE	Transmitidos por DTE
119	SBB	Recepción de datos secundario	DTE	Recibidos por el DTE
		SEÑALES DE CONTROL		
105	CA	Petición de envío	DCE	El DTE desea transmitir
106	CB	Preparado para enviar	DTE	El DCE está preparado para recibir; respuesta a la petición de envío
107	CC	DCE preparado	DTE	El DCE está preparado para funcionar
108.2	CD	DTE preparado	DCE	El DTE está preparado para funcionar
125	CE	Indicador de llamada	DTE	El DCE está recibiendo la señal de llamada
109	CF	Detector de señal recibida	DTE	El DCE está recibiendo una señal dentro de los límites apropiados por la línea
110	CG	Detector de señal de calidad	DTE	Indica si la probabilidad de error es alta en los datos recibidos
111	CH	Selector de la velocidad de transmisión de la señal	DCE	Selecciona una de entre dos velocidades de transmisión
112	CI	Selector de la velocidad de transmisión de la señal	DTE	Selecciona una de entre dos velocidades de transmisión
133	CJ	Preparado para recibir	DCE	Control de flujo ON/OFF
120	SCA	Petición de envío secundaria	DCE	El DTE desea transmitir en el canal reverso
121	SCB	Preparado para enviar secundario	DTE	El DCE está preparado para recibir por el canal reverso
122	SCF	Detector de señal recibida secundario	DTE	Igual que el 109, pero por el canal reverso
140	RL	Bucle remoto	DCE	Solicita al DCE remoto que devuelva las señales recibidas
141	LL	Bucle local	DCE	Solicita al DCE que devuelva las señales recibidas
142	TM	Modo de test	DTE	El DCE se pone en modo de test
		SEÑALES DE TEMPORIZACIÓN		
113	DA	Temporización del elemento de señal transmitido	DCE	Señal de reloj: aparecen transicciones a ON y OFF en el centro de cada elemento de señal
114	DB	Temporización del elemento de señal transmitido	DTE	Señal de reloj: tanto el 113 como el 114 están relacionados con la señal del circuito 103
115	DD	Temporización del elemento de señal recibido	DTE	Señal de reloj para el circuito 104
		TIERRA		
102	AB	Señal de tierra/retorno		Referencia de tierra común para todos los circuitos

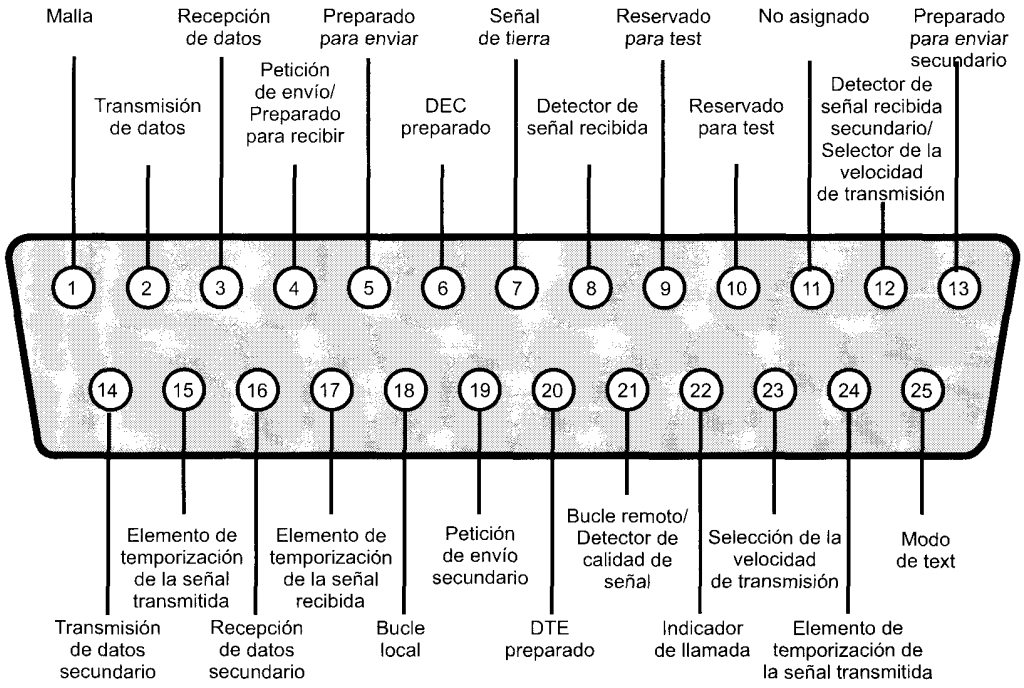


Figura 6.5. Asignación de los terminales de contacto para V.24/EIA-232 (conector en el DTE).

car en datos, control, temporización y los de tierra. Hay un circuito en cada dirección, por lo que es posible el funcionamiento full-duplex. Es más, hay dos circuitos de datos secundarios que son útiles cuando el dispositivo funciona en semi-duplex. En el caso de funcionamiento semi-duplex, el intercambio de datos entre dos DTE (a través de sus DCE y el enlace de comunicaciones correspondiente) se realiza en un instante dado en una única dirección. No obstante, puede que en un momento dado se necesite enviar una petición de parada o un mensaje de control de flujo al dispositivo transmisor. Para llevar a cabo esta funcionalidad, el enlace de comunicaciones se dota de un canal en sentido inverso, normalmente a una velocidad de transmisión muy inferior que el canal primario. En la interfaz DTE-DCE el canal en sentido inverso se establece en una pareja de circuitos de datos independientes.

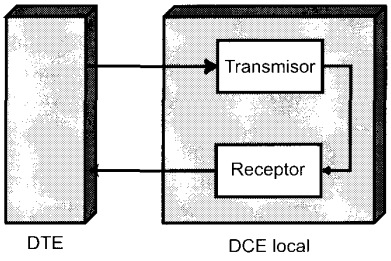
Hay 16 circuitos de control. Los 10 primeros, relacionados con la transmisión de datos sobre el canal primario, se listan en la Tabla 6.1. En el caso de transmisión asíncrona, se utilizan seis de estos circuitos (105, 106, 107 108.2, 125, 109). La utilización de estos circuitos se explica en la subsección relativa a las especificaciones de procedimiento. Además de estos seis circuitos, en la transmisión síncrona se utilizan otros tres circuitos de control. El circuito detector de la calidad de la señal (Signal Quality Detector) se pone a ON por el DCE para indicar que la calidad de la señal de entrada a través de la línea telefónica se ha deteriorado por encima de un umbral predefinido. La mayoría de los modems de alta velocidad admiten más de una velocidad de transmisión por lo que si la línea se vuelve ruidosa, pueden solicitar una reducción de la velocidad de transmisión. Los circuitos de selección para la velocidad de la señal de datos (data signal rate detector) se utilizan para cambiar de velocidad; tanto el DTE como el DCE pueden iniciar la modificación. El circuito 133 habilita al receptor para que aumente o reduzca el flujo de datos del circuito 104. Los tres siguientes circuitos de control (120, 121, 122) se utilizan para controlar el uso del canal secundario, el cual puede ser utilizado como canal de sentido inverso o para algún otro propósito auxiliar.

Tabla 6.2. Valores de los circuitos para los bucles en V.24/EIA-232.

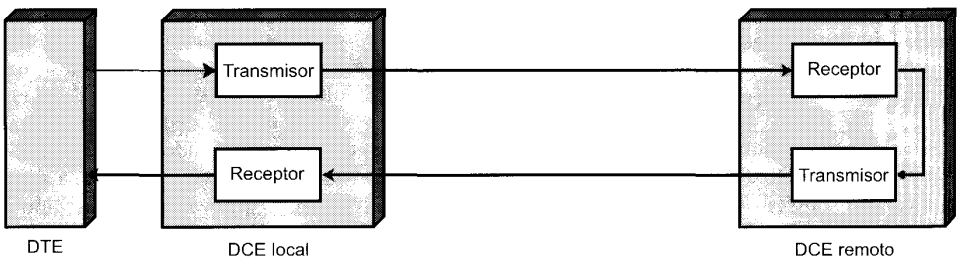
Bucle local		Bucle remoto		
Circuito	**Valor**	**Cicuito**	**Interfaz local**	**Interfaz remota**
DCE preparado	ON	DCE preparado	ON	OFF
Bucle local	ON	Bucle local	OFF	OFF
Bucle remoto	OFF	Bucle remoto	ON	OFF
Modo de test	ON	Modo de test	ON	ON

El último grupo de señales de control está relacionado con la verificación o test de la conexión entre el DTE y el DCE. Estos circuitos permiten que el DTE haga que el DCE realice un test de la conexión. Estos circuitos son útiles sólo si el modem, o el DTE de que se trate, admite un bucle de control; si bien esto es una característica habitual en la mayoría de los modems actuales. Funcionando en bucle local, la salida del transmisor del modem se conecta con la entrada del receptor, desconectando el modem de la línea de transmisión. Al modem se le envía una cadena de datos generada por el dispositivo del usuario, la cual es devuelta posteriormente al usuario formando un bucle. En el bucle remoto, el modem local se conecta a la línea de transmisión en la forma habitual, y la salida del receptor del modem remoto se conecta a la entrada del transmisor del modem. En cualesquiera de los posibles modos de test, el DCE pone a ON el circuito de Modo de Test. En la Tabla 6.2 se muestran los valores de todos los circuitos que están relacionados con el bucle de test y en la Figura 6.6 se explica su utilización.

El control del bucle es una herramienta útil para el diagnóstico de fallos. Por ejemplo, supóngase que un usuario en un computador personal se comunica con un servidor mediante una conexión a través



(a) Test del bucle local



(b) Test del bucle remoto

Figura 6.6. Bucles local y remoto.

de un modem y de pronto la transmisión se interrumpe. El problema podría estar en el bucle local, en los servicios de transmisión, en el modem remoto o en el servidor remoto. El administrador de la red podrá usar los tests para identificar el fallo. Con el test del bucle local se comprueba el funcionamiento de la interfaz local así como del DCE local. Con los tests remotos se puede comprobar el funcionamiento del canal de transmisión y del DCE remoto.

Las señales de temporización proporcionan los pulsos de reloj en la transmisión síncrona. Cuando el DCE envía datos síncronos a través del circuito de Recepción de Datos (104), a la vez envía transiciones de 0 a 1 o de 1 a 0 por el circuito de Temporización del Receptor (115), estando localizadas las transiciones en la mitad de cada elemento de señalización del circuito de Recepción de Datos. Cuando el DTE transmita datos síncronos, tanto el DTE como el DCE pueden proporcionar los pulsos de temporización, dependiendo de las circunstancias.

Finalmente, la señal de retorno de tierra común (102) sirve como un circuito de retorno para todos los circuitos de datos. Por tanto, la transmisión no es equilibrada, teniendo sólo un conductor activo. La transmisión equilibrada y no equilibrada se estudia en la sección dedicada a la interfaz en RDSI.

Especificaciones de procedimiento

Las características de procedimiento definen la secuenciación de los diferentes circuitos en una aplicación determinada. Para tal fin, se pondrán algunos ejemplos.

El primer ejemplo es muy habitual y se trata de la conexión de dos dispositivos separados una distancia corta dentro de un edificio. A los dispositivos en esta configuración se les denomina modem de línea privada o modems de distancia limitada. Como su propio nombre indica, los modems de distancia limitada admiten señales del DTE, como, por ejemplo, un terminal o un computador, las convierten a señales analógicas y las transmiten a una distancia corta a través de un medio, como, por ejemplo, un par trenzado. En el otro extremo de la línea hay otro modem de distancia limitada que acepta las señales digitales de entrada, las convierte a digital y las transfiere al terminal o computador remoto. Evidentemente, se da por su puesto que el intercambio de información es en los dos sentidos. En esta aplicación se necesitan solamente los siguientes circuitos de intercambio:

- Señal de Tierra (102)
- Transmisión de Datos (103)
- Recepción de Datos (104)
- Petición de Envío (105)
- Preparado para Enviar (106)
- DCE Preparado (107)
- Detector de Señal Recibida (109)

Cuando el modem (DCE) se enciende y está preparado para funcionar, activa la línea DCE Preparado (aplicando una tensión negativa y constante). Cuando el DTE está preparado para enviar datos (por ejemplo, cuando el usuario de un terminal ha introducido un carácter), activará la línea Preparado para Enviar. El modem responde, cuando esté preparado, activando el circuito Preparado para Enviar, indicando que se pueden transmitir datos por la línea de Transmisión de Datos. Si la transmisión es semiduplex, el circuito de Petición para Enviar, a su vez, inhibe el modo de recepción. El DTE puede ahora transmitir datos a través de la línea de Transmisión de Datos. Cuando se reciben datos del modem remoto, el modem local activa la línea Detector de Señal Recibida para indicar que el modem remoto está transmitiendo, y además transfiere los datos a través de la línea Recepción de Datos. Obsérvese que no es necesario la utilización de circuitos de temporización, ya que se trata de transmisión asíncrona.

Los circuitos mencionados anteriormente son suficientes para los modems punto a punto sobre líneas privadas, no obstante para transmitir datos a través de una línea de teléfono convencional se nece-

sitan otros circuitos adicionales. En este caso, el que inicie la conexión debe llamar al destino a través de la red. Se necesitan dos circuitos adicionales:

- DTE Preparado (108.2)
- Indicador de Llamada (125)

Con estas dos líneas adicionales, el sistema formado por el modem y el DTE podrá usar la red telefónica de una forma análoga a como se hace en una conversación convencional. En la Figura 6.7 se

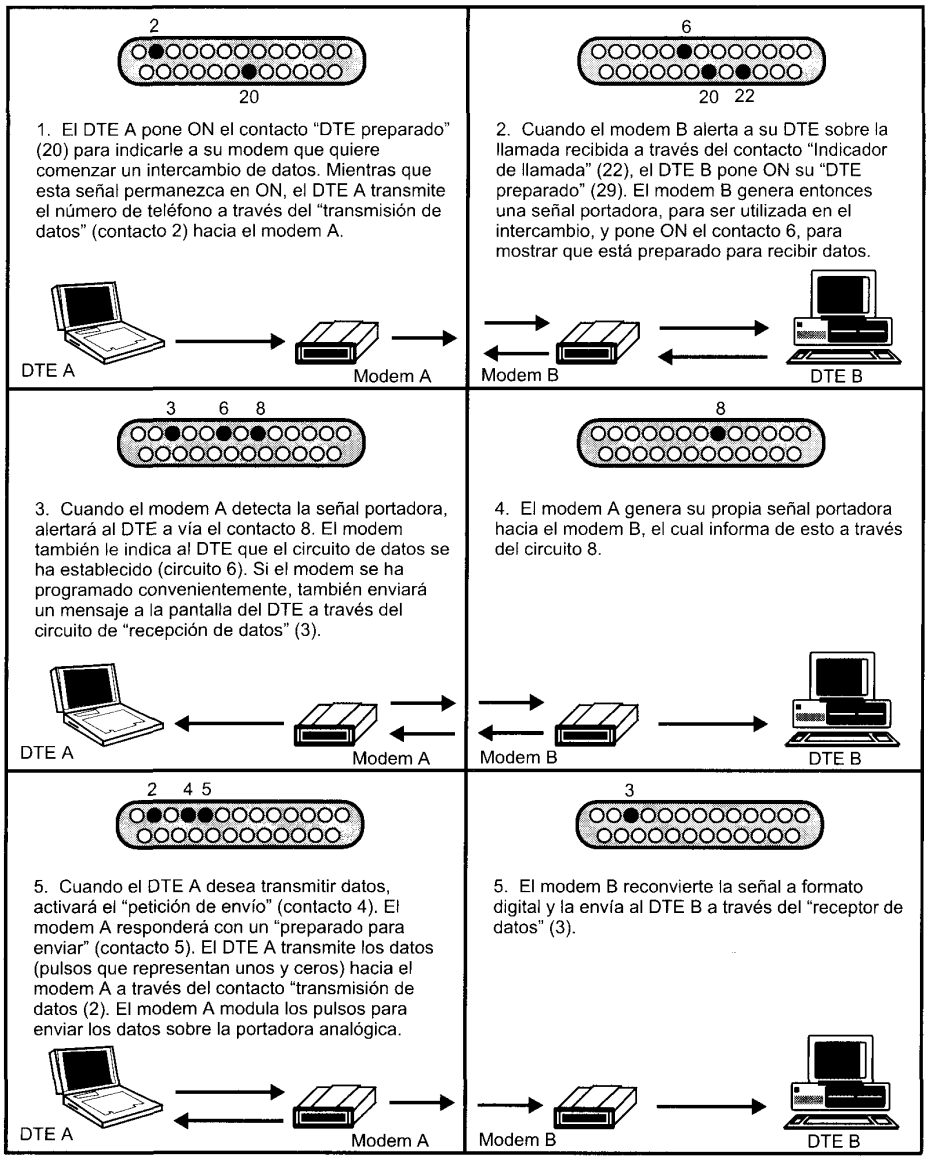


Figura 6.7. Realización de una llamada en V.24/EIA-232.

muestran los pasos necesarios en una llamada semi-duplex. Cuando se realiza la llamada, tanto manualmente como automáticamente, el sistema telefónico envía la señal de llamada. Un teléfono respondería a esta llamada haciendo sonar su timbre; un modem responde activando el circuito Indicación de Llamada. Una persona responde a la llamada descolgando el auricular; el DTE responde activando el circuito Terminal de Datos Preparado. Una persona que contestara una llamada escucharía la otra voz, y si no escuchara nada, colgaría. Un DTE intentará escuchar el Detector de Señal Recibida, que será activado por el modem cuando una señal esté presente; si este circuito no se activa, el DTE desactivará el DTE Preparado. Nos podemos preguntar, ¿bajo qué circunstancias puede darse este último caso? Una situación habitual es, por ejemplo, si una persona accidentalmente marca el número de un modem. Esto activaría el DTE del modem, pero al no recibir portadora, el problema se resuelve como ya se ha indicado.

Es ilustrativo considerar la situación en que la distancia entre los dispositivos sea tan pequeña que permita a los DTE conectarse directamente. En este caso, los circuitos de intercambio del V.24/EIA-232 se pueden usar, pero sin necesidad de usar DCE. Para que este esquema funcione, se necesita una configuración de modem nulo, consistente en conectar los circuitos de tal manera que se engañe a ambos DTE haciéndolos creer que están respectivamente conectados a un modem. En la Figura 6.8 se muestra un ejemplo de configuración de modem nulo; el porqué de las conexiones particulares indicadas en la figura debe ser evidente para el lector que haya seguido perfectamente los razonamientos anteriores.

LA INTERFAZ FÍSICA DE LA RDSI

La gran variedad de funciones que proporciona el V.24/EIA-232 se llevan a cabo mediante el uso de un gran número de circuitos de intercambio. Ésta es una solución costosa. Una alternativa sería utilizar menos circuitos incorporando más lógica de control entre las interfaces del DTE y el DCE. De esta forma se reducen los costos de circuitería, haciendo que esta aproximación sea una alternativa atractiva. Esta filosofía se adoptó en la especificación estándar X.21 (conector de 15 contactos) para la interfaz a redes públicas de conmutación de circuitos. Más recientemente, esta tendencia se ha adoptado de forma

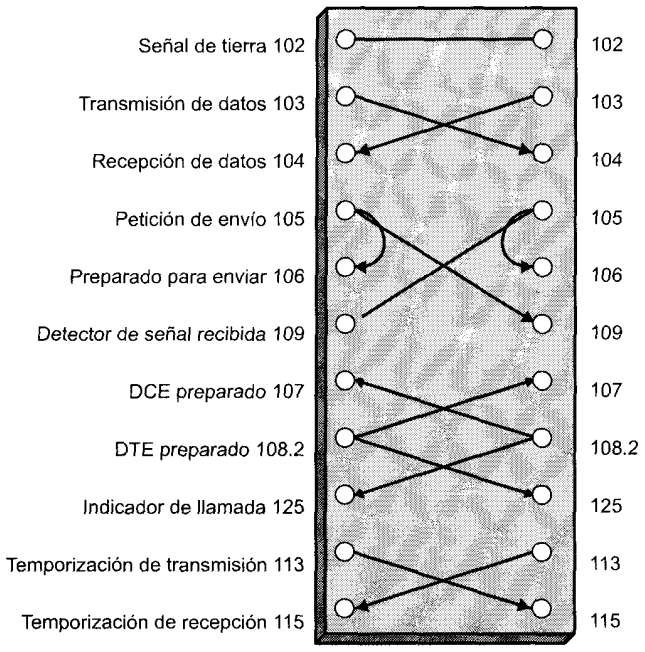


Figura 6.8. Ejemplo de un modem nulo.

más radical en la especificación de un conector de 8 contactos para la Red Digital de Servicios Integrados (RDSI). La RDSI, que se estudiará con más detalle en el Apéndice A, es una red completamente digital alternativa a las redes de telecomunicaciones analógicas y de telefonía pública existentes en la actualidad. Aquí, se considera la interfaz física definida en RDSI.

Conexión física

En la terminología RDSI, se establece una conexión física entre el equipo terminal (TE, Terminal Equipment) y el equipo terminador de línea (NT, Network-Terminating Equipment). Para el estudio que aquí se va a realizar, estos términos corresponden bastante aproximadamente a DTE y DCE respectivamente. La conexión física, definida en ISO 8877, especifica que los cables del NT y del TE tengan los conectores correspondientes, cada uno de ellos con 8 contactos.

En la Figura 6.9 se ilustra la asignación de estos contactos para cada una de las 8 líneas, tanto en el NT como en el TE. Para transmitir datos en cada una de las dos direcciones se usan dos contactos. Los contactos se utilizan para conectar mediante pares trenzados los circuitos entre el NT y el TE. Debido a que los circuitos no tienen especificaciones funcionales específicas, los circuitos de recepción y transmisión se utilizan para transmitir señales de datos y de control. La información de control se transmite usando mensajes.

La especificación prevé la posibilidad de transmitir energía a través de la interfaz, en cualquiera de los dos sentidos, dependiendo de la aplicación en particular de que se trate. En una aplicación determinada, puede ser deseable la transferencia de energía desde la red hacia el terminal para que, por ejemplo, el servicio de telefonía básica funcione incluso en el caso de fallos del suministro eléctrico local. La transferencia de potencia se puede llevar a cabo usando los mismos cables que se usan para la transmi-

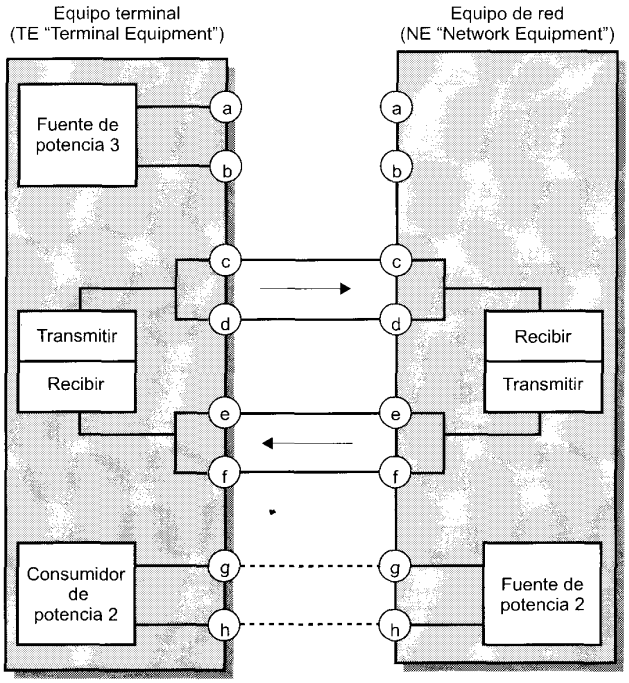


Figura 6.9. Interfaz RDSI.

sión de señal digital (c, d, e, f), o en los otros circuitos g, h. Los otros dos circuitos restantes no se usan en la configuración para RDSI pero pueden ser útiles en otras aplicaciones.

Especificaciones eléctricas

La especificación eléctrica de la RDSI establece que se use transmisión equilibrada. En la *transmisión equilibrada*, las señales se transmiten usando dos conductores como, por ejemplo, un par trenzado. Las señales se transmiten como una corriente que va a través de uno de los conductores y retorna por el otro, formando un circuito cerrado. En el caso de señales digitales, esta técnica se denomina *señalización diferencial*[3], ya que los valores binarios dependen del sentido de las diferencias de tensión entre los dos conductores. La *transmisión no equilibrada* se usa en interfaces más antiguos como la EIA-232, en la que se utiliza un solo conductor para transportar la señal, siendo el camino de retorno el circuito de tierra.

El modo equilibrado tolera más, y produce menos, ruido que el modo no equilibrado. Idealmente, las interferencias en una línea equilibrada afectarán a ambos conductores por igual y no afectarán por tanto a las diferencias de tensión. Debido a que la transmisión no equilibrada no posee estas ventajas, su uso está normalmente restringido a cables coaxiales. Cuando se usa en circuitos de intercambio, como, por ejemplo, en la EIA-232, las distancias son generalmente cortas.

El formato usado en la codificación de los datos en la interfaz RDSI depende de la velocidad de transmisión de los datos. Para la *velocidad en accesos básicos* (192 kbps) el estándar especifica la utilización de codificación pseudoternaria (véase Figura 5.2). Los unos binarios se representan por la ausencia de tensión, y el cero binario se representa por un pulso negativo o positivo de 750 mV $\pm$ 10 por ciento. Para velocidades correspondientes a *accesos primarios*, hay dos posibilidades: si se opta por una velocidad de transmisión igual a 1,544 Mbps se utiliza la codificación con inversión de marca alternante (AMI, alternate mark inversion) con B8ZS (véase Figura 5.6) y si se opta por una velocidad igual a 2,048 Mbps se utiliza la codificación AMI con HDB3. La justificación de por qué se utilizan distintos esquemas para las dos velocidades se debe a motivos históricos, ya que ninguno de los dos presenta ventajas especiales respecto al otro.

6.4. LECTURAS RECOMENDADAS

En [BLAC96] se lleva a cabo un estudio detallado y extenso de un gran número de normalizaciones para la interfaz a nivel físico. [BLAC95] se centra en las series V de las recomendaciones de la UIT-T.

BLAC95 Black, U. *The V Series Recommendations: Standards for Data Communications Over the Telephone Network.* New York: McGraw-Hill, 1996.

BLAC96 Black, U. *Physical Level Interfaces and Protocols.* Los Alamitos, CA: IEEE Computer Society Press, 1996.

6.5. PROBLEMAS

6.1. Supóngase que se envía un fichero de 10.000 bytes por una línea a 2.400 bps.

a) Calcular los bits y tiempos suplementarios introducidos si se utiliza transmisión asíncrona. Suponer un bit de comienzo y un bit de parada con longitudes igual a la de un bit de datos. Supóngase que se transmiten ocho bits de datos por cada carácter sin paridad.

[3] No se confunda con la codificación diferencial; veáse la Sección 5.1.

b) Calcular los bits y tiempos suplementarios introducidos si se utiliza transmisión síncrona. Suponer que los datos se envían en tramas. Cada trama tiene 1.000 caracteres = 8.000 bits, con una cabecera de 48 bits de control por cada trama.

c) ¿Cuáles serían las repuestas a y b para un fichero de 100.000 caracteres?

d) ¿Cuáles serían las repuestas a y b para el fichero original de 10.000 caracteres pero a una velocidad de 9.600 bps?

6.2. Una fuente generadora de datos produce caracteres IRA de 7 bits. Obtener una expresión para la velocidad de transmisión máxima (velocidad de transmisión de los bits de los datos IRA) para una línea de *B*-bps en las siguientes configuraciones:

a) Transmisión asíncrona con 1,5 bits de parada y un bit de paridad.

b) Transmisión síncrona, con una trama con 48 bits de control y 128 bits de información. El campo de información contiene caracteres IRA de 8 bits (con la paridad incluida).

c) Igual que en (b) pero con un campo de información de 1.024 bits.

6.3. Demostrar mediante un ejemplo (escribiendo una serie de bits, considerando que los bits de comienzo y parada tienen una duración de un bit) que un receptor que comete un error en la delimitación de una trama en transmisión asíncrona, puede volverse a realinear.

6.4. Supóngase que el emisor y el receptor acuerdan no usar bits de parada en una transmisión asíncrona. ¿Funcionaría la conexión? Si es así, explicar las condiciones necesarias para ello.

6.5. En un esquema de transmisión asíncrona se usan 8 bits de datos, un bit de paridad par y un elemento de parada de longitud 2 bits. ¿Cuál es el porcentaje de imprecisión que se puede permitir para el reloj del receptor sin que se cometa un error en la delimitación? Supóngase que los bits se muestrean en mitad del intervalo de señalización. Supóngase también que al principio del bit de comienzo el reloj y los bits recibidos están en fase.

6.6. Supóngase que la temporización en una línea serie con transmisión síncrona está controlada por dos relojes (uno en el emisor y otro en el receptor), lo cuales tienen una variación de un minuto cada año. ¿Cuál es la longitud máxima de una secuencia de bits sin que ocurra ningún problema de sincronización? Supóngase que un bit será correcto si se muestrea dentro del cuarenta por ciento en torno a su instante central y que el emisor y el receptor se sincronizan al principio de cada trama. Obsérvese que la velocidad de transmisión no es un factor a tener en cuenta, ya que tanto el periodo de un bit así como el error absoluto de la temporización decrecen proporcionalmente al aumentar la velocidad de transmisión.

6.7. Dibújese un diagrama de tiempos en el que se indiquen el estado de todos los circuitos EIA-232 entre dos parejas de DTC-DCE durante el curso de una llamada en una red telefónica conmutada.

6.8. Explicar el funcionamiento de cada una de las conexiones en la configuración modem-nulo de la Figura 6.8.

6.9. ¿Qué circuitos deben estar lógicamente conectados para que el circuito de bucle remoto funcione correctamente en V.24/EIA-232?

CAPÍTULO 7

Control del enlace de datos

- Las técnicas de sincronización y de transmisión a través de la interfaz son insuficientes por sí mismas debido a la existencia de posibles errores, y a que el receptor puede necesitar regular la velocidad de recepción de los datos. En cada dispositivo se necesita por tanto incluir una capa de control que regule el flujo de información, además de detectar y controlar los errores. Esta capa se denomina **protocolo de control del enlace de datos.**
- **El control del flujo** posibilita que el receptor regule el flujo de los datos enviados por el emisor, de tal manera que la memoria temporal del receptor no se desborde.
- **La detección de errores** se implementa mediante la utilización de un código con capacidad de detección de errores, que dependerá de los bits transmitidos. El código se añadirá a los bits transmitidos. Para detectar errores el receptor calculará el código en función de los bits recibidos y lo comparará con el código recibido.
- En el protocolo para el control del enlace de datos, **el control de errores** se lleva a cabo mediante la retransmisión de las tramas dañadas que no hayan sido confirmadas o las que desde el otro extremo se reciba una petición de retransmisión.

Nuestro estudio hasta ahora se ha centrado en *el envío de señales a través del enlace de transmisión*. Para conseguir que la comunicación de datos sea efectiva, se necesita mucho más: controlar y gestionar el intercambio. En este capítulo centraremos nuestra atención en el *envío de datos a través del enlace de comunicaciones*. Para llevar a cabo el control necesario, se necesita una capa lógica adicional por encima de la interfaz física estudiada en el Capítulo 6; esta lógica se denomina *control del enlace de datos* o *protocolo de control del enlace de datos*. Cuando se usa un protocolo del enlace de datos el medio de transmisión se denomina *enlace de datos*.

Para evidenciar la necesidad del control del enlace de datos, a continuación se enumeran los requisitos y los objetivos para que la comunicación de datos entre la estación emisora y la receptora (conectadas directamente) sea efectiva:

- **Sincronización de la trama:** los datos se envían en bloques que se denominan tramas. El comienzo y el final de cada trama deben ser identificables. Este aspecto se abordó brevemente cuando se estudiaron las tramas síncronas (Figura 6.2).
- **Control del flujo:** la estación emisora no debe enviar tramas a una velocidad más rápida de la que la estación receptora pueda absorber.
- **Control de errores:** se debe corregir cualquier error introducido por el sistema de transmisión en los bits.
- **Direccionamiento:** en una línea multipunto, como, por ejemplo, una red de área local (LAN), se debe identificar a las dos estaciones involucradas en la transmisión.
- **Datos y control sobre el mismo enlace:** normalmente, no se desea tener un enlace independiente para la información de control. Por consiguiente, el receptor deberá ser capaz de diferenciar entre lo que es información de control y lo que son datos.
- **Gestión del enlace:** El inicio, mantenimiento y la conclusión del intercambio de datos un alto grado de coordinación y cooperación entre las estaciones. Se necesitan pues, una serie de procedimientos para gestionar este intercambio.

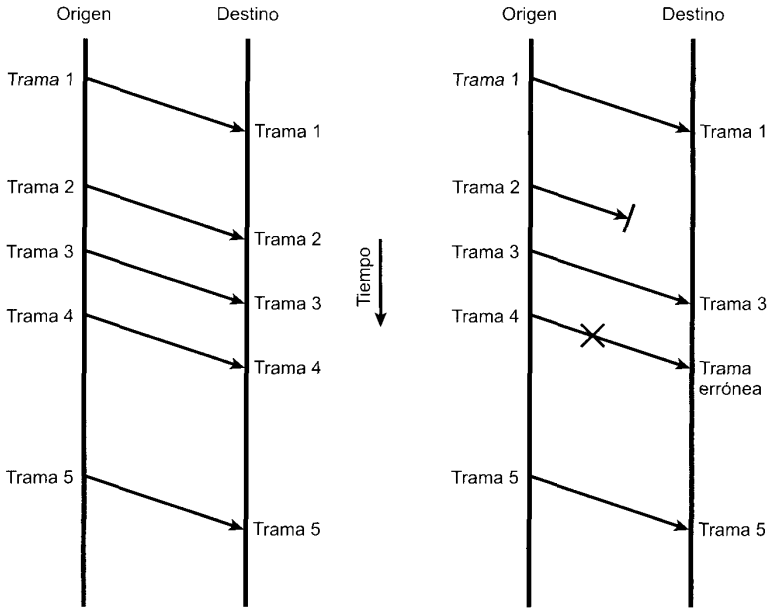
Ninguno de los requisitos anteriores se cumplen en las técnicas para la interfaz física estudiadas en el Capítulo 6. En este capítulo se verá que un protocolo que satisfaga todos los requisitos mencionados

es bastante complejo. Comenzaremos considerando los tres procedimientos clave que son parte del control del enlace de datos: el control del flujo, la detección de errores y el control de errores. Después de estudiar los procedimientos básicos anteriores, se considerará el ejemplo de protocolo de control del enlace más significativo: HDLC (High Level Data Link Control). Este protocolo es importante por dos razones: en primer lugar, porque es un estándar bastante utilizado y segundo, porque HDLC ha servido como referencia para el desarrollo de la mayoría de los protocolos para el control del enlace. Tras el estudio detallado del HDLC, se considerarán brevemente algunos de sus protocolos derivados. Finalmente, en el apéndice de este capítulo se tratan algunas cuestiones relacionadas con la evaluación o medida de las prestaciones del control del enlace de datos.

7.1. CONTROL DEL FLUJO

El control del flujo es una técnica utilizada para asegurar que la entidad de transmisión no sobrecargue a la entidad receptora con una excesiva cantidad de datos. La entidad receptora reserva generalmente una zona de memoria temporal para la transferencia. Cuando se reciben los datos, el receptor debe realizar cierta cantidad de procesamiento antes de pasar los datos al software de los niveles superiores. Si no hubiera procedimientos para el control del flujo, la memoria temporal del receptor se podría llenar y potencialmente desbordarse mientras se estuvieran procesando datos anteriores.

Comenzaremos estudiando el control del flujo en ausencia de errores. El modelo que se va a usar se muestra en la Figura 7.1a, que consiste en un diagrama donde el tiempo se representa sobre la vertical. Este diagrama es útil ya que muestra las dependencias temporales y proporciona una idea correcta de la relación entre el emisor y el receptor. Cada fila representa una única trama que transita por el enlace de datos establecido entre dos estaciones. Los datos se envían usando una secuencia de tramas, en la que



(a) Transmisión sin errores (b) Transmisión con pérdidas y errores

Figura 7.1. Un modelo para la transmisión de las tramas.

cada trama contiene un campo de datos más información de control. Se define tiempo de transmisión como el tiempo empleado por una estación para emitir todos los bits de una trama, que por definición será proporcional a la longitud de la trama. Se define como tiempo de propagación al empleado por un bit en atravesar el medio de transmisión desde el origen hasta el destino. Por ahora, supondremos que todos las tramas que se transmiten se reciben con éxito; ninguna trama se pierde, ni ninguna llega con errores. Es más, las tramas llegan en el mismo orden en que fueron transmitidas. No obstante, cada trama transmitida sufrirá un retardo arbitrario y variable antes de ser recibida[1].

CONTROL DE FLUJO MEDIANTE PARADA-Y-ESPERA

El procedimiento más sencillo para controlar el flujo, denominado control del flujo mediante parada-y-espera, funciona de la siguiente manera. Una entidad fuente transmite una trama. Tras la recepción, la entidad destino indica su deseo de aceptar otra trama enviando una confirmación de la trama que se acaba de recibir. La fuente antes de transmitir la trama siguiente debe esperar hasta que se reciba la confirmación. El destino puede de esta manera parar el flujo de los datos, simplemente reteniendo las confirmaciones. Este procedimiento funciona bien y, de hecho, es difícil mejorar sus prestaciones cuando el mensaje se envía usando un número reducido de tramas de gran tamaño. No obstante, es frecuente que la fuente rompa el bloque de datos en bloques pequeños, transmitiendo los datos en varias tramas. Esto se efectúa así por las siguientes razones:

- El tamaño de la memoria temporal del receptor puede ser limitado.
- Cuanto más larga sea la transmisión, es más probable que haya errores, necesitando en ese caso la retransmisión de la trama completa. Si se usan tramas más pequeñas, los errores se detectarán antes, y en ese caso se necesitará retransmitir una cantidad de datos menor.
- En un medio compartido, como, por ejemplo, en una LAN, es frecuente que no se permita que una estación ocupe el medio durante un periodo largo, evitando así que las otras estaciones que intenten transmitir sufran grandes retardos.

Si se usan varias tramas para un solo mensaje, el procedimiento de parada-y-espera puede ser inadecuado. Esencialmente, el problema radica en que cada vez sólo puede haber una trama en tránsito. En situaciones donde la longitud del enlace[2] sea mayor que la longitud de la trama, aparecen ineficiencias importantes. Estos problemas se muestran en la Figura 7.2. En la figura, el tiempo de transmisión (el tiempo que tarda una estación en transmitir una trama) se normaliza a la unidad, y el retardo de propagación (el tiempo que tarda un bit en llegar desde el emisor hasta el receptor) se expresa como la variable a. En otras palabras, cuando a es menor que 1, el tiempo de propagación es menor que el tiempo de transmisión. En este caso, la trama es lo suficientemente larga para que los primeros bits de la misma lleguen al destino antes de que la fuente haya terminado la transmisión de la trama. Cuando a es mayor que 1, el tiempo de propagación es mayor que el tiempo de transmisión. En este caso, el emisor termina la transmisión de toda la trama antes que el primer bit de la misma llegue al receptor. Es decir, para velocidades de transmisión y/o distancias grandes es aconsejable la utilización de valores grandes de a. En el Apéndice 7A se discuten cuestiones relacionadas con las prestaciones del enlace de datos y el parámetro a.

Las dos partes de la Figura 7.2 (a y b) consisten en una secuencia de instantáneas del proceso de transmisión tomadas a lo largo del tiempo. En ambos casos, las cuatro primeras instantáneas muestran el proceso de la transmisión de una trama que contienen datos, y la última muestra la devolución de una trama pequeña de confirmación. Nótese que para $a > 1$, la línea está siempre infrautilizada, y para el

[1] En un enlace punto a punto directo, el retardo es fijo y no variable. No obstante, se puede utilizar un protocolo de control del enlace de datos en una conexión de red, como, por ejemplo, un circuito conmutado o una red TAM, en cuyo caso el retardo puede ser variable.

[2] La longitud del enlace en bits se define como el número de bits presentes en el enlace cuando el enlace se ocupa completamente por una secuencia de bits. Matemáticamente, la longitud del enlace = $R \times (d/V)$, don de R = velocidad de transmisión en bps, d = la distancia del enlace en metros, y V = velocidad de propagación en m/s.

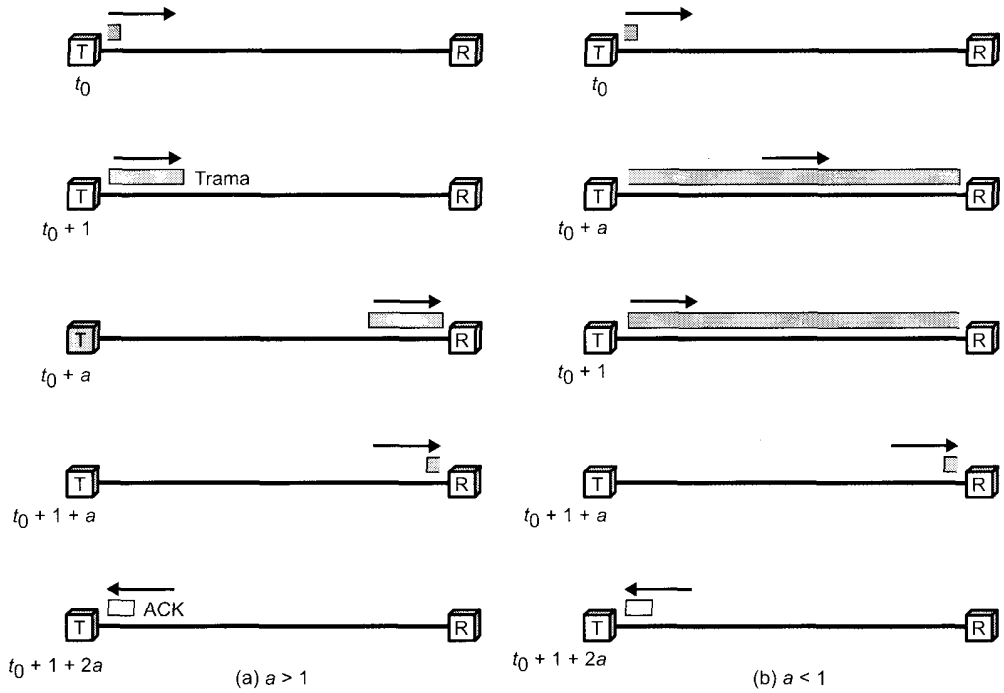


Figura 7.2. Utilización del enlace mediante parada-y-espera (tiempo de transmisión = 1; tiempo de propagación = a).

caso en que $a < 1$, la línea está utilizada ineficientemente. Resumiendo, el procedimiento de control del flujo mediante parada-y-espera da lugar a una utilización ineficiente de la línea para el caso de velocidades de transmisión muy altas entre emisores y receptores que estén separados por grandes distancias.

CONTROL DE FLUJO MEDIANTE VENTANA DESLIZANTE

El problema comentado con anterioridad radica fundamentalmente en el hecho de que cada vez sólo una trama puede estar en tránsito. En todas aquellas situaciones en las que la longitud del enlace en bits sea mayor que la longitud de la trama ($a > 1$), aparecerán problemas de ineficiencia. Si se permite que varias tramas transiten al mismo tiempo en el enlace, la eficiencia se podrá mejorar significativamente.

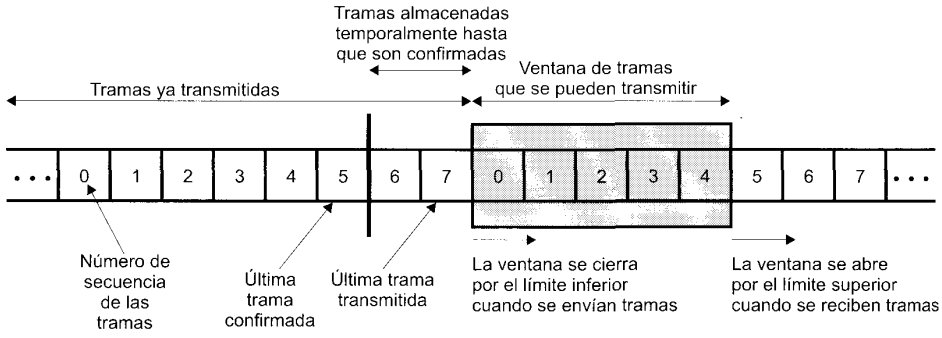
Examinemos cómo funcionaría este procedimiento para dos estaciones, A y B, conectadas mediante un enlace full-duplex. La estación B reserva memoria temporal suficiente para almacenar W tramas. Por lo tanto, B puede aceptar W tramas, y a A se le permite enviar W tramas sin tener que esperar ninguna confirmación. Para mantener un seguimiento sobre qué tramas se han confirmado, cada una de ellas se etiqueta con un número de secuencia. B confirma una trama enviando una confirmación que incluye el número de secuencia de la siguiente trama que se espera recibir. Esta confirmación implícitamente también informa de que B está preparado para recibir las W tramas siguientes, a partir de la especificada. Este esquema también se puede utilizar para confirmar varias tramas simultáneamente. Por ejemplo, B podría recibir las tramas 2, 3 y 4, pero retener la confirmación hasta que la trama 4 llegara. Al devolver la confirmación con número de secuencia 5, B confirma simultáneamente las tramas 2, 3 y 4. A mantiene una lista con los números de secuencia que se le permite transmitir, y B mantiene una lista con los números de secuencia que está esperando recibir. Cada una de estas listas se puede considerar como una *ventana* de tramas. De ahí que este procedimiento se denomine *control de flujo mediante ventana deslizante* (sliding-window flow control).

Es necesario hacer algunos comentarios adicionales. Debido a que la numeración de las tramas ocupa un campo en las mismas, evidentemente dicha numeración tendrá un tamaño limitado. Por ejemplo, si se considera un campo de 3 bits, los números de secuencia pueden variar entre 0 y 7. Por consiguiente, las tramas se numeran módulo 8; es decir, después del número 7 vendrá el 0. En general, para un campo de k bits el rango de números de secuencia irá desde 0 hasta $2^k - 1$, y las tramas se numerarán módulo 2^k.

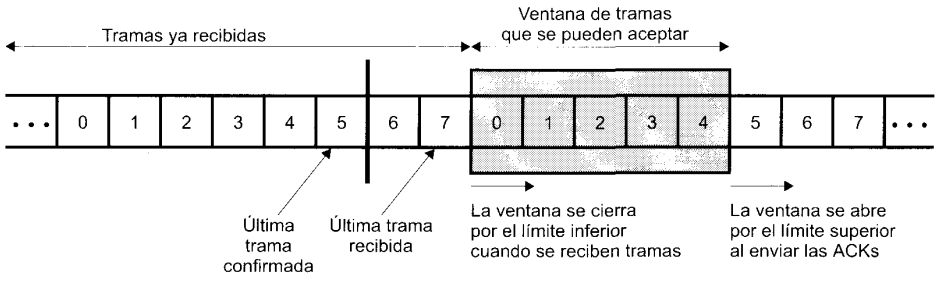
Teniendo esto en cuenta, la Figura 7.3 muestra una forma útil de representar el procedimiento de la ventana deslizante. En la figura, se supone la utilización 3 bit para los números de secuencia, luego las tramas se numeran secuencialmente desde 0 a 7, utilizando los mismos números cíclicamente para las tramas sucesivas. El rectángulo sombreado indica las tramas que se pueden transmitir; en el ejemplo de la figura el emisor debe transmitir 5 tramas empezando por la 0. Cada vez que se envíe una trama, la ventana sombreada se cerrará reduciendo su tamaño; cada vez que se reciba una confirmación, la ventana sombreada se abrirá. Las tramas que estén entre la barra vertical y la ventana sombreada han sido ya enviadas pero todavía no han sido confirmadas. Como se verá posteriormente, el emisor debe almacenar estas tramas en la memoria temporal por si hubiera que retransmitirlas.

Dada una longitud para los números de secuencia, el tamaño de la ventana real no necesita ser el máximo posible. Por ejemplo, si se usan números de secuencia de 3 bits, para las estaciones que utilicen el protocolo de ventana deslizante, se podría configurar un tamaño de la ventana igual a 4.

En la Figura 7.4 se muestra un ejemplo, en el que se supone un campo de 3 bits para los números de secuencia y un tamaño máximo para las ventanas igual a siete tramas. Inicialmente, A y B tienen las ventanas indicando que A puede transmitir siete tramas, comenzando con la trama 0 (F0). Tras transmitir tres tramas (F0, F1, F2) sin confirmación, A habrá cerrado su ventana hasta tener un tamaño de 4



(a) Desde el punto de vista del transmisor



(b) Punto de vista del receptor

Figura 7.3. Descripción de la ventana deslizante.

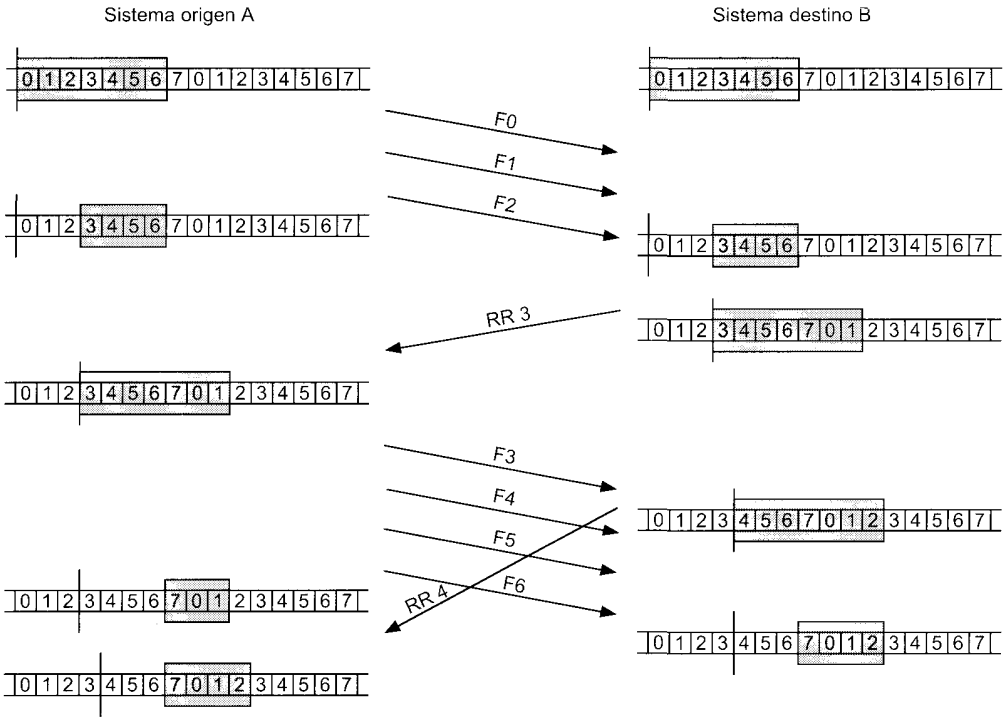


Figura 7.4. Ejemplo de un protocolo de ventana deslizante.

tramas, quedándose con una copia de las tres tramas transmitidas. La ventana indica que A puede transmitir cuatro tramas, empezando a partir de la trama número 3. B entonces transmite una trama receptor preparado RR 3 (receive ready), lo que significa: «He recibido todas las tramas hasta la trama número 2 y estoy preparado para recibir la trama 3; de hecho, estoy preparado para recibir siete tramas, empezando por la trama número 3». Con esta confirmación, a la estación A se le permite transmitir siete tramas, empezando por la trama 3; también A puede descartar las tramas almacenadas en la memoria temporal que acaban de ser confirmadas. A empieza transmitiendo las tramas 3, 4, 5 y 6. B devuelve una RR 4, con la que se confirma F3, y permite la posterior transmisión de la F4 y siguientes, hasta la F2. Cuando la RR llega a A, se ha transmitido ya la F4, F5 y F6, por lo que A sólo abre su ventana para permitir la transmisión de cuatro tramas a partir de la F7.

El mecanismo que se ha descrito, de hecho proporciona un procedimiento para controlar el flujo: el receptor sólo es capaz de aceptar las siete tramas siguientes a última que haya sido confirmada. La mayoría de los protocolos también permiten que una estación pueda interrumpir totalmente la transmisión de tramas desde el otro extremo enviando un mensaje Receptor No Preparado (RNR, Receive Not Ready), con el que se confirman las tramas anteriores pero prohíbe la transmisión de tramas adicionales. Por tanto, RNR 5 significa: «He recibido todas las tramas hasta la número 4 pero soy incapaz de aceptar más». En algún momento posterior, la estación deberá transmitir una confirmación que reabra la ventana.

Hasta ahora, hemos considerado la transmisión de tramas en una sola dirección. Si hay dos estaciones intercambiando datos, cada una de ellas deberá mantener dos ventanas, una para recibir y otra para transmitir, y cada extremo deberá enviar al otro tanto datos como confirmaciones. Para llevar a cabo esto, se utiliza un procedimiento denominado *incorporación de confirmación*. Cada *trama de datos* incluirá un campo en el que se indica el número de secuencia de esa trama más un campo que indicará el número de secuencia confirmado. Por tanto, si una estación tiene datos y una confirmación que enviar, lo hará conjuntamente utilizando una sola trama, ahorrando así capacidad del canal. Por supuesto, si una

estación tiene que enviar una confirmación pero no tiene datos, se enviará una *trama de confirmación*, como, por ejemplo, una RR o una RNR. Si la estación tiene datos pero nada que confirmar, en ausencia de nada mejor, repetirá la última confirmación enviada con anterioridad. Esto se debe a que en la trama de datos se prevé un campo para el número de secuencia confirmada, y, por tanto, habrá que rellenar este campo con algo. Cuando una estación recibe una confirmación repetida, simplemente la ignorará.

El control del flujo mediante ventanas deslizantes es potencialmente mucho más eficiente que el control del flujo mediante un procedimiento de parada-y-espera. La razón reside en que, con un control del flujo mediante ventana deslizante, el enlace de transmisión se considera como si se tratara de una tubería que se puede rellenar con tramas en tránsito. Por el contrario, en el control del flujo mediante parada-y-espera, sólo cabe una sola trama en la tubería. En el Apéndice 7A se mide en términos cuantitativos las mejoras obtenidas en la eficiencia.

7.2. DETECCIÓN DE ERRORES

En los primeros capítulos se comentaron las limitaciones y defectos de las líneas de transmisión y el efecto de la velocidad de transmisión y de la relación señal-ruido en la tasa de errores por bit. En todo sistema de transmisión habrá ruido, independientemente de cómo haya sido diseñado. El ruido dará lugar a errores que modificarán uno o varios bits de la trama.

Definamos las probabilidades en términos de los errores en las tramas transmitidas:

P_b: Probabilidad de un bit erróneo, también denominada tasa de error por bit BER (Bit Error Rate).

P_1: Probabilidad de que una trama llegue sin errores.

P_2: Probabilidad de que una trama llegue con uno o más errores no detectables.

P_3: Probabilidad de que una trama llegue con uno o más errores detectables pero sin errores indetectables.

Primero se considerará el caso en el que no se toman medidas para detectar errores. En ese caso, la probabilidad de errores detectables (P_3) es cero. Para calcular las otras probabilidades, se supondrá que todos los bits tienen una probabilidad de error (P_b) constante, independientemente de donde estén situados en la trama. Entonces se tiene que:

$$P_1 = (1 - P_b)^F$$
$$P_2 = 1 - P_1$$

Donde F es el número de bits por trama. En otras palabras, como cabría esperar, la probabilidad de que una trama llegue sin ningún bit erróneo disminuye al aumentar la probabilidad de que un bit sea erróneo. Además, la probabilidad de que una trama llegue sin errores disminuye al aumentar la longitud de la misma; cuanto mayor es la trama, mayor número de bits tendrá, y mayor será la probabilidad de que alguno de los bits sea erróneo.

Consideremos un ejemplo sencillo para mostrar estas relaciones. Un objetivo predefinido en las conexiones RDSI es la BER en un canal a 64 kbps debe ser menor que 10^{-6} para por lo menos el 90 por ciento de los intervalos observados de 1 minuto de duración. Supóngase ahora que se tiene un usuario con requisitos menos exigentes para el que como mucho una trama con un bit erróneo no detectable ocurriera por cada día de funcionamiento continuo de un canal a 64 kbps, y supóngase que la longitud de la trama es de 1.000 bits. El número de tramas que se pueden transmitir por día es $5{,}529 \times 10^6$, lo que implica una tasa de tramas erróneas $P_2 = 1/(5{,}529 \times 10^6) = 0{,}18 \times 10^{-6}$. Pero si se supone un valor de P_b igual a 10^{-6}, entonces $P_1 = (0{,}999999)^{1.000} = 0{,}999$ y, por tanto, $P_2 = 10^{-3}$, que está tres órdenes de magnitud por encima de lo requerido.

Éste es el tipo de resultados que justifica el uso de técnicas para la detección de errores. Todas ellas se basan en el siguiente principio (Figura 7.5). Dada una trama de bits, se añaden bits adicionales por

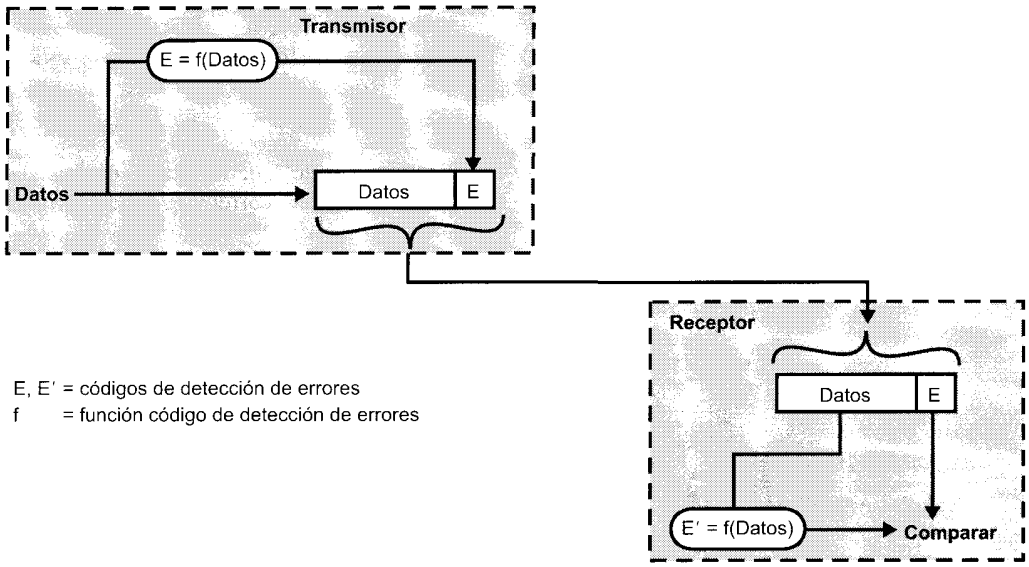


Figura 7.5. Detección de errores.

parte del transmisor para formar un código con capacidad de detectar errores. Este código se calculará en función de los otros bits que se vayan a transmitir. El receptor realizará el mismo cálculo y comparará los dos resultados. Se detectará un error si y solamente si los dos resultados mencionados no coinciden. Por tanto, P_3 es la probabilidad de que la trama contenga errores y el sistema los detecte. P_2 se denomina tasa de error residual, y es la probabilidad de que no se detecte un error aunque se esté usando un esquema de detección de errores.

COMPROBACIÓN DE PARIDAD

El esquema más sencillo para detectar errores consiste en añadir un bit de paridad al final del bloque de datos. Un ejemplo típico es la transmisión de caracteres, en la que se añade un bit de paridad por cada carácter IRA de 7 bits. El valor de este bit se determina de tal forma que el carácter resultante tenga un número impar de unos (paridad impar) o un número par (paridad par). Así, por ejemplo, si el transmisor está transmitiendo una G en IRA (1110001) y se utiliza paridad impar, se añadirá un 1 y se transmitirá 11100011. El receptor examina el carácter recibido y, si el número total de unos es impar, supondrá que no ha habido errores. Si un bit (o cualquier número impar de bits) se invierte erróneamente durante la transmisión (por ejemplo, 11000011), entonces el receptor detectará un error. Nótese, no obstante, que si dos (o cualquier número par) de bits se invierten debido a un error, aparecerá un error no detectado. Generalmente, se utiliza paridad par para la transmisión síncrona y paridad impar para la asíncrona.

La utilización de bits de paridad no es infalible, ya que los impulsos de ruido son a veces lo suficientemente largos como para destruir más de un bit, especialmente a velocidades de transmisión altas.

COMPROBACIÓN DE REDUNDANCIA CÍCLICA (CRC, CYCLIC REDUNDANCY CHECK)

Uno de los códigos para la detección de errores más habitual y más potente son los de comprobación de redundancia cíclica (CRC), que se pueden explicar de la siguiente manera. Dado un bloque o mensaje de k-bits, el transmisor genera una secuencia de n-bits, denominada secuencia de comprobación de la trama (FCS, frame check sequence), de tal manera que la trama resultante, con $n + k$ bits, sea divisible por algún número predeterminado. El receptor entonces dividirá la trama recibida por ese número y, si no hay resto en la división, se supone que no ha habido errores.

Para aclarar este procedimiento, se presenta el procedimiento de tres maneras: usando aritmética módulo 2, mediante polinomios y usando lógica digital.

Aritmética módulo 2

La aritmética módulo 2 hace uso de sumas binarias sin acarreo, que es exactamente igual que la operación lógica «exclusive-OR». La operación de resta binaria sin acarreos es también igual que la lógica «exclusive-OR». Por ejemplo:

$$\begin{array}{rrr} 1111 & 1111 & 11001 \\ +\ 1010 & -\ 0101 & \times\ 11 \\ \hline 0101 & 1010 & 11001 \\ & & 110010 \\ & & \hline & & 101011 \end{array}$$

Algunas definiciones:

T = trama de $(k + n)$ bits a transmitir, con $n < k$
M = mensaje de k-bits, los primeros k bits de T
F = n-bits del FCS, los últimos n bits de T
P = patrón de $n + 1$ bits; éste es el divisor elegido

El objetivo es que la división T/P no dé resto alguno. Es evidente que

$$T = 2^n M + F$$

Multiplicar M por 2^n, en realidad equivale a desplazar hacia la izquierda n bits, añadiendo ceros al resultado. Finalmente en la obtención de T, al sumar F lo que estamos haciendo es, en realidad, concatenar M y F. El objetivo es hacer T divisible por P. Supóngase que se divide $2^n M$ por P:

$$\frac{2^n M}{P} = Q + \frac{R}{P} \tag{7.1}$$

Hay un cociente y un resto. El resto será siempre al menos un bit más corto que el divisor, ya que la división es módulo 2. Finalmente, la secuencia de comprobación de la trama o FCS será igual al resto de la división. Entonces

$$T = 2^n M + R$$

¿Satisface R la condición exigida de que la división T/P tenga resto cero? Para comprobarlo considérese que:

$$\frac{T}{P} = \frac{2^n M + R}{P}$$

Sustituyendo en la Ecuación (7.1), se tiene que

$$\frac{T}{P} = Q + \frac{R}{P} + \frac{R}{P}$$

No obstante, cualquier número binario sumado módulo 2 consigo mismo da cero. Por tanto

$$\frac{T}{P} = Q + \frac{R + R}{P} = Q$$

No hay resto, y por tanto T es divisible por P. Así pues la FCS se genera fácilmente: simplemente se divide 2^nM por P y se usa el resto como FCS. En el receptor, se divide T por P, no obteniéndose resto alguno mientras no haya habido errores.

Considérese el siguiente ejemplo.

1. Dado

el mensaje M = 1010001101 (10 bits)
el patrón P = 110101 (6 bits)
la FCS R = se debe calcular (5 bits)

2. El mensaje M se multiplica por 2^5, resultando 101000110100000.
3. El resultado anterior se divide por P:

```
                    1 1 0 1 0 1 0 1 1 0 ← Q
P→ 1 1 0 1 0 1 ⟌ 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 ← 2^nM
                  1 1 0 1 0 1
                    1 1 1 0 1 1
                    1 1 0 1 0 1
                        1 1 1 0 1 0
                        1 1 0 1 0 1
                            1 1 1 1 1 0
                            1 1 0 1 0 1
                                1 0 1 1 0 0
                                1 1 0 1 0 1
                                    1 1 0 0 1 0
                                    1 1 0 1 0 1
                                        0 1 1 1 0 ← R
```

4. El resto se suma a 2^nM para dar T = 1010001101011110, que es lo que se transmite.
5. Si no hay errores, el receptor recibe T intacto. La trama recibida se divide por P:

```
                    1 1 0 1 0 1 0 1 1 0 ← Q
P→ 1 1 0 1 0 1 ⟌ 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0 ← 2^nM
                  1 1 0 1 0 1
                    1 1 1 0 1 1
                    1 1 0 1 0 1
                        1 1 1 0 1 0
                        1 1 0 1 0 1
                            1 1 1 1 1 0
                            1 1 0 1 0 1
                                1 0 1 1 1 1
                                1 1 0 1 0 1
                                    1 1 0 1 0 1
                                    1 1 0 1 0 1
                                        0 ← R
```

Ya que no hay resto, se supone que no habrá habido errores.

El patrón P se elige con una longitud de un bit más que la FCS deseada, y el patrón elegido en particular depende del tipo de errores que se esperan sufrir. Como mínimo, el bit más significativo y el menos significativo de P deben ser 1.

Hay un método conciso para detectar la presencia de uno o más errores. Un error dará lugar a que un bit se invierta. Esto es equivalente a calcular la función «exclusive-OR» entre el bit y 1 (es decir sumar módulo 2 un 1 a dicho bit): $0 + 1 = 1$; $1 + 1 = 0$. Por tanto los errores en una trama de $(n + k)$ bits se pueden representar mediante una palabra de $(n + k)$ bits, teniendo 1 en aquellas posiciones que coincidan con un error. La trama T_r resultante se puede expresar como

$$T_r = T \oplus E$$

donde

T = es la trama transmitida

E = es el patrón de errores con 1 en las posiciones donde haya un error

T_r = es la trama recibida

El receptor fallará en la detección de un error si y solamente si T_r es divisible por P, lo que es equivalente a que E sea divisible por P. Intuitivamente, esto parece que es un evento improbable.

Polinomios

Una segunda forma de ver el proceso CRC es expresar todos los valores como polinomios de una variable muda X, con coeficientes binarios. Los coeficientes corresponderán con los bits del número en binario. Así, si $M = 110011$, se tendrá que $M(X) = X^5 + X^4 + X + 1$, y si $P = 11001$, se tiene que $P(X) = X^4 + X^3 + 1$. De nuevo las operaciones aritméticas son en módulo 2. El procedimiento CRC se puede describir de la siguiente manera:

$$1. \quad \frac{X^n M(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$

$$2. \quad T(X) = X^n M(X) + R(X)$$

Un error $E(X)$ no se detectará si es divisible por $P(X)$. Se puede demostrar [RAMA88] que los siguientes errores no son divisibles mediante la elección del polinomio adecuado $P(X)$, y, por tanto, se podrán detectar:

- Todos los errores de un único bit.
- Todos los errores dobles, siempre que $P(X)$ tenga al menos tres 1.
- Cualquier número impar de errores, siempre que $P(X)$ contenga el factor $(X + 1)$.
- Cualquier ráfaga de errores en la que la longitud de la ráfaga sea menor que la longitud del polinomio divisor; es decir, menor o igual que la longitud de la FCS.
- La mayoría de la ráfagas de mayor longitud.

Es más, se puede demostrar que si todos los patrones de error son equiprobables, entonces para una ráfaga de errores de longitud $r + 1$, la probabilidad de que no se detecte un error [$E(X)$ sea divisible por $P(X)$] es $1/2^{r-1}$, y para ráfagas mayores, la probabilidad es $1/2^r$, donde r es la longitud de la FCS.

Es frecuente utilizar alguna de las cuatro definiciones siguientes para $P(X)$:

$$\text{CRC-12} \quad = X^{12} + X^{11} + X^3 + X^2 + X + 1$$

$$\text{CRC-16} \quad = X^{16} + X^{15} + X^2 + 1$$

$$\text{CRC-CCITT} \quad = X^{16} + X^{12} + X^5 + 1$$

$$\text{CRC-22} \quad = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

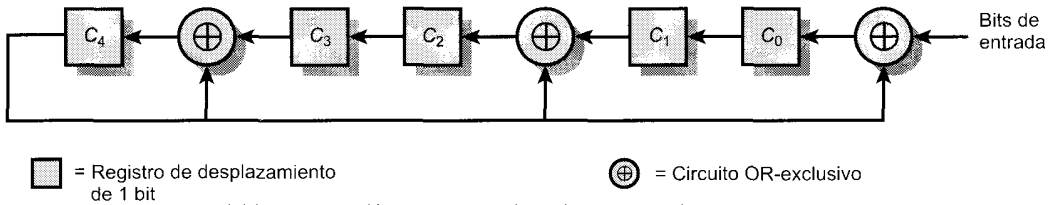
El CRC-12 se utiliza para la transmisión de secuencias de caracteres de 6 bits y genera una FCS de 12 bits. Tanto el CRC-16 como el CRC-CCITT son habituales para los caracteres de 8 bits, y se utilizan en los Estados Unidos y en Europa respectivamente, ambos generan una FCS de 16 bits. Esto podría parecer adecuado para la mayoría de las aplicaciones, aunque el CRC-32 se ha especificado como una opción en algunas normas para la transmisión síncrona sobre enlaces punto a punto.

Lógica digital

El procedimiento CRC se puede representar, y de hecho implementar, con un circuito divisor formado por puertas «exclusive-OR» y un registro de desplazamiento. El registro de desplazamiento es una cadena de elementos de memoria de 1 bit. Cada elemento tiene una línea de salida, que indica el valor almacenado actualmente, así como una línea de entrada. A instantes discretos de tiempo, establecidos por una señal de reloj, el valor almacenado en el elemento de memoria se reemplaza por el valor que se encuentre en la línea de entrada. Todo el registro utiliza una señal de reloj común, que provoca un desplazamiento de un bit a lo largo de todo el registro.

El circuito se realiza de la siguiente manera:

1. El registro contendrá n bits, igual a la longitud de la FCS.
2. Hay n puertas «exclusive-OR».



(a) Implementación mediante registro de desplazamiento

	C_4	C_3	C_2	C_1	C_0	$C_4 \oplus C_3$	$C_4 \oplus C_1$	$C_4 \oplus$ entrada	entrada	
Iniciali-zación	0	0	0	0	0	0	0	1	1	
Paso1	0	0	0	0	1	0	0	0	0	
Paso2	0	0	0	1	0	0	1	1	1	
Paso3	0	0	1	0	1	0	0	0	0	
Paso4	0	1	0	1	0	1	1	0	0	
Paso5	1	0	1	0	0	1	1	1	0	Mensaje a enviar
Paso6	1	1	1	0	1	0	1	0	1	
Paso7	0	1	1	1	0	1	1	1	1	
Paso8	1	1	1	0	1	0	1	1	0	
Paso9	0	1	1	1	1	1	1	1	1	
Paso10	1	1	1	1	1	0	0	1	0	
Paso11	0	1	0	1	1	1	1	0	0	
Paso12	1	0	1	1	0	1	0	1	0	Cinco ceros añadidos
Paso13	1	1	0	0	1	0	1	1	0	
Paso14	0	0	1	1	1	0	1	0	0	
Paso15	0	1	1	1	0	1	1	0	—	

(b) Ejemplo con entrada 1010001101

Figura 7.6. Circuito con registros de desplazamiento para dividir el polinomio $X^5 + X^4 + X^2 + 1$.

3. La presencia o ausencia de puerta corresponderá con la presencia o ausencia del término correspondiente en el polinomio divisor, $P(X)$, excluyendo al término X^n.

La arquitectura de este circuito se explica mejor considerando un caso particular, como el ejemplo que se muestra en la Figura 7.6. En este ejemplo se usa:

$$\text{Mensaje } M = 1010001101; \qquad M(X) = X^9 + X^7 + X^3 + X^2 + 1$$

$$\text{Divisor } P = 110101; \qquad P(X) = X^5 + X^4 + X^2 + 1$$

definidas anteriormente.

En la Figura 7.6a se muestra la realización del registro de desplazamiento. El proceso comienza con la puesta a cero de todo el registro. El mensaje o dividendo, se introduce a continuación, bit a bit, comenzado con el bit más significativo. La Figura 7.6b es una tabla que muestra el funcionamiento paso a paso por cada bit de entrada. Cada fila de la tabla muestra los valores almacenados en los cinco elementos de memoria del registro de desplazamiento. Es más, las filas muestran los valores que aparecerán en las salidas de los tres circuitos «exclusive-OR». Finalmente, en cada columna se muestra el valor del siguiente bit de entrada, que estará disponible para el siguiente paso.

Debido a que no hay realimentación hasta que un 1 del dividendo aparezca en el extremo más significativo del registro, las primeras cinco operaciones son simplemente desplazamientos. Siempre que un 1 llegue al extremo izquierdo del registro (C_4), se resta 1 («exclusive-OR») del segundo (C_3), cuarto (C_1) y sexto (entrada) bit del siguiente desplazamiento. Esto es idéntico al procedimiento de la división binaria mencionado anteriormente. El procedimiento continúa para todos los bits del mensaje más los cinco bits igual a cero. Estos últimos son para desplazar M cinco posiciones a la izquierda para dar cabida a la FCS. Tras procesar el último bit, el registro de desplazamiento contendrá el resto (la FCS), que puede ser transmitido (se muestra sombreado).

En el receptor, se utiliza la misma lógica. Cada bit de la trama M se introducirá en el registro de desplazamiento. Si no ha habido errores, el registro de desplazamiento debería contener el patrón de bits R al final de M. Los bits transmitidos de R empiezan a llegar, y el efecto consistirá en que cuando concluya la recepción, el registro debe contener todas las posiciones igual a cero.

La Figura 7.7 muestra una arquitectura genérica para la realización de un CRC mediante un registro de desplazamiento para el polinomio $P(X) = \sum_{i=0}^{n} A_i X^i$, donde $A_0 = A_n = 1$, y todos los otros A_i son igual a 0 o 1.

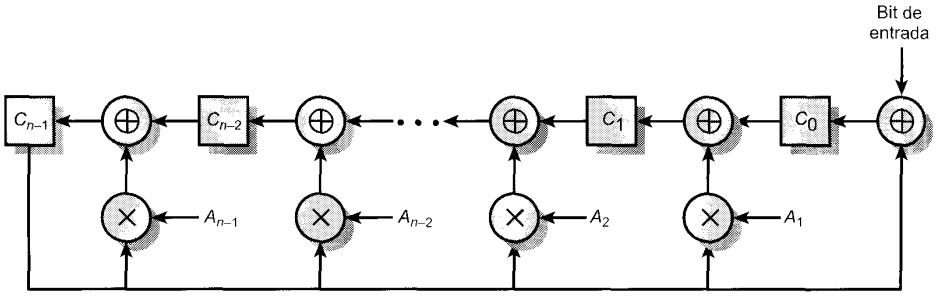


Figura 7.7. Arquitectura de un CRC genérico para implementar la división por $1 + A_1X + A_2X^2 + \cdots + A_{n-1}X^{n-1} + X^n$.

7.3. CONTROL DE ERRORES

El control de errores hace referencia a los mecanismos necesarios para la detección y la corrección de errores que aparecen en la transmisión de tramas. En la Figura 7.1b se muestra el caso típico que se va a considerar como modelo. Como se ha venido haciendo hasta ahora, los datos se envían mediante una secuencia de tramas; las tramas llegan en el mismo orden con el que fueron enviadas; y cada trama transmitida sufre antes de recibirse un retardo de magnitud arbitraria y variable. En el estudio que se va a llevar a cabo, se contemplan dos tipos de errores potenciales:

- **Trama perdida:** que se da cuando una trama enviada no llega al otro lado. Así, por ejemplo, una ráfaga de ruido puede dañar a una trama de tal manera que el receptor no se dé cuenta incluso de que se haya recibido.
- **Trama dañada:** ocurre cuando llega una trama, pero con algunos bits erróneos (modificados durante la transmisión).

Las técnicas más usuales para el control de errores se basan en algunas (o todas) de las siguientes aproximaciones:

- **Detección de errores:** discutida en la sección anterior.
- **Confirmaciones positivas:** el destino devuelve una confirmación positiva por cada trama recibida con éxito y libre de errores.
- **Retransmisión después de la expiración de un intervalo de tiempo:** la fuente retransmite las tramas que no se han confirmado tras un periodo de tiempo predeterminado.
- **Confirmación negativa y retransmisión:** el destino devuelve una confirmación negativa al detectar errores en las tramas recibidas. La fuente retransmitirá de nuevo esas tramas.

Todos estos mecanismos se denominan genéricamente **solicitud de repetición automática** (ARQ, automatic repeat request); el objetivo del ARQ es convertir un enlace de datos no seguro en seguro. Hay tres variantes del ARQ que se han normalizado:

- ARQ con parada-y-espera
- ARQ con vuelta-atrás-N
- ARQ con rechazo selectivo

Todos estos procedimientos se basan en la utilización de la técnica de control del flujo presentada en la Sección 7.1. Estudiemos cada una de ellas.

ARQ CON PARADA-Y-ESPERA

La ARQ con parada-y-espera se basa en la técnica para el control del flujo con parada-y-espera mencionada anteriormente. La estación fuente transmite una única trama y entonces debe esperar la recepción de una confirmación (ACK, «acknowledgment»). No se podrá enviar ninguna otra trama hasta que la respuesta de la estación destino vuelva al emisor.

Pueden ocurrir dos tipos de error. El primero, consistirá en que la trama que llega al destino puede estar dañada. El receptor detectará esto mediante la utilización de las técnicas de detección de errores mencionadas anteriormente y simplemente descartará la trama. Para llevar a cabo esto, la estación fuente utiliza un temporizador. Tras el envío de una trama la estación fuente espera la recepción de una confirmación. Si no se recibe confirmación antes de que el temporizador expire, la trama anterior se reenvía de nuevo. Obsérvese que este método exige que el transmisor conserve una copia de la trama transmitida hasta que se reciba la correspondiente confirmación.

El segundo tipo de error puede originarse si la confirmación se deteriora. Considérese la siguiente situación. La estación A envía una trama. La trama se recibe correctamente en la estación B, la cual responde con una confirmación (ACK). La ACK se deteriora en el camino y se modifica tal que no es

identificable por A como tal, en este caso se producirá una expiración del temporizador y se reenviará la trama. La trama duplicada llega y se acepta por B. B ha aceptado por tanto dos copias de la misma trama como si fueran distintas. Para evitar este problema, las tramas se pueden etiquetar alternadamente con 0 o 1, y las confirmaciones positivas serán de la forma ACK0 y ACK1. Para mantener las convenciones adoptadas en los procedimientos de ventanas deslizantes, un ACK0 confirma la recepción de la trama numerada con 1 e indica que el receptor está preparado para aceptar la trama numerada con 0.

En la Figura 7.8 se proporciona un ejemplo de la utilización del ARQ con parada-y-espera; en ella se muestra la transmisión de una secuencia de tramas desde el origen A al destino B. La figura muestra los dos tipos de error que se han comentado previamente. La tercera trama transmitida por A se daña o pierde y por tanto no se devuelve ninguna ACK a B. En A se produce una expiración del temporizador y retransmite la trama. Posteriormente, A transmite la trama etiquetada con 1 pero ahora se pierde su correspondiente ACK0. El temporizador en A expira y se retransmite la trama. Al recibir B dos tramas

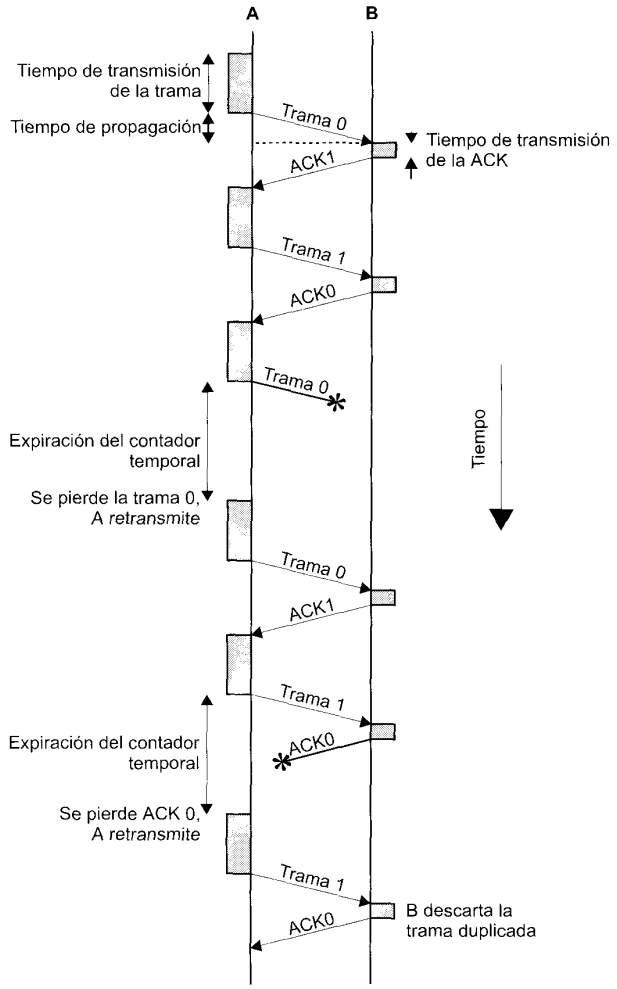


Figura 7.8. ARQ mediante parada-y-espera.

consecutivas con la misma etiqueta, descartará la segunda trama recibida pero devolverá una ACK0 para cada una de las tramas recibidas.

La ventaja principal del ARQ con parada-y-espera es su sencillez. Su desventaja principal se discutió en la Sección 7.1, y no es otra sino que el parada-y-espera es un procedimiento ineficiente. Las técnicas de control del flujo mediante ventana deslizante proporcionan una utilización mejor de la línea; en este sentido, a veces la técnica de parada-y-espera se denomina *ARQ continua*.

ARQ CON VUELTA-ATRÁS-N

La técnica de control de errores más frecuente está basada en el procedimiento para control del flujo mediante ventanas deslizantes y se denomina ARQ con vuelta-atrás-N. En esta técnica, una estación puede enviar una serie de tramas numeradas secuencialmente módulo algún valor máximo dado. Al utilizar la técnica para control del flujo mediante ventanas deslizantes el número de tramas pendientes de confirmar se determina mediante el tamaño de la ventana. Mientras no aparezcan errores, el destino confirmará (mediante una RR, «receive ready» o mediante la incorporación de la confirmación) las tramas recibidas como es habitual. Si la estación destino detecta un error en una trama, enviará una confirmación negativa (REJ, reject) para esa trama. La estación destino descartará esa trama y todas las que se reciban en el futuro hasta que la trama errónea se reciba correctamente. Por tanto, cuando la estación fuente reciba un REJ, deberá retransmitir la trama errónea más todas las tramas posteriores que hayan sido transmitidas entre tanto.

Considérese que la estación A envía tramas a la estación B. Después de cada transmisión, A inicia un temporizador para la confirmación de la trama que se acaba de enviar. Supóngase que B ha recibido la trama $(i - 1)$ sin errores y que A acaba de enviar la trama i. La técnica vuelta-atrás-N tiene en cuenta las siguientes contingencias:

1. **Trama deteriorada.** Si la trama recibida es no válida (es decir, B detecta un error), B descarta dicha trama sin más. Llegados a este punto se plantean dos posibilidades:
   - **a)** A envía la trama $(i + 1)$ dentro de un periodo de tiempo razonable. B recibe la trama $(i + 1)$ fuera de orden y envía un REJ i. A debe retransmitir la trama i y todas las posteriores.
   - **b)** A no envía tramas adicionales en un breve espacio de tiempo. B no recibe nada por lo que ni devuelve una RR ni una REJ. Cuando el temporizador de A expira, se transmitirá una trama RR que incluirá un bit denominado P, que será puesto a 1. B interpretará la trama RR con el bit P igual a 1, como si fuera una orden que debe ser confirmada enviando una RR para indicar la siguiente trama que se espera recibir, es decir la trama i. Cuando A recibe la RR, retransmite la trama i.
2. **Una RR deteriorada.** Hay dos casos posibles:
   - **a)** B recibe la trama i y envía RR $(i + 1)$, que se pierde en el camino. Ya que las confirmaciones son acumulativas (por ejemplo, RR 6 significa que todas las tramas hasta la 5 se confirman), puede ocurrir que A reciba una RR posterior para una trama posterior y que llegue antes de que el temporizador asociado a la trama i expire.
   - **b)** Si el temporizador de A expira, se transmite una orden RR, como en el caso 1b. Se inicia otro temporizador, denominado el temporizador del bit P. Si B no responde a la orden RR, o si la respuesta se deteriora, entonces el temporizador del bit P en A expirará. En este caso A lo intentará de nuevo enviando otra orden RR, reiniciando el temporizador del bit P. Este procedimiento se repite una serie de veces. Si A no recibe la confirmación tras un número máximo de intentos, comenzará un procedimiento de reinicio.
3. **Una trama REJ deteriorada.** La pérdida de una trama REJ es equivalente al caso 1b.

La Figura 7.9 es un ejemplo del flujo de tramas para un ARQ con vuelta-atrás-N. Debido al retardo de propagación en la línea, mientras que la confirmación (positiva o negativa) vuelve a la estación emi-

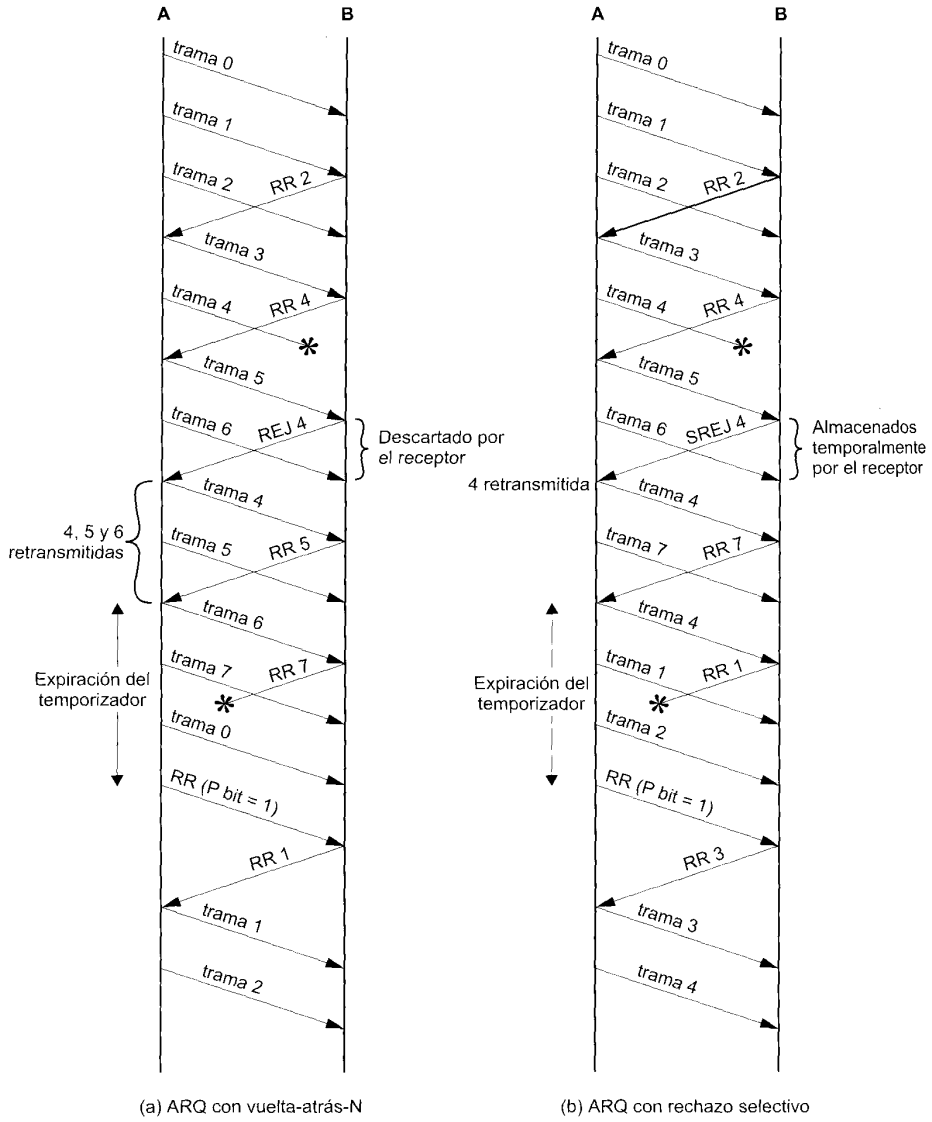


Figura 7.9. Protocolos ARQ con ventana deslizante.

sora, se habrá enviado al menos una trama más tras la primera que está siendo confirmada. En el ejemplo la trama 4 se deteriora. Las tramas 5 y 6 se reciben fuera de orden y son descartadas por B. Cuando llega la trama 5, B envía inmediatamente un REJ 4. Al recibir la REJ correspondiente a la trama 4, se debe retransmitir no sólo 4, sino que además se deberá hacer lo mismo con la 5 y con la 6. Obsérvese que el transmisor debe conservar una copia de todas las tramas que haya enviado y que no estén confirmadas.

En la Sección 7.1, se mencionó que si se tiene un campo para los números de secuencia de k bits (lo que permitiría un rango para los números de secuencia igual a 2^k) el tamaño máximo de la ventana

estará limitado a $2^k - 1$. Esto se debe a la interacción entre los procedimientos para el control de errores y las confirmaciones. Considérese que si los datos se están transmitiendo en ambas direcciones, la estación B puede enviar las confirmaciones a las tramas enviadas por A, incluidas en sus propias tramas de datos, incluso en el caso de que se hayan confirmado con anterioridad. Como ya se ha mencionado, esto es debido a que B debe poner algún número en el campo previsto para las confirmaciones en sus tramas de datos. A modo de ejemplo, supóngase que se utilizan números de secuencia de 3 bits (es decir 8 números de secuencia). Supóngase que una estación envía la trama 0 y recibe de vuelta una RR 1, posteriormente envía las tramas 1, 2, 3, 4, 5, 6, 7, 0 y recibe otra RR 1. Esto podría significar que todas las 8 tramas se recibieron correctamente y que la RR 1 es una confirmación acumulativa. También podría interpretarse como que las 8 tramas se han deteriorado o incluso perdido en el camino, y que la estación receptora está repitiendo la RR 1 anterior. Esta posible ambigüedad se evita si el tamaño máximo de la ventana se fija a 7 (es decir $2^3 - 1$).

ARQ CON RECHAZO SELECTIVO

En la ARQ con rechazo selectivo las únicas tramas que se retransmiten son aquellas para las que se recibe una confirmación negativa, denominada en este caso SREJ, o aquellas para las que el temporizador correspondiente expira. En la Figura 7.9b se muestra este esquema. Cuando la trama 5 se recibe fuera de orden, B envía un SREJ 4, indicando que la trama 4 no se ha recibido. No obstante, B sigue aceptando tramas y las almacena en la memoria temporal hasta que se reciba correctamente la trama 4. Llegados a este punto, B podrá proporcionar al software de las capas superiores las tramas en el orden correcto.

El rechazo selectivo podría parecer más eficiente que el procedimiento vuelta-atrás-N, debido a que se minimiza el número de retransmisiones. Por otra parte, el receptor deberá reservar una zona de memoria temporal lo suficientemente grande para almacenar las tramas tras una SREJ, hasta que la trama errónea se retransmita, y además debe tener lógica adicional para reinsertar la trama reenviada en la posición correspondiente. Igualmente, el transmisor también necesita una lógica más compleja para con ello ser capaz de enviar tramas fuera de orden. Debido a estas complicaciones, el ARQ con rechazo selectivo se utiliza mucho menos que el ARQ con vuelta-atrás-N.

La limitación en cuanto al tamaño máximo de la ventana es más restrictiva en el caso del rechazo selectivo que en el caso de vuelta-atrás-N. Considérese el caso de un rechazo selectivo que utilice 3 bits para los números de secuencia. Permítase un tamaño de ventana igual a 7, y ténganse en cuenta las siguientes consideraciones [TANE96]:

1. La estación A envía las tramas numeradas desde la 0 hasta la 6 a la estación B
2. La estación B recibe las siete tramas y las confirma acumulativamente con RR 7.
3. Debido a una ráfaga de ruido, la RR 7 se pierde.
4. El temporizador de A expira y se retransmite la trama 0.
5. B ha desplazado su ventana de recepción indicando que acepta las tramas 7, 0, 1, 2, 3, 4, y 5. Al recibir la numero 0 anterior supone que la trama 7 se ha perdido, y que se trata de una trama 0 diferente, por tanto la acepta.

El problema en la casuística anterior está en que se produce un solapamiento entre las ventanas de emisión y recepción. Para evitar este problema, el tamaño máximo de la ventana no debería ser mayor que la mitad del rango de los números de secuencia. En la situación anterior, si se permitiera que sólo 4 tramas estuvieran pendientes de confirmación, se evitarían las ambigüedades. En general, para un campo de números de secuencia de k bits, es decir, para un rango de 2^k, el tamaño máximo de la ventana se limita a 2^{k-1}.

7.4. CONTROL DEL ENLACE DE DATOS A ALTO NIVEL (HDLC, HIGH-LEVEL DATA LINK CONTROL)

El protocolo más importante para el enlace de datos es el HDLC (ISO 3309, ISO 4335). No sólo porque es el más utilizado, sino porque además es la base para otros protocolos importantes de esta capa, en los que se usan formatos similares e iguales procedimientos a los que se usan en HDLC. Por consiguiente, en esta sección se realiza un estudio detallado del HDLC. En la Sección 7.5 se revisan los protocolos relacionados.

CARACTERÍSTICAS BÁSICAS

Para satisfacer las demandas de un buen número de aplicaciones, HDLC define tres tipos de estaciones, dos configuraciones del enlace y tres modos de operación para la transferencia de los datos. Los tres tipos de estaciones son:

- **Estación primaria:** se caracteriza porque tiene la responsabilidad de controlar el funcionamiento del enlace. Las tramas generadas por la primaria se denominan órdenes.
- **Estación secundaria:** funciona bajo el control de la estación primaria. Las tramas generadas por la estación secundaria se denominan respuestas. La primaria establece un enlace lógico independiente para cada una de las secundarias presentes en la línea.
- **Estación combinada:** es una mezcla entre las características de las primarias y las secundarias. Una estación de este tipo puede generar tanto órdenes como respuestas.

Las dos posibles configuraciones del enlace son:

- **Configuración no balanceada:** está formada por una estación primaria y una o más secundarias. Permite tanto transmisión «full-duplex» como «semi-duplex».
- **Configuración balanceada:** consiste en dos estaciones combinadas. Permite igualmente transmisión «full-duplex» o «semi-duplex».

Los tres modos de transferencia de datos son:

- **Modo de respuesta normal** (NRM, Normal Response Mode): se utiliza en la configuración no balanceada. La estación primaria puede iniciar la transferencia de datos a la secundaria, pero la secundaria sólo puede transmitir datos usando respuestas a las órdenes emitidas por la primaria.
- **Modo balanceado asíncrono** (ABM, Asynchronous Balanced Mode): se utiliza en la configuración balanceada. En este modo cualquier estación combinada podrá iniciar la transmisión sin necesidad de recibir permiso por parte de la otra estación combinada.
- **Modo de respuesta asíncrono** (ARM, Asynchronous Response Mode): se utiliza en la configuración no balanceada. La estación secundaria puede iniciar la transmisión sin tener permiso explícito por parte de la primaria. La estación primaria sigue teniendo la responsabilidad del funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores, y la desconexión lógica.

El NRM se usa en líneas que tienen múltiples conexiones, en las que varios terminales se conectan a un computador central. El computador sondea cada una de las entradas correspondientes a los distintos terminales. El NRM se usa a veces en enlaces punto a punto, principalmente si el enlace conecta un terminal u otros periféricos al computador. El ABM es el más utilizado de los tres modos; debido a que en ABM no se necesitan hacer sondeos, la utilización de los enlaces punto a punto con full-duplex es más eficiente con este modo. ARM no se utiliza tan frecuentemente; es utilizable en algunas situaciones particulares en las que la estación secundaria necesite iniciar la transmisión.

ESTRUCTURA DE LA TRAMA

HDLC usa transmisión síncrona. Todos los intercambios se realizan a través de tramas, HDLC utiliza un formato único de tramas que es válido para todos los posibles intercambios: datos e información de control.

En la Figura 7.10 se muestra la estructura de una trama HDLC. Al campo de delimitación, de dirección y de control, que preceden al campo de información se denominan cabecera. La FCS junto con el otro campo de delimitación final que está a continuación del campo de datos de denomina *cola*.

Los campos de delimitación

Los campos de delimitación están localizados en los dos extremos de la trama, y ambos corresponden a la siguiente combinación de bits 01111110. Se puede usar un único delimitador como final y comienzo de la siguiente trama simultáneamente. A ambos lados de la interfaz entre el usuario y la red, los receptores estarán continuamente intentando detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama. Cuando se recibe una trama, la estación seguirá intentando detectar esa misma secuencia para determinar así el final de la trama. Debido a que el protocolo permite cualquier combinación de bits (es decir, el protocolo no impone restricción alguna en el contenido de los campos) no hay

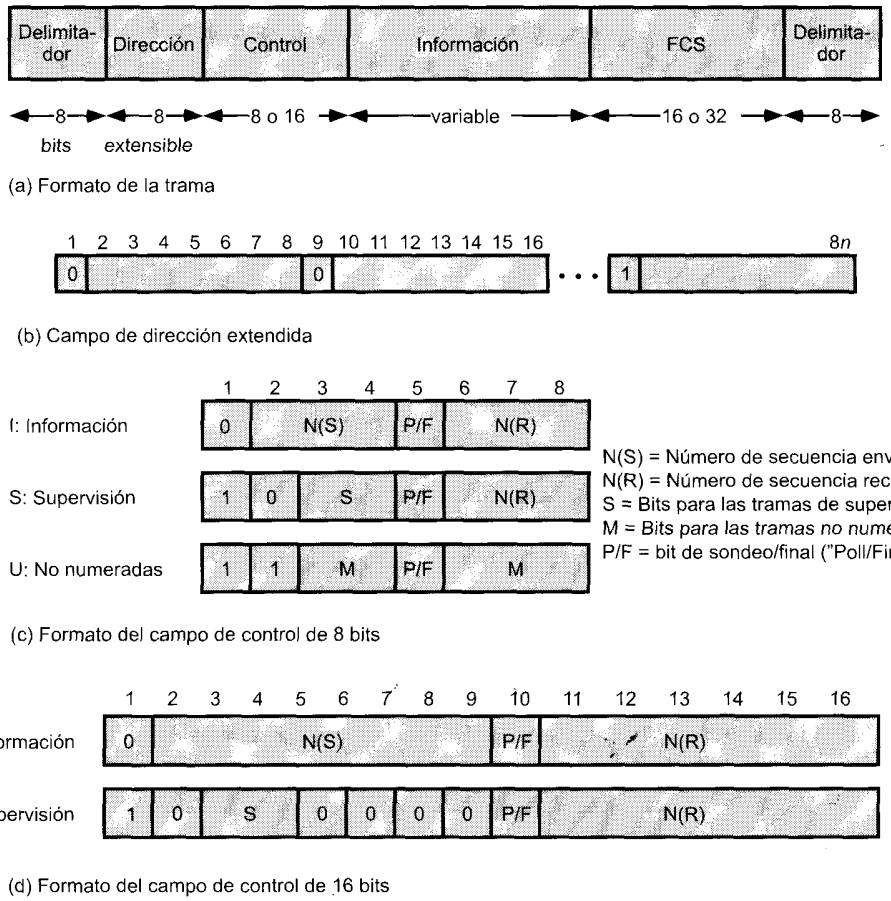


Figura 7.10. Estructura de la trama HDLC.

garantía de que la combinación 01111110 no aparezca en algún lugar dentro de la trama, destruyendo de esta manera la sincronización de las tramas. Para evitar esta situación no deseable, se utiliza un procedimiento denominado *inserción de bits*. En la transmisión de los bits que estén entre los dos delimitadores de comienzo y final, el transmisor insertará un 0 extra siempre que se encuentre con la aparición de cinco 1 consecutivos. El receptor, tras la detección del delimitador de comienzo, monitorizará la cadena de bits recibida, de tal manera que cuando aparezca una combinación de cinco 1 seguidos, el sexto bit se examinará. Si dicho bit es 0, se eliminará sin más. Si el sexto bit es un 1 y el séptimo es un 0, la combinación se considera como un delimitador. Si los bits sexto y séptimo son ambos igual a 1 se interpreta como una indicación de cierre generada por el emisor.

Al usar el procedimiento de inserción de bits, el campo de datos puede contener cualquier combinación arbitraria de bits. Esta propiedad se denomina *transparencia en los datos*.

En la Figura 7.11 se muestra un ejemplo de inserción de bits. Obsérvese que para los dos primeros casos, el 0 extra no es estrictamente necesario, pero se necesita para el buen funcionamiento del algoritmo. En la misma figura se muestran situaciones no deseadas que dan lugar a errores en la delimitación al utilizar la inserción de bits. Al usar un solo delimitador como fin y comienzo, un simple error en un solo bit causaría que las dos tramas se fundieran en una. Igualmente, la aparición de un error en un solo bit y en determinadas circunstancias podría erróneamente partir una trama en dos.

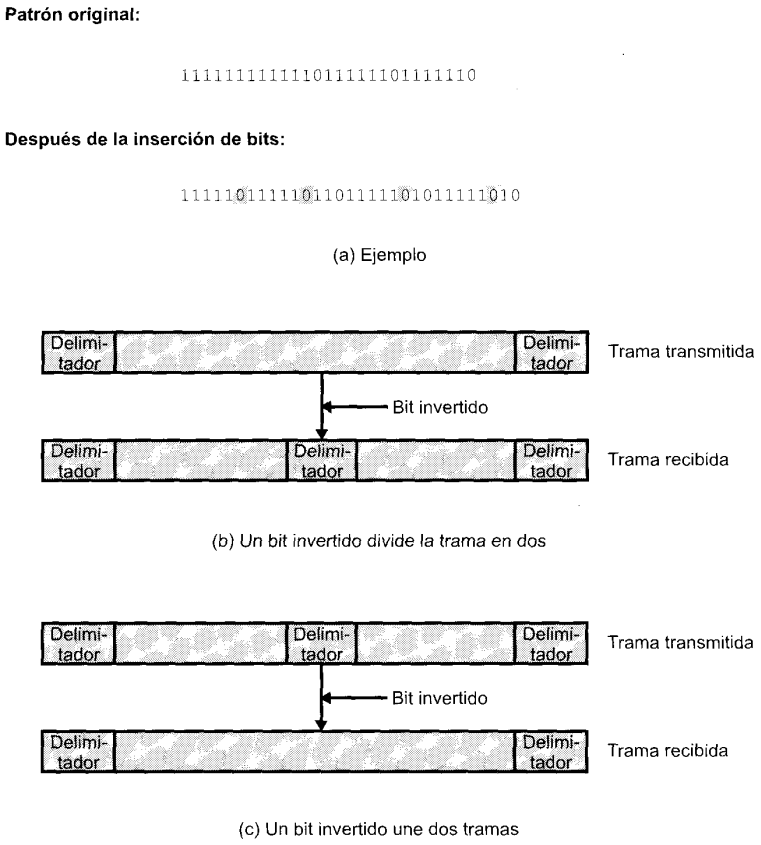


Figura 7.11. Inserción de bits.

Campo de dirección

El campo de dirección identifica a la estación secundaria que ha transmitido o que va a recibir la trama. Este campo no se necesita en enlaces punto a punto, si bien se incluye siempre por cuestiones de uniformidad. El campo de dirección tiene normalmente 8 bits, si bien tras una negociación previa, se puede utilizar un formato ampliado en el que la dirección tendrá un múltiplo de siete bits. El bit menos significativo de cada octeto será respectivamente 1 o 0, si es o no el último octeto del campo de dirección. Los siete bits restantes en cada octeto formarán la dirección propiamente dicha. Un octeto de la forma 11111111 se interpretará como una dirección que corresponde a todas las direcciones, tanto en el formato básico como ampliado. Este tipo de direccionamiento se utiliza cuando la estación primaria quiere enviar una trama a todas las secundarias.

Campo de control

En HDLC se definen tres tipos de tramas, cada una de ellas con un formato diferente para el campo de control. Las *tramas de información* (tramas-I) transportan los datos generados por el usuario (esto es, por la lógica situada en la capa superior, usuaria del HDLC). Además, en las tramas de información se incluye información para el control ARQ de errores y del flujo. Las *tramas de supervisión* (tramas-S) proporcionan el mecanismo ARQ cuando la incorporación de las confirmaciones en las tramas de información no es factible. Las *tramas no numeradas* (tramas-N) proporcionan funciones complementarias para controlar el enlace. El primer o los dos primeros bits del campo de control se utilizan para identificar el tipo de la trama. Los bits restantes se estructuran en subcampos como se indica en la Figura 7.10c y d. Su utilización se explicará posteriormente en este mismo capítulo al estudiar el funcionamiento del HDLC.

Todos los formatos posibles del campo de control contienen el bit sondeo/fin (P/F «poll/final»). Su utilización es dependiente del contexto. Normalmente, en las tramas de órdenes se denomina bit P, y se fija a 1 para solicitar (sondear) una respuesta a la entidad HDLC par. En las tramas de respuesta, el bit se denomina F, y se fija a un valor igual a 1 para identificar a la trama tipo respuesta devuelta tras la recepción de una orden.

Obsérvese que el campo de control básico en las tramas-S y en las tramas-I utiliza números de secuencia de tres bits. Utilizando una orden que fije el modo adecuado, en estas tramas se puede hacer uso de un campo de control ampliado en el que los números de secuencia sean de 7 bits. Las tramas-N siempre tienen un campo de control de 8 bits.

Campo de información

El campo de información sólo está presente en las tramas-I y en algunas tramas-N. Este campo puede contener cualquier secuencia de bits, con la única restricción de que el número de bits sea igual a un múltiplo entero de 8. La longitud del campo de información es variable y siempre será menor que un valor máximo predefinido.

Campo para la secuencia de comprobación de la trama

La secuencia de comprobación de la trama (FCS, Frame Check Sequence) es un código para la detección de errores calculado a partir de los bits de la trama excluyendo los delimitadores. El código que se usa normalmente es el CRC-CCITT de 16 bits definido en la Sección 7.2. Se puede utilizar alternativamente una FCS de 32 bits, que use el polinomio CRC-32, si así lo aconseja la longitud de la trama o las características de la línea.

FUNCIONAMIENTO

El funcionamiento del HDLC consiste en el intercambio de tramas-I, tramas-S y tramas-N entre dos estaciones. En la Tabla 7.1 se definen las órdenes y respuestas posibles para los distintos tipos de tramas. Al describir el funcionamiento del HDLC se explicarán a su vez estos tres tipos de tramas.

Tabla 7.1. Órdenes y respuestas del protocolo HDLC.

Nombre	Órdenes/ respuestas	Descripción
Información (I)	C/R	Intercambio de datos de usuario
Supervisión (S)		
Receptor preparado (RR)	C/R	Confirmación positiva; preparado para recibir tramas I
Receptor no preparado (RNR)	C/R	Confirmación positiva; no preparado para recibir
Rechazo (REJ)	C/R	Confirmación negativa; adelante-atrás-N
Rechazo selectivo (SREJ)	C/R	Confirmación negativa; rechazo selectivo
No numerada (N)		
Fijar el modo de respuesta normal/extendido (SNRM/SNRME)	C	Fija el modo; extendido = números de secuencia de 7 bits
Fijar el modo de respuesta asíncrono/extendido (SARM/SARME)	C	Fija el modo; extendido = números de secuencia de 7 bits
Fijar el modo balanceado asíncrono/extendido (SABM/SABME)	C	Fija el modo; extendido = números de secuencia de 7 bits
Fijar el modo de iniciación (SIM)	C	Inicia las funciones de control del enlace en la estación direccionada
Desconectar (DISC)	C	Finaliza la conexión lógica del enlace
Confirmación no numerada (UA)	R	Confirma la aceptación de una de las órdenes para fijar el modo
Modo desconectado (DM)	R	Finaliza la conexión lógica del enlace
Solicitud de desconexión (RD)	R	Solicitud de una orden DISC
Solicitud de modo de iniciación (RIM)	R	Se necesita iniciación; solicitud de la orden SIM
Información no numerada (UI)	C/R	Se utiliza para intercambiar información de control
Sondeo no numerado (UP)	C	Se utiliza para intercambiar información de control
Reset (RSET)	C	Se utiliza para las recuperaciones; pone N(R) y N(S) a sus valores iniciales
Intercambio de identificación (XID)	C/R	Se utiliza para solicitar o informar sobre el estado
Test (TEST)	C/R	Intercambio de campos idénticos de información para test
Rechazo de trama (FRMR)	R	Informa sobre la recepción de una trama inaceptable

El funcionamiento del HDLC implica tres fases. Primero, uno de los dos extremos inicia el enlace de datos, de tal manera que las tramas se puedan intercambiar de una forma ordenada. Durante esta fase, se pactan las opciones que se usarán en el intercambio posterior. Después de la iniciación, los dos extremos intercambian los datos generados por los usuarios así como información de control para llevar a cabo los procedimientos de control del flujo y de errores. Finalmente, uno de los dos extremos comunicará la finalización de la transmisión.

Iniciación

La iniciación la puede solicitar cualquiera de los dos extremos transmitiendo una de entre las seis órdenes previstas para fijar el modo. Esta orden sirve para tres objetivos:

1. Se avisa al otro extremo sobre la solicitud de la iniciación.
2. Se especifica cuál de los tres modos (NRM, ABM, ARM) se está solicitando.
3. Se especifica si se van a utilizar números de secuencia de 3 o 7 bits.

Si el otro es extremo acepta la solicitud, se informará al extremo sobre esta contingencia mediante la transmisión de una trama de confirmación no numerada (UA, unnumbered acknowledged). Si la solicitud se rechaza, se envía una trama de modo desconectado (DM, disconnected mode).

Transferencia de datos

Cuando la iniciación se haya solicitado y hay sido aceptada, entonces se habrá establecido la conexión lógica. A partir de entonces, ambos lados pueden comenzar a enviar datos mediante tramas-I, comenzando con el número de secuencia igual a 0. Los campos N(S) y N(R) de una trama-I contendrán los números de secuencia con los que se lleva a cabo el control del flujo y de errores. La secuencia de tramas-I se numerará secuencialmente módulo 8 o módulo 128, dependiendo de si se utilizan respectivamente 3 o 7 bits, utilizando el campo N(S). El campo N(R) se utiliza para la confirmación de las tramas-I recibidas; de esta forma se facilita que el módulo HDLC indique al otro extremo el número de trama-I que se espera recibir.

Las tramas-S también se usan para controlar el flujo y los errores. La trama receptor preparado (RR, receive ready) confirma una trama-I recibida, indicando a la vez la siguiente trama-I que se espera recibir. La RR se usa cuando no hay tráfico en el sentido contrario (tramas-I) en el que se puedan incluir las confirmaciones. La trama receptor no preparado (RNR, receive not ready) confirma una trama-I, como la hace la RR, pero a la vez solicita a la entidad situada al otro extremo del enlace que suspenda la transmisión de tramas-I. Cuando la entidad que envió la RNR esté de nuevo preparada, enviará una RR. La trama REJ sirve para iniciar el procedimiento ARQ con vuelta-atrás-N. Con ella se indica que la última trama-I recibida se ha rechazado y solicita la retransmisión de todas las tramas-I con números de secuencia posteriores a la N(R). La trama de rechazo selectivo (SREJ, selective reject) se usa para solicitar la retransmisión de una única trama.

Desconexión

Cualquiera de las dos entidades situadas a ambos lados del enlace pueden iniciar la desconexión; tanto por iniciativa propia (si es que ha habido algún tipo de fallo) como tras la petición cursada por capas superiores. HDLC lleva a cabo la desconexión transmitiendo una trama de desconexión (DISC, disconnect). El otro extremo podrá aceptar dicha desconexión devolviendo una trama UA e informando al usuario de la capa 3 sobre el cierre de la conexión. Se puede perder cualquier trama-I pendiente de confirmarse, en ese caso su recuperación es responsabilidad de las capas superiores.

Ejemplos de funcionamiento

Para comprender mejor el funcionamiento del HDLC, en la Figura 7.12 se presentan varios ejemplos. En los diagramas utilizados, cada fila incluye un texto que especifica el nombre de la trama, el bit P/F, y, allí donde sea oportuno, los valores de los campos N(R) y N(S). El bit P/F se considera que se pone a 1 si explícitamente aparece y en caso contrario se considera que se fija a 0.

En la Figura 7.12a se muestran las tramas involucradas en el establecimiento y desconexión del enlace. Una de las entidades enviará una orden SABM e iniciará un temporizador. El otro extremo, tras recibir la SABM, devolverá una respuesta UA, iniciará las variables locales y los contadores correspon-

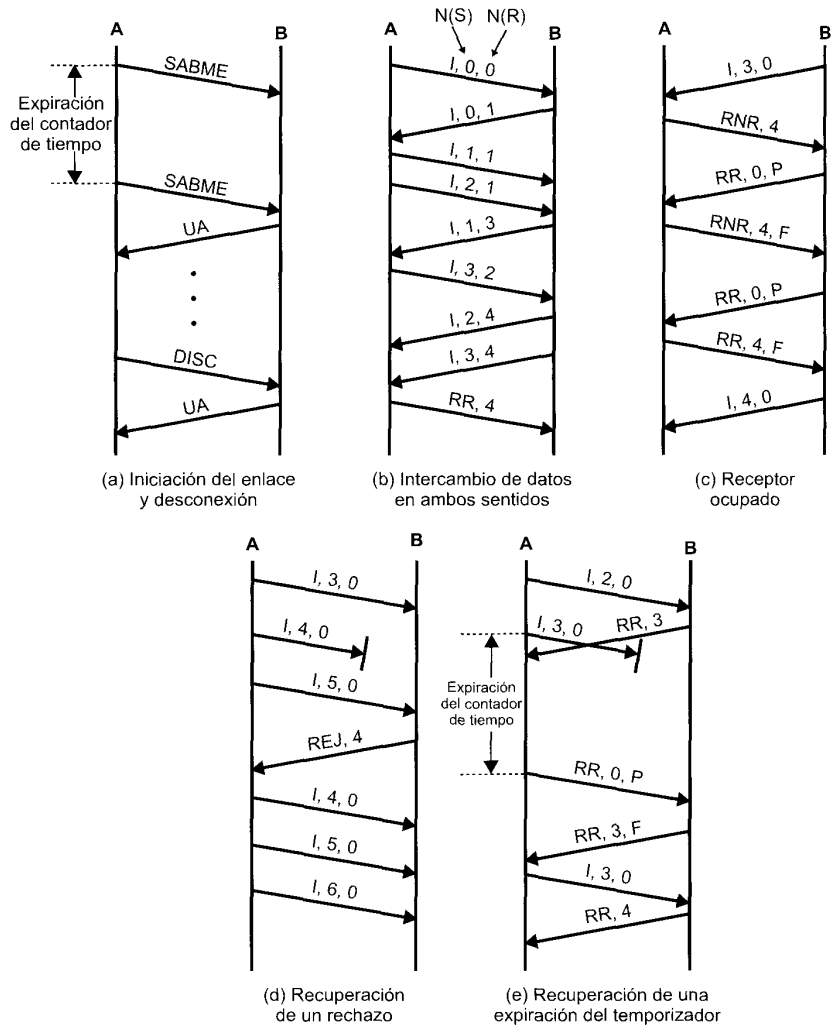


Figura 7.12. Ejemplo de funcionamiento de HDLC.

dientes. La entidad que inició el enlace recibe la respuesta UA, inicia sus variables y contadores, y detiene el temporizador. La conexión lógica ya está establecida, por lo que ambos extremos pueden comenzar a enviar tramas. Si el temporizador anterior expirara sin obtener la respuesta esperada, el extremo correspondiente repetirá la transmisión de la trama SABM, como se ha mencionado. Este procedimiento se debe repetir hasta que se reciba una trama UA, una trama DM o hasta que, tras una serie de intentos, la entidad que esté intentando establecer la conexión renuncie a sus pretensiones e informe sobre la condición de fallo a la entidad de gestión. En tal caso, se necesitará la intervención de las capas superiores. En la misma figura (Figura 7.12a) se muestra el procedimiento de desconexión. Uno de los dos extremos enviará una orden DISC, y el otro responderá con una trama UA.

En la Figura 7.12b se muestra el intercambio de tramas-I. Cuando una de las entidades envíe una serie de tramas-I consecutivas sin que se reciban tramas de datos, el número de secuencia recibida N(R)

se repetirá en todas ellas (por ejemplo, I,1,1; I,2,1 en el sentido de A a B). Cuando una entidad reciba una serie de tramas-I contiguas sin que entre tanto se envíe ninguna trama-I, en ese caso, el número de secuencia recibida de la siguiente trama que se envíe reflejará toda esta actividad acumulada (por ejemplo, I,1,3 en el sentido de B hacia A). Obsérvese que además de las tramas-I, el intercambio de datos puede implicar la utilización de tramas de supervisión.

En la Figura 7.12c se muestra el funcionamiento para el caso en el que el receptor esté ocupado. Tal situación se presentará cuando la entidad HDLC no sea capaz de procesar las tramas-I a la velocidad recibida, o cuando el usuario no sea capaz de aceptar datos tan rápidamente. En ambos casos, la memoria temporal de la entidad receptora se desbordará, por lo que se debe detener de alguna manera la recepción de tramas-I, esto se realiza transmitiendo una orden RNR. En el ejemplo, A envía una trama RNR, con la que solicita a B que detenga la transmisión de tramas-I. La estación que reciba la RNR normalmente sondeará periódicamente a la estación ocupada enviando tramas RR con el bit P igual a 1. Esto exige que el otro extremo responda con una RR o con una RNR. Cuando la situación de ocupado cesa, A devolverá una trama RR, con lo que la transmisión de tramas-I hacia B se podrá reanudar.

En la Figura 7.12b se muestra un ejemplo de cómo recuperar errores mediante el uso de la orden REJ. En este ejemplo, A transmitirá tramas-I numeradas con 3, 4 y 5. La número 4 sufre un error y se pierde. Cuando B recibe la trama-I número 5 la descartará debido a que su número no corresponde con lo esperado, y enviará una trama REJ con el campo N(R) igual a 4. Esto hará que A retransmita todas las tramas-I enviadas a partir de la 4, pudiendo continuar la transmisión de tramas adicionales tras haber retransmitido las anteriores.

En la Figura 7.12e se muestra un ejemplo de cómo recuperar un error usando los temporizadores. En este ejemplo, A transmite la trama-I número 3 tras haber enviado una secuencia de tramas previas. Dicha trama sufre un error. B detecta el error y descarta la trama. Sin embargo, B no puede enviar una REJ. Esto se debe a que no hay forma de saber si se trataba de una trama-I. Si se detecta un error en la trama, todos los bits son sospechosos de ser erróneos, por tanto el receptor no sabrá qué hacer. A, sin embargo, inició un temporizador al transmitir dicha trama. Este temporizador tendrá una duración suficiente ajustada al tiempo esperado de respuesta. Si el temporizador expira, A empezará con el procedimiento de recuperación, que se realiza sondeando al otro extremo mediante una orden RR con el bit P fijado a 1, de esta forma se pretende determinar el estado del otro extremo. Ya que el sondeo exige una respuesta, la entidad recibirá una trama conteniendo el campo N(R), con lo que podrá obrar en consecuencia. En el ejemplo considerado, la respuesta indicará que la trama 3 se ha perdido, con lo que A la retransmitirá.

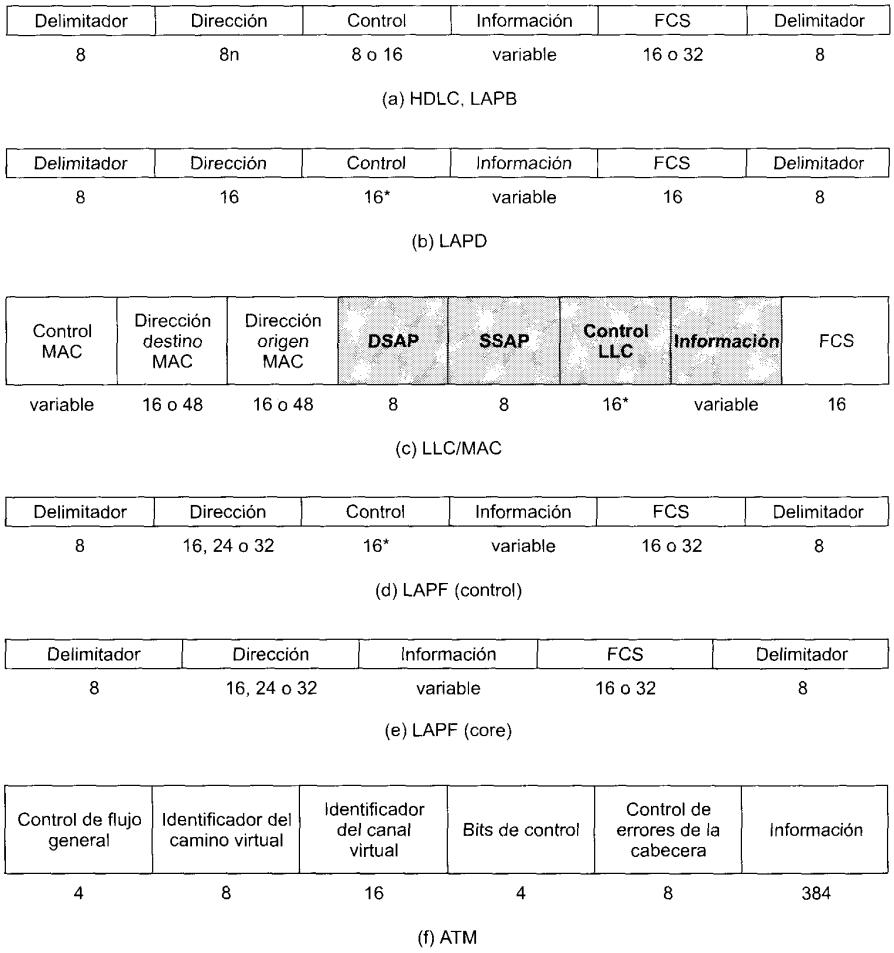
Estos ejemplos no constituyen una lista exhaustiva de todas las posibilidades. No obstante, pueden ser ilustrativos sobre el funcionamiento del HDLC.

7.5. OTROS PROTOCOLOS PARA EL CONTROL DEL ENLACE DE DATOS

Además del HDLC, hay una serie de otros protocolos relevantes para el control del enlace de datos. En la Figura 7.13 se muestran los formatos de las tramas, y a continuación se resumen brevemente.

LAPB

El procedimiento de acceso al enlace balanceado (LAPB, Link Access Procedure, Balanced) se desarrolló por la UIT-T como una parte de la norma X.25 para la interfaz a redes de conmutación de paquetes. Es un subconjunto del HDLC que proporciona solamente el modo balanceado asíncrono (ABM); se diseñó para enlaces punto a punto entre el sistema del usuario y un nodo de una red de conmutación de paquetes. El formato de las tramas es igual que el de HDLC.



* = campo de control de 16 bits (números de secuencia de 7 bits) para tramas I y S, 8 bits para tramas N.

Figura 7.13. Formatos de trama para el control del enlace de datos.

LAPD

El procedimiento de acceso al enlace sobre canal D (LAPD, Link Access Procedure, D-channel) se desarrolló por la UIT-T como parte de las recomendaciones para la RDSI (red digital de servicios integrados). LAPD proporciona el procedimiento para el control del enlace de datos sobre canal D, que es el canal lógico en la interfaz entre el usuario y la RDSI.

Hay varias diferencias entre LAPD y HDLC. Al igual que LAPB, LAPD se restringe al ABM. LAPD siempre usa números de secuencia de 7 bits, estando los de 3 bits prohibidos. La FCS para LAPD es siempre el CRC de 16 bits. Por último, el campo de dirección en LAPD tiene 16 bits y está formado por dos subdirecciones que identifican respectivamente al dispositivo y al usuario lógico del LAPD, ambos situados en el lado de la interfaz correspondiente al usuario.

CONTROL DEL ENLACE LÓGICO (LLC, LOGICAL LINK CONTROL)

El LLC es parte de la familia de estándares IEEE 802 para el control el funcionamiento en redes de área local (LAN, local area network). En LLC no se usan todas las características del HDLC y a la vez tiene algunas adicionales que no están en el anterior.

La diferencia más evidente entre LLC y HDLC está en el formato de las tramas. En LLC las funciones para controlar el enlace se dividen en dos capas: la capa de control de acceso al medio (MAC, medium access control), y la capa LLC que funciona por encima de la capa MAC.

En la Figura 7.13c se muestra la estructura de la trama que combina MAC y LLC; la parte sombreada corresponde con los campos generados en la capa LLC, y los no sombreados corresponden con la cabecera y la cola de la trama MAC. La capa MAC incluye las direcciones del origen y del destino para identificar a los dispositivos conectados en la LAN. Estas dos direcciones son necesarias ya que en el entorno LAN no existe el concepto de estación primaria o secundaria. Por tanto, el emisor y el receptor deben ser identificados. La detección de errores se realiza en el nivel MAC, utilizando un CRC de 32 bits. Finalmente, hay algunas funciones de control peculiares del control del acceso al medio que se deben incluir en el campo de control MAC.

En la capa LLC hay cuatro campos. Los puntos de acceso al servicio del destino y del origen (DSAP y SSAP, destination/source service access point), identifican al usuario lógico del LLC en los sistemas origen y destino. El campo de control del LLC tiene el mismo formato que el HDLC, pero limitado a la utilización de números de secuencia de 7 bits.

Funcionalmente, LLC ofrece tres tipos de servicios. El servicio con modo de conexión es el mismo que el ABM de HDLC. Los otros dos, sin conexión confirmado y sin conexión confirmado, se explicarán en la Parte Cuarta.

RETRANSMISIÓN DE TRAMAS (FRAME RELAY)

La retransmisión de tramas es una utilidad para el control del enlace de datos diseñada para proporcionar una utilización más eficiente de la capacidad de las redes de alta velocidad de conmutación de paquetes. Se utiliza en lugar de X.25, consistente en el protocolo LAPB y un protocolo de la capa de red (denominada capa de paquetes X.25). La retransmisión de tramas se considerará con más detalle en la Parte Tercera.

El protocolo para el control del enlace de datos definido en la retransmisión de tramas es el LAPF («link access procedure for frame-mode bearer service»). En realidad hay dos protocolos: un *protocolo de control*, de similares características al HDLC y un *protocolo básico*, que es un subconjunto del protocolo de control.

Hay varias diferencias esenciales entre el LAPF y el HDLC. Al igual que en LAPB, el control LAPF se restringe a ABM. LAPF utiliza siempre números de secuencia de 7 bits; los números de 3 bits no están permitidos. La FCS para el control LAPF siempre es un CRC de 16 bits. Por último, el campo de direcciones en el LAPF tiene una longitud de dos, tres o cuatro, y contiene al identificador de la conexión del enlace de datos (DLCI, data link connection identifier) de 10, 16 o 23 bits. El DLCI identifica a la conexión lógica entre el sistema origen y el destino. Además el campo de dirección contiene algunos bits de control que son útiles para controlar el flujo.

El protocolo LAPF básico tiene el mismo campo de delimitación, dirección, información y FCS que el protocolo LAPF de control. La diferencia estriba en que no hay campo de control en el LAPF básico. Por tanto, no hay forma de realizar control de flujo ni de errores, consiguiendo así un funcionamiento más eficiente.

MODO DE TRANSFERENCIA ASÍNCRONO (ATM, ASYNCHRONOUS TRANSFER MODE)

Al igual que la retransmisión de tramas, ATM se ha diseñado para proporcionar un procedimiento de transferencia de datos muy eficiente para su utilización en redes de alta velocidad. A diferencia de la

retransmisión de tramas, ATM no está basado en HDLC. En su lugar, ATM está basado en unas tramas con formato radicalmente diferente, llamadas celdas, con las que se reduce el procesamiento adicional necesario.

Cada celda tiene una longitud fija de 53 octetos, es decir 424 bits. En la Parte Tercera de este libro se estudiarán con detalle los distintos campos de las celdas ATM.

7.6. LECTURAS RECOMENDADAS

[BERT92] presenta un tratamiento excelente y muy detallado sobre el control de errores y del flujo. [BLAC93] proporciona una revisión acertada de los protocolos para el control del enlace de datos. [FIOR95] trata algunos de los problemas relacionados con la fiabilidad del HDLC en entornos reales.

BERT92 Bertsekas, D., y Gallager, R. *Data Networks*. Englewood Cliffs, NJ: Prentice Hall, 1992.

BLAC93 Black, U. *Data Link Protocols*. Englewood Cliffs, NJ: Prentice Hall, 1993.

FIOR95 Fiorini, D.; Chiani, M.; Tralli, V.; y Salati, C. «Can We Trust HDLC?». *Computer Communications Review*, October 1995.

7.7. PROBLEMAS

7.1. Considérese un enlace punto a punto semi-duplex en el que se utiliza un esquema de parada-y-espera, en este enlace se envía una serie de mensajes, cada uno de los cuales se segmenta en una serie de tramas. Si no se consideran errores y los bits suplementarios en las tramas:

a) ¿Qué repercusiones tiene en la utilización de la línea un aumento del tamaño de los mensajes de forma que se necesite transmitir un menor número de ellos? Todos los otros factores se mantienen constantes.

b) ¿Qué repercusión tendría en la utilización de la línea aumentar el número de tramas manteniendo constante el tamaño del mensaje?

c) ¿Qué repercusión tendría en la utilización de la línea aumentar el tamaño de las tramas?

7.2. Un canal tiene una velocidad de transmisión de 4 kbps y un retardo de propagación de 20 ms. ¿Para qué rango de tamaños de las tramas se conseguirá un esquema con parada-y-espera con una eficiencia de al menos el 50 %?

7.3. Supóngase que se están utilizando tramas de 1.000 bits en un canal vía satélite a 1Mbps con 270 ms de retardo. ¿Cuál es la utilización máxima de la línea para

a) un control del flujo mediante parada-y-espera?

b) un control del flujo continuo con un tamaño de ventana igual a 7?

c) un control del flujo continuo con un tamaño de ventana igual a 127?

d) un control del flujo continuo con un tamaño de ventana igual a 255?

7.4. En la Figura 7.14 en el nodo A se generan tramas que se envían al nodo C a través del nodo B. Determinar la velocidad de transmisión mínima entre los nodos B y C de tal manera que la memoria temporal del nodo B no se sature, teniendo en cuenta que:

- La velocidad de transmisión entre A y B es 100 kbps.
- El retardo de propagación es 5 μs/km para ambas líneas.

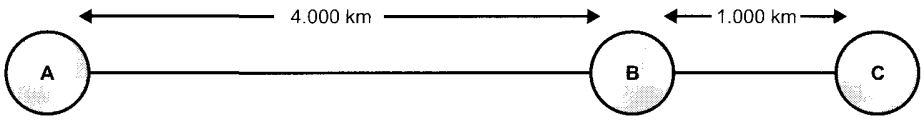


Figura 7.14. Configuración para el Problema 7.4.

- Haya líneas full-duplex entre los nodos.
- Todas las tramas de datos tienen 1.000 bits; las tramas ACK son independientes y de longitud despreciable.
- Se usa entre A y B un protocolo de ventana deslizante de tamaño 3.
- Entre B y C se usa un protocolo de parada-y-espera.
- No hay errores.

Sugerencia: Para no saturar la memoria temporal de B, el número medio de tramas entrantes debe ser igual al número medio de tramas salientes, durante un intervalo grande.

7.5. Un canal tiene una velocidad de transmisión de R bps y un retardo de propagación de t segundos por kilometro. La distancia entre el nodo emisor y el receptor es de L kilómetros. Los nodos intercambian tramas de longitud fija igual a B bits. Encontrar la expresión que dé el tamaño del campo de numeración de secuencia mínimo en función de R, t, B y L (considerando utilización máxima). Suponer que las tramas CONF tienen un tamaño despreciable y el procesamiento en los nodos es instantáneo.

7.6. ¿La inclusión de un bit de paridad en cada carácter modificará la probabilidad de recibir correctamente un mensaje?

7.7. ¿Por qué se utiliza aritmética en módulo 2 en lugar de usar aritmética binaria al calcular la FCS?

7.8. Considérese una trama formada por dos caracteres de cuatro bit cada uno. Supóngase que la probabilidad de error en un bit es 10^{-3}, siendo ésta independiente para cada bit.

a) ¿Cuál es la probabilidad de recibir la trama con al menos un error?

b) Ahora añádase un bit de paridad a cada carácter. ¿Cuál es la probabilidad en este caso?

7.9. Usando un polinomio CRC-CCITT, obtener el código CRC de 16 bits para un mensaje formado por un 1 seguido de 15 ceros:

a) Utilice una división.

b) Utilice un registro de desplazamiento como el de la Figura 7.6.

7.10. Explicar cualitativamente por qué un CRC con un registro de desplazamiento dará una cadena de todo ceros si no hay errores. Demuéstrese con un ejemplo.

7.11. Encontrar el CRC para $P = 110011$ y $M = 11100011$.

7.12. Un CRC se construye para generar una FCS de 4 bits para mensajes de 11 bits. El polinomio generador es $X^4 + X^3 + 1$.

a) Dibujar el circuito correspondiente a la realización con un registro de desplazamiento para el código (véase Figura 7.6).

b) Codificar la secuencia de bits 10011011100 (siendo el bit menos significativo el situado a la izquierda) mediante el polinomio generador y obtener la palabra código.

c) Supóngase que el bit 7 (contando desde el bit menos significativo) en la palabra código tiene error, mostrar cómo el algoritmo de detección detectaría este error.

7.13. Frecuentemente en los estándares de comunicación se usa un procedimiento CRC modificado. Definido por:

$$\frac{X^{16}M(X) + X^k L(X)}{P(X)} = Q + \frac{R(X)}{P(X)}$$

$$FCS = L(X) + R(X)$$

donde

$$L(X) = X^{15} + X^{14} + X^{13} + \cdots + X + 1$$

siendo k el número de bits comprobados (dirección, control, y campos de información).

a) Describir cualitativamente el efecto de este procedimiento.

b) Explicar las ventajas potenciales.

c) Mostrar la implementación mediante un registro de desplazamiento para $P(X) = X^{16} + X^{12} + X^5 + 1$.

7.14. En el estudio del ARQ con parada-y-espera no se ha hecho mención a las tramas de rechazo REJ0 y REJ1. ¿Por qué no es necesario utilizar REJ0 y REJ1 en un ARQ con parada-y-espera?

7.15. Supóngase que se usa un ARQ con rechazo selectivo con $N = 4$. Muéstrese, mediante un ejemplo, que se necesitará una secuencia de numeración de 3 bits.

7.16. Considerando las mismas suposiciones que las adoptadas en la Figura 7.17 del Apéndice 7A, represente la utilización de la línea en función de P, la probabilidad de que una única trama sea errónea para los siguientes procedimientos de control del flujo:

a) Parada-y-espera.

b) Vuelta-atrás-N con $N = 7$.

c) Vuelta-atrás-N con $N = 127$.

d) Rechazo selectivo con $N = 7$.

e) Rechazo selectivo con $N = 127$.

Considérense los siguientes valores para a: 0,1, 1, 10, 100. Obtenga las conclusiones pertinentes sobre qué técnica es la más adecuada para los distintos valores de a.

7.17. Dos nodos vecinos (A y B) usan un protocolo con ventana deslizante con 3 bits para los números de secuencia. Se utiliza como procedimiento ARQ un vuelta-atrás-N con un tamaño de ventana igual a 4. Supóngase que A transmite y B recibe, mostrar las distintas posiciones de las ventanas para la siguiente sucesión de eventos:

a) Antes de que A envíe ninguna trama.

b) Después de que A envíe las tramas 0, 1, 2, y B confirme 0 y 1 y las ACK se hayan recibido en A.

c) Después de que A envíe las tramas 3, 4, y 5 y B confirma 4 y la ACK 4 se recibe en A.

7.18. En ARQ con rechazo selectivo no se pueden usar confirmaciones desordenadas. Es decir, si la estación X rechaza la trama i, todas las tramas-I y RR siguientes enviadas por X deben tener N(R) = i hasta que la trama i se reciba correctamente, incluso en el caso de que otras tramas con N(S) > i se reciban entre tanto sin errores. Un posible refinamiento es el siguiente: una trama-I o

una RR con N(R) = j se interpretarán como que la trama $j - 1$ y todas las precedentes se han aceptado excepto aquellas que explícitamente se hayan rechazado mediante una trama SREJ. Discutir los posibles problemas que puede plantear este procedimiento.

7.19. El estándar ISO para los procedimientos DLC (ISO 4335) incluye las siguientes definiciones: (1) la situación tras una REJ se considera finalizada cuando se reciba una trama-I con N(S) igual al N(R) de la trama REJ de salida; y (2) la situación tras una SREJ se considera finalizada cuando se reciba una trama-I con N(S) igual al N(R) de la trama SREJ. Estas reglas indican qué ocurre (en términos de transmitir tramas REJ y SREJ) si la situación tras recibir una REJ no ha finalizado y qué ocurre si la situación tras la transmisión de una SREJ no ha finalizado. Deduzca las reglas justificando la respuesta.

7.20. Dos estaciones se comunican vía satélite a 1 Mbps con un retardo de propagación de 270 ms. El satélite lo que hace únicamente es retransmitir los datos recibidos de una estación a otra, con un retardo de conmutación despreciable. Si se usan las tramas HDLC de 1.024 bits con números de secuencia de 3 bits, ¿cuál es el rendimiento máximo posible? Es decir, ¿cuál es el rendimiento para los bits de datos transportados en las tramas HDLC?

7.21. Es evidente que en una trama HDLC la inserción de bits se necesita en los campos de dirección, datos y en la FCS. ¿Es necesaria en el campo de control?

7.22. Proponga posibles mejoras al algoritmo de inserción de bits para evitar los problemas existentes cuando hay un error en un bit.

7.23. Usando el ejemplo de la Figura 7.11, obtener la señal correspondiente a una codificación NRZ-L. ¿Sugiere lo anterior alguna ventaja para la inserción de bits?

7.24. Suponer que una estación primaria en HDLC en NRM envía seis tramas-I a una secundaria. El N(S) de la primaria es tres (011 en binario) antes de enviar las seis tramas. Si el bit P está a ON en la sexta trama, ¿cuál será el N(R) de vuelta de la secundaria tras la última trama? Supóngase que no hay errores.

7.25. Supóngase que se disponen de varios enlaces para conectar dos estaciones. Se utiliza un «HDLC multienlace» con el que se hace un uso eficiente de estos enlaces enviando las tramas con una estrategia FIFO (first in first out) utilizando el siguiente enlace que quede libre. ¿Qué modificaciones serían necesarias en el HDLC para esta situación?

7.26. Un servidor WWW (World Wide Web) está diseñado para recibir mensajes relativamente pequeños generados por sus clientes y para transmitir hacia éstos, mensajes muy largos. Explíquese qué tipo de protocolo ARQ (rechazo selectivo o vuelta-atrás-N) utilizaría para un servidor WWW.

APÉNDICE 7A. ANÁLISIS DE PRESTACIONES

En este apéndice se realizará una análisis de las prestaciones de los protocolos para el control del flujo con ventana deslizante.

CONTROL DEL FLUJO CON PARADA-Y-ESPERA

Calculemos la eficiencia máxima potencial en una línea punto a punto semi-duplex usando el esquema parada-y-espera descrito en la Sección 7.1. Supóngase que se va a enviar un mensaje largo en una serie de tramas F_1, F_2, ..., F_n, de la siguiente manera:

- La estación S_1 envía F_1.
- La estación S_2 envía una confirmación.
- La estación S_1 envía F_2.
- La estación S_2 envía una confirmación.

  .
  .
  .

- La estación S_1 envía F_n.
- La estación S_2 envía una confirmación.

El tiempo total para enviar los datos, T, se puede expresar como $T = nT_F$, donde T_f es el tiempo en enviar una trama y recibir la confirmación. T_f se puede expresar de la siguiente manera:

$$T_F = t_{prop} + t_{trama} + t_{proc} + t_{prop} + t_{conf} + t_{proc}$$

donde

t_{prop} = tiempo de propagación de S_1 a S_2.

t_{trama} = tiempo en transmitir una trama (tiempo para que el transmisor envíe todos los bits de la trama).

t_{conf} = tiempo de procesamiento para que cada estación reaccione a un evento de entrada.

t_{proc} = tiempo en transmitir una confirmación.

Supóngase que el tiempo de procesamiento es despreciable en términos relativos, y que la trama de confirmación es muy pequeña comparada con la trama de datos, ambas suposiciones son razonables. Por tanto, el tiempo total para enviar datos se puede expresar como:

$$T = n(2t_{prop} + t_{trama})$$

De ese tiempo, realmente sólo se emplea $n \times t_{trama}$ en transmitir datos y el resto es suplementario. La utilización, o eficiencia, de la línea es:

$$U = \frac{n \times t_{trama}}{n(2t_{prop} + t_{trama})} = \frac{t_{trama}}{2t_{prop} + t_{trama}} \tag{7.1}$$

Es útil definir el parámetro $a = t_{prop}/t_{trama}$ (véase Figura 7.2). Entonces

$$U = \frac{1}{1 + 2a} \tag{7.2}$$

Ésta es la máxima utilización posible de la línea. Debido a que la trama contiene bits suplementarios, la utilización real es inferior. El parámetro a será constante si tanto t_{prop} como t_{trama} lo son, lo cual es la situación más habitual: en un enlace punto a punto, normalmente se utilizarán tramas con longitud fija, excepto la última trama de la secuencia, y el retardo de propagación será constante.

Para clarificar un poco más la Ecuación (7.2), consideremos una expresión diferente para el parámetro a. Sea

$$a = \frac{\textit{Tiempo de propagación}}{\textit{Tiempo de transmisión}} \tag{7.3}$$

El tiempo de propagación es igual a la distancia d del enlace dividida por la velocidad de propagación V. Para transmisión no guiada a través del aire o el espacio, V es la velocidad de la luz, aproximadamente igual a 3×10^8 m/seg. Para transmisión guiada (fibra óptica y cable de cobre), V es aproximada-

mente igual a 0,67 veces la velocidad de la luz. El tiempo de transmisión es igual a la longitud de la trama en bits, L, dividida por la velocidad de transmisión R. Por tanto,

$$a = \frac{d/V}{L/R} = \frac{Rd}{VL}$$

Luego, para tramas de longitud fija, a es proporcional a la velocidad de transmisión multiplicada por la longitud del medio. Una forma útil de considerar al parámetro a es que representa la longitud del medio en bits $\left(R \times \frac{d}{V}\right)$ en relación con la longitud de la trama (L).

Teniendo presente esta interpretación, en la Figura 7.2 se ilustra la Ecuación (7.2). En esta figura, el tiempo de transmisión se normaliza a la unidad y, por tanto, el tiempo de propagación, considerando la Ecuación (7.3), es a. Para el caso de $a < 1$, la longitud del enlace en bits es menor que la de la trama. La estación T empieza a transmitir la trama en el instante de tiempo t_0. En $t_0 + a$, el primer bit de la trama llega a la estación receptora R, mientras que T estará todavía transmitiendo la trama. En $t_0 + 1$, T concluye la transmisión. En $t_0 + 1 + a$, R habrá recibido la trama completa e inmediatamente después transmitirá una trama de confirmación pequeña. Esta confirmación vuelve a T en $t_0 + 1 + 2a$. El tiempo total transcurrido es $1 + 2a$. El tiempo total de transmisión es 1. Por tanto, la utilización es $1/(1 + 2a)$. El mismo resultado se puede conseguir con $a > 1$, tal y como se muestra en la Figura 7.2.

Consideremos a continuación una serie de ejemplos. Primero, sea una red de área amplia (WAN) utilizando ATM («asynchronous transfer mode», que se explicará en la Parte III), con dos estaciones separadas miles de kilómetros. El tamaño normalizado para la trama ATM (denominada celda) es 424 bits y una de las velocidades de transmisión normalizada es 155,52 Mbps. Por tanto el tiempo de transmisión es igual a $424/(155{,}52 \times 10^6) = 2{,}7 \times 10^{-6}$ segundos. Si se supone un enlace de fibra óptica, entonces el tiempo de propagación es $(10^6 \text{ metros})/(2 \times 10^8 \text{ m/seg}) = 0{,}5 \times 10^{-2}$ segundos. Por tanto, $a = (0{,}5 \times 10^{-2})/(2{,}7 \times 10^{-6}) \approx 1.850$, por lo que la eficiencia es sólo $1/3.701 = 0{,}00027$.

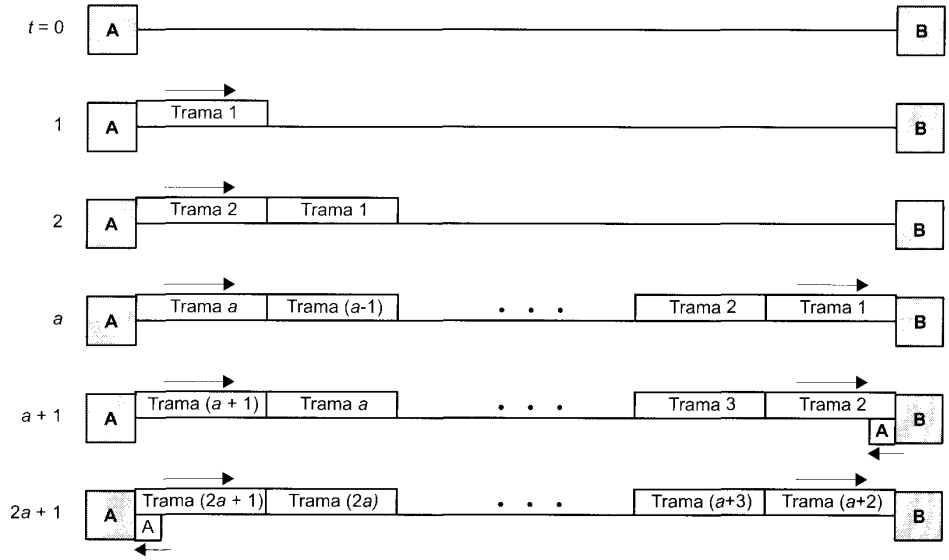
En términos de distancia, el otro caso extremo es el de las redes de área local (LAN). Las distancias aquí varían entre 0,1 y 10 km, con velocidades de transmisión comprendidas entre 10 Mbps y 1 Gbps; las velocidades superiores se tienden a asociar con las distancias más cortas. Usando un valor de $V = 2 \times 10^8$ m/seg, un tamaño de la trama de 1.000 bits, y una velocidad de transmisión igual a 10 Mbps, el valor de a estará en el rango que va desde 0,005 a 0,5. Esto implica una utilización comprendida entre 0,5 y 0,99. Para una LAN a 100 Mbps, considerando distancias más cortas, se puede obtener una utilización comparable.

Se puede observar que las LAN son normalmente bastante eficientes, mientras que las WAN de alta velocidad no. Como último ejemplo, considérese una transmisión de datos vía modem entre distancias incluso superiores, como por ejemplo $d = 5.000$ km, se tendrá que $a = (56.000 \times 5 \times 10^6)/(2 \times 10^8 \times 1.000 \text{ bits}) = 1{,}4$ y la eficiencia será igual a 0,26.

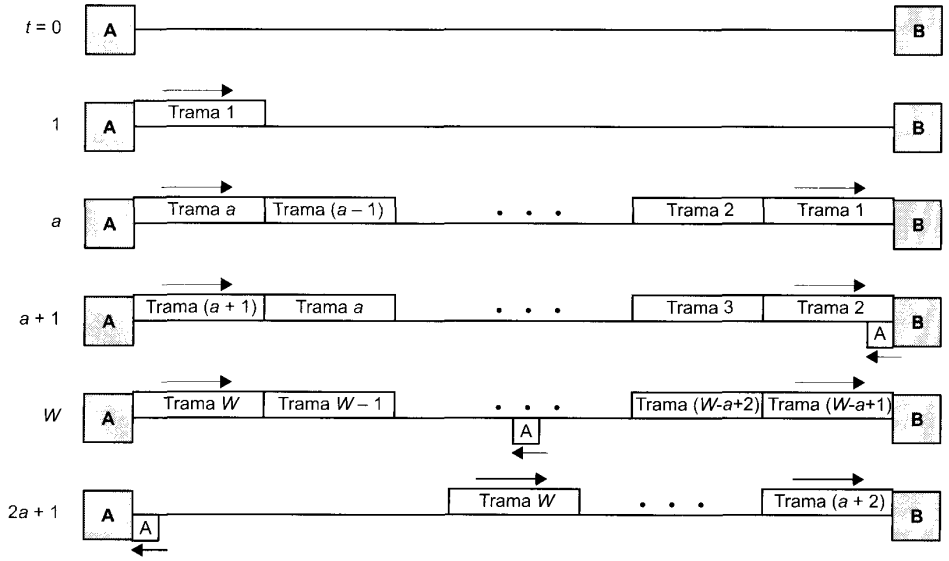
CONTROL DEL FLUJO CON VENTANA DESLIZANTE

En el control del flujo mediante ventanas deslizantes, la eficiencia de la línea depende de tanto el tamaño de la ventana W, como del valor de a. Por comodidad, normalizamos igualmente el tiempo de transmisión de la trama a la unidad; por tanto el tiempo de propagación es a. En la Figura 7.15 se muestra la eficiencia de una línea punto a punto full-duplex[3]. La estación A empieza a transmitir una serie de tramas en $t = 0$. El primer bit de la primera trama llega a la estación B en $t = a$. La primera trama se recibe completamente en $t = a + 1$. Suponiendo un tiempo de procesamiento despreciable, B confirmará inmediatamente la primera trama (ACK). Supóngase también que la trama de confirmación es tan

[3] Por sencillez se supone que a es un valor entero, de esta forma en la línea cabrán un número entero de tramas. La argumentación es igualmente válida para valores de a no enteros.



(a) $W \geq 2a + 1$



(b) $W < 2a + 1$

Figura 7.15. Temporización de un protocolo de ventana deslizante.

pequeña que el tiempo de transmisión es despreciable. Entonces ACK llega a A en $t = 2a + 1$. Para evaluar las prestaciones, se necesitan considerar dos casos:

- **Caso 1:** $W \geqslant 2a + 1$. La confirmación de la trama 1 llega a A antes de que A agote su ventana. Por tanto A puede transmitir continuamente sin pausa, por lo que la utilización será 1,0.

- **Caso 2:** $N < 2a + 1$. A agota su ventana en $t = W$ y no podrá enviar tramas adicionales hasta $t = 2a + 1$. Por tanto, la utilización de la línea es W unidades de tiempo por cada periodo de $(2a + 1)$ unidades de tiempo.

Por tanto se puede afirmar que:

$$\mathcal{U} = \begin{cases} 1 & W \geq 2a + 1 \\ \dfrac{W}{2a + 1} & W < 2a + 1 \end{cases} \tag{7.4}$$

Generalmente, el número de secuencia se da mediante un campo de n-bits y el tamaño máximo de la ventana es $W = 2^n - 1$ (no 2^n, como se explicó en la Sección 7.3). En la Figura 7.16 se muestra la máxima eficiencia que se puede conseguir para ventanas de tamaño 1, 7 y 127 en función de a. Una ventana de tamaño 1 corresponde con un parada-y-espera. Una ventana de tamaño igual a 7 (3 bits) es adecuada para muchas aplicaciones. Una ventana de tamaño 127 (7 bits) es adecuada para valores grandes de a, como los que se pueden encontrar en WAN de alta velocidad.

ARQ

Ya se ha comentado que el control del flujo con ventanas deslizantes es más eficiente que el control del flujo con parada-y-espera. Sería de esperar que si se incorporan procedimientos para el control de los errores esto seguiría siendo verdad; es decir, que ARQ con vuelta-atrás-N y con rechazo selectivo son más eficientes que el ARQ con parada-y-espera. Desarrollemos algunas expresiones para determinar el grado de mejora que se puede esperar.

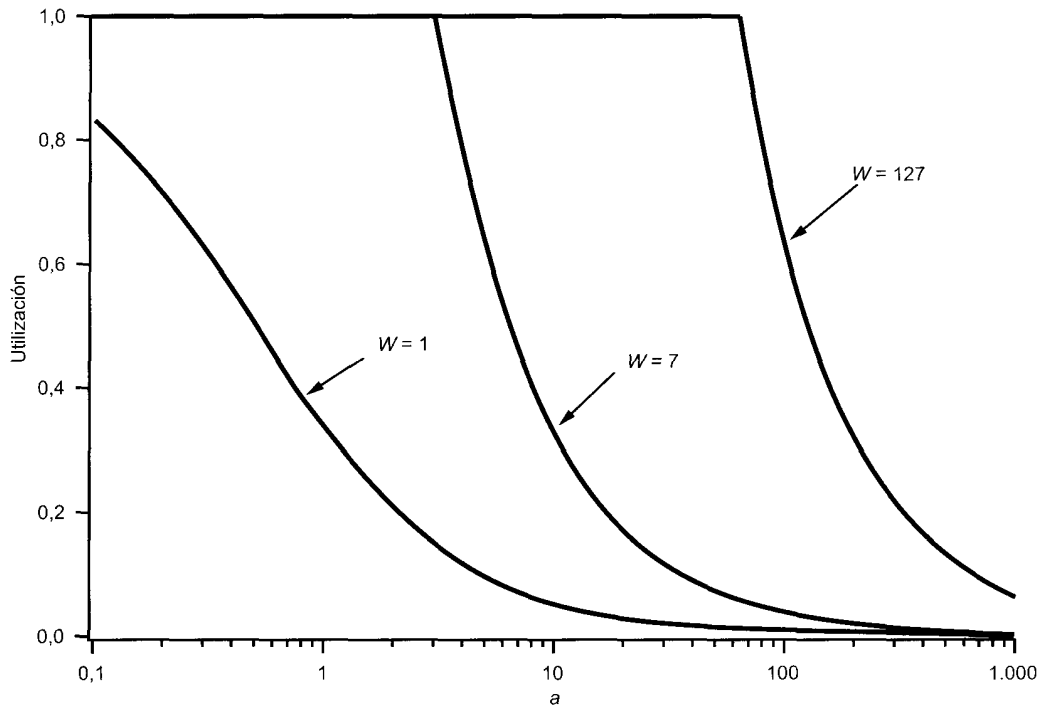


Figura 7.16. Utilización de la línea en función del tamaño de la ventana.

Primero, considérese un ARQ con parada-y-espera. Si no hay errores, la utilización máxima es $1/(1 + 2a)$ como se muestra en la Ecuación (7.2). Supóngase ahora que puede que haya algunas tramas repetidas debido a la aparición de errores. Para comenzar, obsérvese que la utilización, U, se puede definir como

$$U = \frac{T_f}{T_t} \tag{7.5}$$

donde

T_f = tiempo empleado en el transmisor para emitir una trama.

T_t = tiempo total durante el cual la línea está ocupada transmitiendo una única trama.

Para el caso sin errores usando ARQ con parada-y-espera:

$$U = \frac{T_f}{T_f + 2T_p}$$

donde T_p es el tiempo de propagación. Dividiendo por T_f y recordando que $a = T_p/T_f$, se obtiene de nuevo la Ecuación (7.2). Si hay errores, se debe modificar la Ecuación (7.5) de la siguiente manera

$$U = \frac{T_f}{N_r T_t}$$

donde N_r es el valor esperado del número de transmisiones para una trama. Por tanto, en ARQ con parada-y-espera, se tiene que:

$$U = \frac{1}{N_r(1 + 2a)}$$

donde N_r es el número esperado de transmisiones de una trama. Por tanto, para ARQ con parada-y-espera, se tiene que

$$U = \frac{1}{N_r(1 + 2a)}$$

Se puede obtener una expresión sencilla para N_r considerando la probabilidad P de que una única trama sea errónea. Si se supone que las ACK y las ACK negativas nunca tienen errores, la probabilidad de que se necesiten k intentos para transmitir una trama con éxito es $P^{(k-1)}(1 - P)$. Es decir, se tendrán $(k - 1)$ intentos infructuosos seguidos de un intento con éxito; la probabilidad de que esto ocurra es justo el producto de las probabilidades de los eventos individuales. Entonces[4]

$$N_r = \text{E[transmisiones]} = \sum_{i=1}^{\infty} (i \times \Pr[i \text{ transmisiones}])$$

$$= \sum_{i=1}^{\infty} (iP^{i-1}(1 - P)) = \frac{1}{1 - P}$$

Por tanto se tiene que

Parada-y-espera: $$U = \frac{1 - P}{1 + 2a}$$

[4] Para obtener esta expresión se usa la igualdad $\sum_{i=1}^{\infty} (iX^{i-1}) = \frac{1}{(1 - X^2)}$ para $(-1 < X < 1)$.

En el protocolo de ventana deslizante, la Ecuación (7.4) se aplica en el caso de que no haya errores. En el ARQ con rechazo selectivo, se puede utilizar el mismo razonamiento que el que se utilizó en ARQ con parada-y-espera. Es decir, las ecuaciones obtenidas para cuando no hay errores se deben dividir por N_r. Donde de nuevo $N^r = 1/(1 - P)$. Por tanto

$$\textbf{Rechazo selectivo:} \qquad \mathcal{U} = \begin{cases} 1 & W \geq 2a + 1 \\ \dfrac{W(1 - P)}{2a + 1} & W < 2a + 1 \end{cases}$$

El mismo razonamiento es trasladable a ARQ con vuelta-atrás-N, pero en este caso hay que ser más cuidadoso al aproximar N_r. Por cada error se necesitan retransmitir K tramas en lugar de sólo una como hasta ahora se había considerado. Por tanto

$$N_r = \text{E[Número de tramas transmitidas para transmitir una trama con éxito]}$$
$$= \sum_{i=1}^{\infty} f(i)P^{i-1}(1 - P)$$

donde $f(i)$ es el número total de tramas transmitidas si la trama original se debe transmitir i veces. Esto se expresa de la siguiente manera[5]

$$N_r = (1 - K) \sum_{i=1}^{\infty} P^{i-1}(1 - P) + K \sum_{i=1}^{\infty} (1 - P)$$
$$= 1 - K + \frac{K}{1 - P}$$
$$= \frac{1 - P + KP}{1 - P}$$

Estudiando la Figura 7.15, el lector podría concluir que K es aproximadamente igual a $(2a + 1)$ para $W \geq (2a + 1)$, y $K = W$ para $W < (2a + 1)$. Por tanto

$$\textbf{Adelante-atrás-N:} \qquad \mathcal{U} = \begin{cases} \dfrac{1 - P}{1 + 2aP} & W \geq 2a + 1 \\ \dfrac{W(1 - P)}{(2a + 1)(1 - P + WP)} & W < 2a + 1 \end{cases}$$

Obsérvese que para $W = 1$, el ARQ con rechazo selectivo y el ARQ vuelta-atrás-N se reducen al de parada-y-espera. En la Figura 7.17[6] se comparan las tres técnicas para el control de errores para un valor de $P = 10^{-3}$. Esta figura así como las ecuaciones son sólo aproximaciones. Por ejemplo, no se han considerado errores en las tramas de confirmación y, en el caso de vuelta-atrás-N, no se han tenido en cuenta la posibilidad de errores en las tramas retransmitidas. No obstante, los resultados mostrados dan una idea de las prestaciones relativas de las tres técnicas estudiadas.

---

[5] Para obtener esta expresión se usa la igualdad $\sum_{i=1}^{\infty} X^{i-1} = \dfrac{1}{1 - X}$ para $(-1 < X < 1)$.

[6] Para $W = 7$, las curvas para los esquemas vuelta-atrás-N y rechazo selectivo están tan próximas que en la figura aparecen como idénticas.

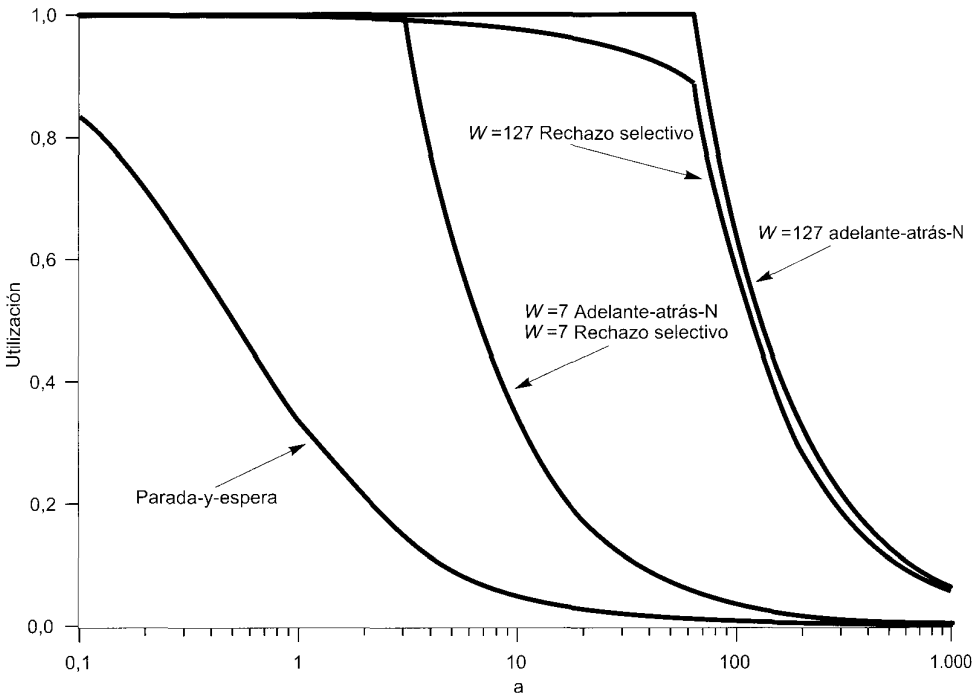


Figura 7.17. Utilización de la línea para varias técnicas de control de errores ($P = 10^{-3}$).

CAPÍTULO 8

Multiplexación

- Para hacer un uso eficiente de las líneas de telecomunicaciones de alta velocidad se emplean técnicas de multiplexación, las cuales permiten que varias fuentes de transmisión compartan una capacidad de transmisión superior. Las dos formas usuales son multiplexación por división en frecuencias (FDM, frecuency-division multiplexing) y multiplexación por división en el tiempo (TDM, time-division multiplexing).
- La multiplexación por división en frecuencias se puede usar con señales analógicas, de modo que se transmiten varias señales a través del mismo medio gracias a la asignación de una banda de frecuencia diferente para cada señal. El equipamiento de modulación es preciso para desplazar cada señal a la banda de frecuencia requerida, siendo por su parte necesarios los equipos de multiplexación para combinar las señales moduladas.
- La multiplexación por división en el tiempo síncrona se puede utilizar con señales digitales o con señales analógicas que transportan datos digitales. En esta forma de multiplexación, los datos procedentes de varias fuentes se transmiten en tramas repetitivas. Cada trama consta de un conjunto de ranuras temporales, asignándosele a cada fuente una o más ranuras por trama. El efecto obtenido es la mezcla de los bits de datos de varias fuentes.
- La multiplexación por división en el tiempo estadística proporciona un servicio generalmente más eficiente que la técnica TDM síncrona para el caso de soporte a terminales. Las ranuras temporales en TDM estadística no están preasignadas a fuentes de datos concretas, sino que los datos de usuario se almacenan y transmiten tan rápido como es posible haciendo uso de las ranuras temporales disponibles.

En el Capítulo 7 se llevó a cabo una descripción de técnicas eficientes para utilizar un enlace de datos en condiciones de alta carga. En particular, con dos dispositivos conectados mediante un enlace punto a punto es deseable por lo general emitir múltiples tramas de modo que el enlace no constituya un cuello de botella entre las estaciones. Considérese a continuación la situación contraria. Usualmente, dos estaciones de comunicaciones no hacen uso de la capacidad total de un enlace de datos; con objeto de mejorar la eficiencia sería posible compartir esta capacidad. Un concepto general para tal compartimiento es el de **multiplexación**.

Una aplicación usual de la multiplexación son las comunicaciones de larga distancia. Los enlaces de las redes de larga distancia son líneas de fibra, de cable coaxial o de microondas de alta capacidad, de modo que pueden transportar simultáneamente varias transmisiones de voz y de datos haciendo uso de las técnicas de multiplexación.

La Figura 8.1 muestra la función de multiplexación en su forma más simple. Existen n entradas a un multiplexor, que se conecta a un demultiplexor mediante un único enlace de datos. El enlace es capaz de transportar n canales de datos independientes. El multiplexor combina (multiplexa) los datos de las n líneas de entrada y los transmite a través de un enlace de datos de capacidad superior. El demultiplexor capta la secuencia de datos multiplexados, separa (demultiplexa) los datos de acuerdo con el canal y los envía hacia las líneas de salida correspondientes.

El amplio uso de las técnicas de multiplexación en comunicaciones de datos se puede explicar como sigue:

- A medida que la velocidad es superior, la transmisión es más efectiva desde el punto de vista del coste. Es decir, para una aplicación y distancia dadas el coste por kbps decrece con el incremento en la velocidad de transmisión de datos. De forma análoga, el coste de los equipos de transmisión y recepción, por kbps, decrece con el aumento de la velocidad.

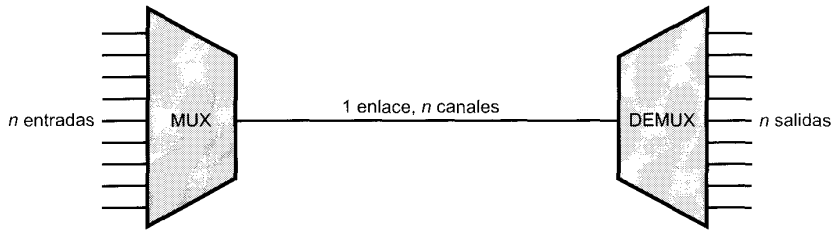


Figura 8.1. Multiplexación.

- La mayor parte de los dispositivos de comunicación de datos requiere velocidades de datos relativamente bajas. Por ejemplo, para la mayoría de las aplicaciones de terminales y de computadores personales resulta adecuada una velocidad comprendida entre 9.600 bps y 64 kbps.

Los puntos anteriores se refieren a dispositivos de comunicación de datos, pudiéndose aplicar también a comunicaciones de voz. Es decir, cuanto mayor sea la capacidad de la transmisión, en términos de canales de voz, menor será el coste por canal de voz individual, siendo modesta la capacidad requerida por cada canal de voz.

Este capítulo centra su interés en tres tipos de técnicas de multiplexación. La primera, multiplexación por división en frecuencias (FDM), es la más utilizada, resultando familiar para quienes hayan usado una radio o una televisión. La segunda es un caso particular de la multiplexación por división en el tiempo (TDM) conocida como TDM síncrona. Ésta se emplea generalmente para multiplexar secuencias de voz digitalizadas y secuencias de datos. El tercer tipo persigue la mejora en la eficiencia de la técnica TDM síncrona haciendo más complejo el multiplexor. Esta técnica se conoce con varios nombres, incluyendo TDM estadística, TDM asíncrona y TDM inteligente. En este libro se emplea el término TDM estadística, resaltándose así una de sus propiedades principales. Finalmente se estudiará el bucle de abonado digital, que combina las tecnologías FDM y TDM síncrona.

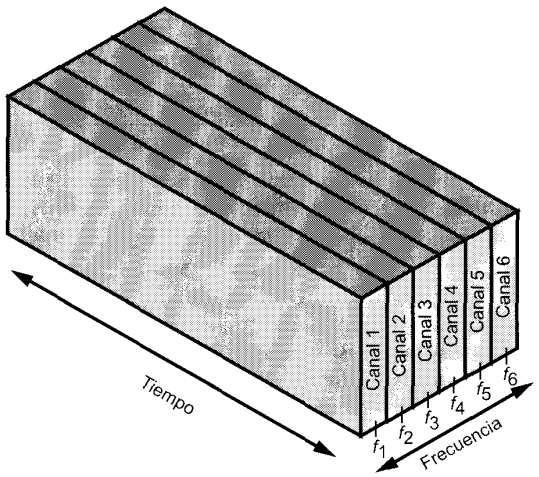
8.1. MULTIPLEXACIÓN POR DIVISIÓN EN FRECUENCIAS

CARACTERÍSTICAS

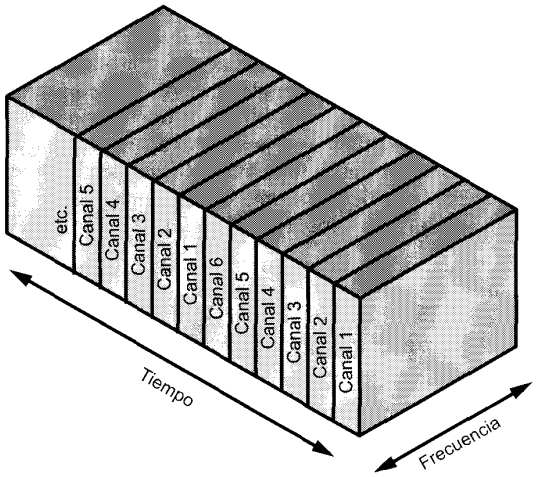
Es posible utilizar FDM cuando el ancho de banda útil del medio de transmisión supera el ancho de banda requerido por las señales a transmitir. Se pueden transmitir varias señales simultáneamente si cada una de ellas se modula con una frecuencia portadora diferente y las frecuencias portadoras están suficientemente separadas para que los anchos de banda de las señales no se solapen de forma importante. En la Figura 8.2a se muestra un caso general de FDM. En él se observa la entrada de seis líneas a un multiplexor, el cual modula cada señal a una frecuencia diferente (f_1, ..., f_6). Cada señal modulada precisa un cierto ancho de banda centrado alrededor de su frecuencia portadora y conocido como *canal*. Para evitar interferencias los canales se separan mediante bandas guardas o de seguridad, las cuales son zonas no utilizadas del espectro.

La señal compuesta transmitida a través del medio es analógica. Sin embargo, hemos de indicar que las señales de entrada pueden ser tanto digitales como analógicas. En el caso de que la entrada sea digital, las señales se deben pasar a través de modems para ser convertidas en analógicas. En cualquier caso, la señal de entrada analógica se debe modular para trasladarla a la banda de frecuencia apropiada.

Un ejemplo típico de FDM es la televisión convencional y por cable. La señal de televisión estudiada en el Capítulo 3 ocupa un ancho de banda de 6 MHz. La Figura 8.3 muestra la señal de TV transmiti-



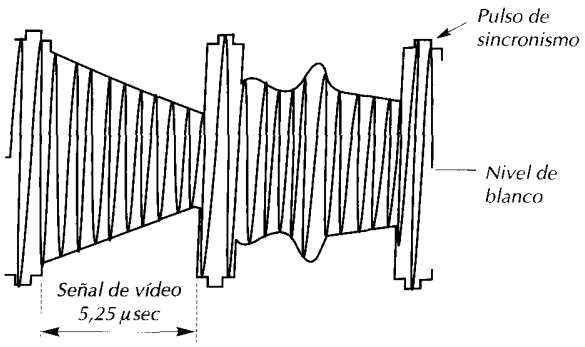
(a) Multiplexación por división en frecuencias



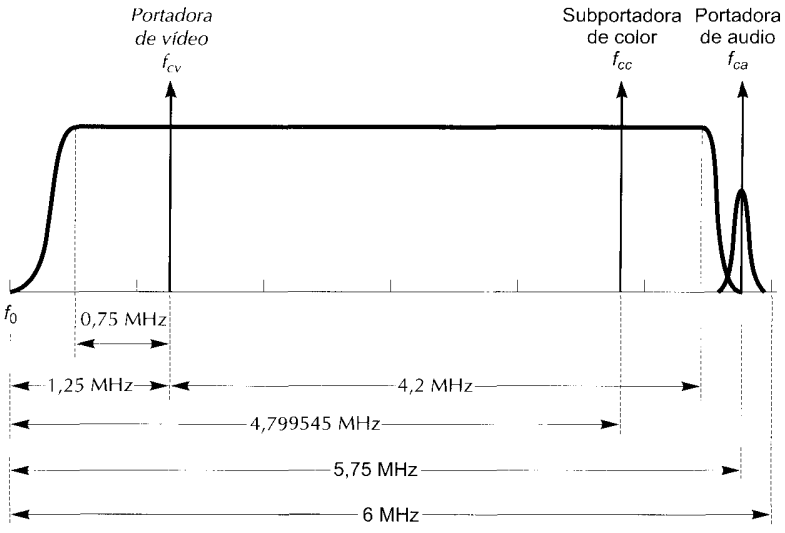
(b) Multiplexación por división en el tiempo

Figura 8.2. FDM y TDM.

da y su ancho de banda. La señal de vídeo en blanco y negro se modula en AM con una portadora f_{cv}. Dado que la señal de vídeo en banda base tiene un ancho de banda de 4 MHz, es de esperar que la señal modulada ocupe un ancho de banda de 8 MHz centrados en torno a f_{cv}. Para ahorrar ancho de banda la señal se hace pasar por un filtro de banda lateral con objeto de suprimir la mayor parte de la banda lateral inferior. La señal resultante se extiende desde aproximadamente los f_{cv} − 0,75 MHz hasta los f_{cv} + 4,2 MHz. Para transmitir información correspondiente al color se usa una subportadora de color independiente, f_{cc}, la cual estará lo suficientemente alejada de f_{cv} para evitar la existencia de interferencias importantes. Finalmente, la señal de audio se modula a f_{ca}, fuera del ancho de banda efectivo de las otras dos señales. Para la señal de audio se reserva un ancho de banda de 50 kHz. La señal compuesta cabe en



(a) Modulación de amplitud de la señal de vídeo

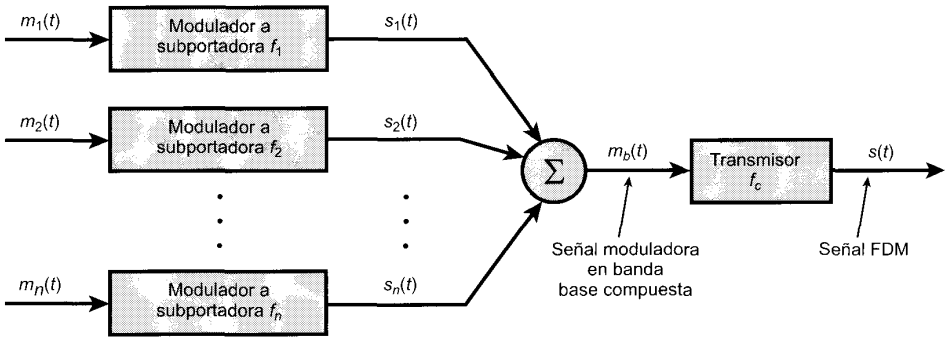


(b) Magnitud del espectro de la señal RF de vídeo

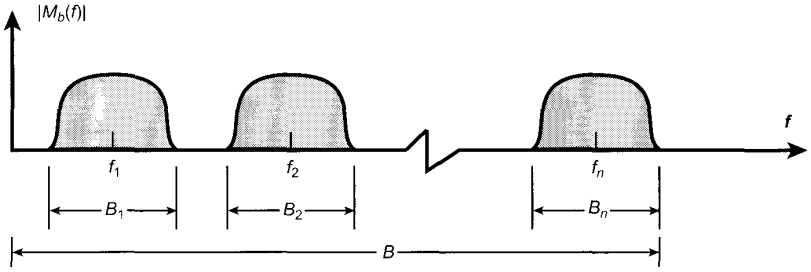
Figura 8.3. Señal de TV transmitida.

un ancho de banda de 6 MHz, con las portadoras de vídeo, color y audio desplazadas a 1,25 MHz, 4,799545 MHz y 5,75 MHz respecto del extremo inferior de la banda, respectivamente. Así pues, haciendo uso de FDM se pueden multiplexar varias señales de TV en un cable CATV, cada una de ellas con un ancho de banda de 6 MHz. Dado el enorme ancho de banda de un cable coaxial (hasta 500 MHz), haciendo uso de FDM se pueden transmitir simultáneamente docenas de señales de TV. Es claro que la propagación en radiofrecuencia a través de la atmósfera es también una forma de FDM; en la Tabla 8.1 se muestra la asignación de frecuencias para la televisión por cable en los Estados Unidos.

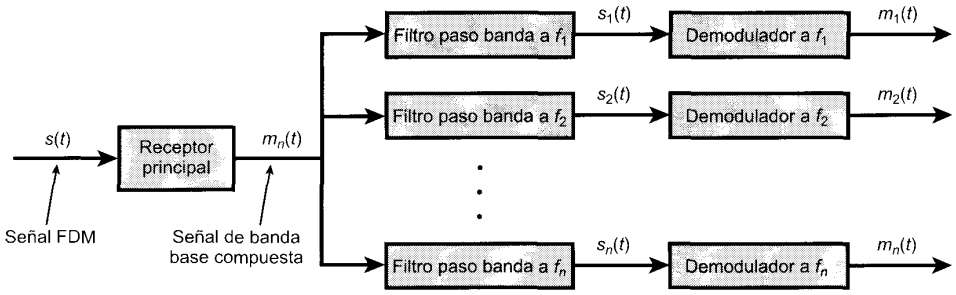
En la Figura 8.4 se muestra un esquema general de un sistema FDM. Se multiplexan varias señales analógicas o digitales $[m_i(t),\ i = 1,\ n]$ a través del mismo medio de transmisión. Cada señal $m_i(t)$ se modula por una portadora f_i. Dado que se usan varias portadoras, cada una de ellas se denomina subportadora. Se puede hacer uso de cualquier tipo de modulación. Las señales moduladas analógicas resultan-



(a) Transmisor



(b) Espectro de la señal moduladora en banda base compuesta



(c) Receptor

Figura 8.4. Sistema FDM [COUC97].

tes se suman para dar lugar a una señal $m_b(t)$ en banda base compuesta[1]. En la Figura 8.4b se muestra el resultado. El espectro de la señal $m_i(t)$ se desplaza hasta quedar centrado en f_i. Para que este esquema funcione adecuadamente, f_i se debe elegir de modo que los anchos de banda de las distintas señales

[1] El término *banda base* se emplea para designar la banda de frecuencias de la señal transmitida por la fuente y potencialmente usada como señal moduladora. Generalmente, el espectro de una señal banda base es significativo en una banda que incluye o está en la vecindad de $f = 0$.

Tabla 8.1. Asignación de frecuencia para canales de televisión por cable.

Número del canal	Banda (MHz)	Número del canal	Banda (MHz)	Número del canal	Banda (MHz)
2	54-60	22	168-174	42	330-336
3	60-66	23	216-222	43	336-342
4	66-72	24	222-228	44	342-348
5	76-82	25	228-234	45	348-354
6	82-88	26	234-240	46	354-360
7	174-180	27	240-246	47	360-366
8	180-196	28	246-252	48	366-372
9	186-192	29	252-258	49	372-378
10	192-198	30	258-264	50	378-384
11	198-204	31	264-270	51	384-390
12	204-210	32	270-276	52	390-396
13	210-216	33	276-282	53	396-402
FM	88-108	34	282-288	54	402-408
14	120-126	35	288-294	55	408-414
15	126-132	36	294-300	56	414-420
16	132-138	37	300-306	57	420-426
17	138-144	38	306-312	58	426-432
18	144-150	39	312-318	59	432-438
19	150-156	40	318-324	60	438-444
20	156-162	41	324-330	61	444-450
21	162-168				

no se solapen de forma significativa. En caso contrario resultaría imposible recuperar las señales originales.

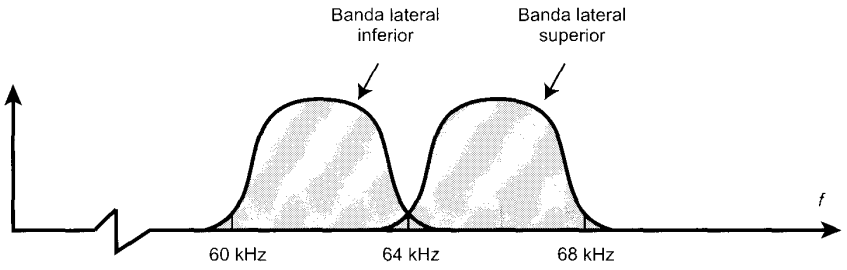
Tras esto, la señal compuesta puede desplazarse como un todo a otra frecuencia portadora a través de un proceso adicional de modulación. Posteriormente veremos ejemplos de esto. Este segundo paso de modulación no requiere hacer uso de la misma técnica de modulación que el primero.

La señal FDM $s(t)$ tiene un ancho de banda total B, donde $B > \sum_{i=1}^{n} B_i$. Esta señal analógica se puede transmitir a través de un medio adecuado. En el extremo receptor, se demodula la señal FDM para recuperar $m_b(t)$, la cual se hace pasar a través de n filtros paso banda cada uno centrado en torno a f_i con un ancho de banda B_i, para $1 \leqslant i \leqslant n$. De esta forma, la señal se divide de nuevo en sus componentes, siendo cada una de ellas demodulada para recuperar la señal original correspondiente.

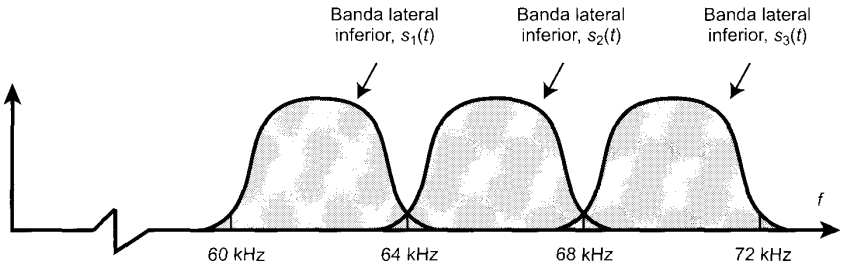
Considérese un ejemplo sencillo consistente en la transmisión simultánea de tres señales de voz a través de un medio. Como se ha mencionado, el ancho de banda de una señal de voz se considera generalmente igual a 4 kHz, con un espectro efectivo comprendido entre los 300 y los 3.400 Hz (Figura 8.5a). Si una señal de este tipo se usa para modular en amplitud una portadora de 64 kHz, se obtiene el espectro de la Figura 8.5b. La señal modulada tiene un ancho de banda de 8 kHz, extendiéndose desde los 60 hasta los 68 kHz. Para hacer un uso eficiente del ancho de banda elegimos transmitir sólo la banda lateral inferior. Si ahora las tres señales de voz se usan para modular portadoras a frecuencias de 64, 68 y 72 kHz, y sólo se utiliza la banda lateral inferior de cada una de ellas, se obtiene el espectro de la Figura 8.5c.

Esta figura pone de manifiesto dos problemas con que se enfrenta un sistema FDM. El primero es la diafonía, que puede aparecer si los espectros de señales componentes adyacentes se solapan de forma importante. En el caso de señales de voz, con un ancho de banda efectivo de sólo 3.100 Hz (de 300 a 3.400), resulta adecuado un ancho de banda de 4 kHz. El espectro de señales generadas por modems para transmisiones en la banda de voz también cabe bien en este ancho de banda. Otro problema potencial es el ruido de intermodulación, estudiado en el Capítulo 3. En un enlace largo, los efectos no linea-

(a) Espectro de $m_1(t)$, f positivas



(b) Espectro de $s_1(t)$ para f_1 = 64 kHz



(c) Espectro de la señal compuesta usando subportadoras de 64 kHz, 68 kHz y 72 kHz

Figura 8.5. FDM de tres señales en la banda de voz.

les de los amplificadores sobre una señal en un canal pueden dar lugar a componentes en frecuencia en otros canales.

SISTEMAS CON PORTADORA ANALÓGICA

El sistema de larga distancia existente en los Estados Unidos y en todo el mundo ha sido diseñado para transmitir señales en la banda de voz a través de enlaces de transmisión de alta capacidad tales como cable coaxial y sistemas de microondas. La primera, y aún hoy de amplio uso, técnica para la utilización de enlaces de alta capacidad es FDM. En los Estados Unidos, AT&T diseñó una jerarquía de esquemas FDM para dar cabida a sistemas de transmisión de distintas capacidades. Un sistema similar, aunque desafortunadamente distinto, fue adoptado internacionalmente bajo los auspicios de la ITU-T (Tabla 8.2).

Tabla 8.2. Estándares de portadora FDM norteamericanos e internacionales.

Número de canales de voz	Ancho de banda	Espectro	AT & T	ITU-T
12	48 kHz	60-108 kHz	Grupo	Grupo
60	240 kHz	312-552 kHz	Supergrupo	Supergrupo
300	1,232 MHz	812-2.044 kHz		Grupo maestro
600	2,52 MHz	564-3.084 kHz	Grupo maestro	
900	3,872 MHz	8,516-12,388 MHz		Grupo supermaestro
N × 600			Grupo maestro multiplexado	
3.600	16,984 MHz	0,564-17,548 MHz	Grupo jumbo	
10.800	57,442 MHz	3,124-60,566 MHz	Grupo jumbo multiplexado	

En el primer nivel de la jerarquía AT&T se combinan 12 canales de voz para dar lugar a una señal grupo con un ancho de banda de 12 × 4 kHz = 48 kHz, en el rango 60-108 kHz. Las señales se generan de forma similar a la descrita previamente haciendo uso de frecuencias subportadoras de entre 64 y 108 kHz en incrementos de 4 kHz. El siguiente bloque es el supergrupo de 60 canales, que está formado por cinco señales de grupo multiplexadas en frecuencias. En este nivel, cada grupo se trata como una única señal con un ancho de banda de 48 kHz, modulándose por la correspondiente subportadora. Las subportadoras tienen frecuencias comprendidas entre 420 y 612 kHz en incrementos de 48 kHz. La señal resultante ocupa la banda 312-552 kHz.

Existen numerosas variantes para la formación de un supergrupo. Cada una de las cinco entradas al multiplexor de supergrupo puede ser un canal de grupo con 12 señales de voz multiplexadas. Es más, cualquier señal de hasta 48 kHz de ancho de banda contenida entre los 60 y los 108 kHz se puede usar como entrada al multiplexor de supergrupo. Otra posibilidad consiste en combinar 60 canales de ancho de banda de voz en un supergrupo, lo cual puede reducir los costes de multiplexación ya que no se precisa una interfaz con el multiplexor de grupo.

El siguiente nivel de la jerarquía es el grupo maestro, en el que se combinan 10 supergrupos. Una vez más, cualquier señal con un ancho de banda de 240 kHz en el rango 312-552 kHz puede servir como entrada al multiplexor de grupo maestro. El grupo maestro tiene un ancho de banda de 2,52 MHz y puede soportar 600 canales de frecuencia de voz (VF, voice frequency). Como se muestra en la Tabla 8.2, por encima del grupo maestro se definen niveles de multiplexación superiores.

Obsérvese que la señal de voz o de datos original se puede modular varias veces. Por ejemplo, una señal de datos se puede codificar haciendo uso de QPSK para generar una señal de voz analógica. Esta señal se podría usar para modular una portadora de 76 kHz para producir una componente de una señal de grupo. Dicha señal de grupo puede usarse a su vez para modular una portadora de 516 kHz para dar lugar a una componente de una señal de supergrupo. Cada etapa puede distorsionar los datos originales; esto ocurre si, por ejemplo, el modulador/multiplexor presenta no linealidades o introduce ruido.

8.2. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO SÍNCRONA

CARACTERÍSTICAS

La multiplexación por división en el tiempo síncrona es posible cuando la velocidad de transmisión alcanzable (a veces llamada inapropiadamente ancho de banda) por el medio excede la velocidad de las señales digitales a transmitir. Se pueden transmitir varias señales digitales (o señales analógicas que transportan datos digitales) a través de una única ruta de transmisión mediante la mezcla temporal de partes de cada una de las señales. El proceso de mezcla puede ser a nivel de bit o en bloques de octetos o cantidades superiores. Por ejemplo, el multiplexor de la Figura 8.2b tiene seis entradas de, digamos, 9,6 kbps. Una única línea con capacidad de al menos 57,6 kbps (más la capacidad suplementaria) puede dar cabida a las seis fuentes.

En la Figura 8.6 se proporciona un esquema general de un sistema TDM. Se multiplexan varias señales $[m_i(t), i = 1, n]$ a través del mismo medio de transmisión. Las señales transportan datos digitales y son en general señales digitales. Los datos de entrada procedentes de cada fuente se almacenan brevemente en una memoria temporal o «buffer». Cada memoria temporal tiene una longitud típica de un bit o un carácter. Estas memorias temporales se sondean secuencialmente para componer una secuencia de datos digital compuesta $m_c(t)$. El sondeo es lo suficientemente rápido para que cada memoria temporal se vacíe antes de que se reciban nuevos datos. Por tanto, la velocidad de $m_c(t)$ debe ser al menos igual a la suma de las velocidades de las señales $m_i(t)$. La señal digital $m_c(t)$ se puede transmitir directamente o se puede hacer pasar a través de un módem para dar lugar a una señal analógica. En ambos casos la transmisión es generalmente síncrona.

Los datos transmitidos pueden tener un formato similar al mostrado en la Figura 8.6b. Los datos se organizan en tramas, cada una de las cuales contiene un ciclo de ranuras temporales. En cada trama se dedican una o más ranuras a cada una de las fuentes. La secuencia de ranuras dedicadas a una fuente, de trama en trama, se llama canal. La longitud de la ranura es igual a la longitud de la memoria temporal de transmisión, generalmente un bit o un carácter.

La técnica de mezcla de caracteres se usa con fuentes asíncronas, conteniendo cada ranura temporal un carácter de datos. Usualmente, los bits de principio y de fin de cada carácter se eliminan antes de la transmisión y se reinsertan por parte del receptor, mejorando así la eficiencia. La técnica de mezcla de bits se usa con fuentes síncronas, pudiendo utilizarse también con fuentes asíncronas. Cada ranura temporal contiene un único bit.

Los datos mezclados se demultiplexan en el receptor y se encaminan hacia la memoria temporal de destino apropiada. Para cada fuente de entrada $m_i(t)$ existe una fuente de salida idéntica que recibirá los datos de entrada a la misma velocidad a la que fueron generados.

La técnica TDM síncrona se denomina síncrona no porque se emplee transmisión síncrona, sino porque las ranuras temporales se preasignan y fijan a las distintas fuentes. Las ranuras temporales asociadas a cada fuente se transmiten tanto si éstas tienen datos que enviar como si no. Esto, por supuesto, también ocurre en FDM. En ambos casos se desaprovecha la capacidad a costa de simplificar la implementación. Sin embargo, un dispositivo TDM síncrono puede gestionar fuentes a distintas velocidades incluso cuando se hacen asignaciones fijas de las ranuras temporales. Por ejemplo, al dispositivo de entrada más lento se le podría asignar una ranura por ciclo, mientras que a los más rápidos se podrían asignar varias ranuras por ciclo.

CONTROL DEL ENLACE EN TDM

El lector habrá observado que la secuencia de datos transmitida mostrada en la Figura 8.6b no contiene las cabeceras y colas propias de la transmisión síncrona. La razón es que no es necesario el mecanismo de control proporcionado por un protocolo de enlace de datos. Resulta instructivo hacer hincapié en este

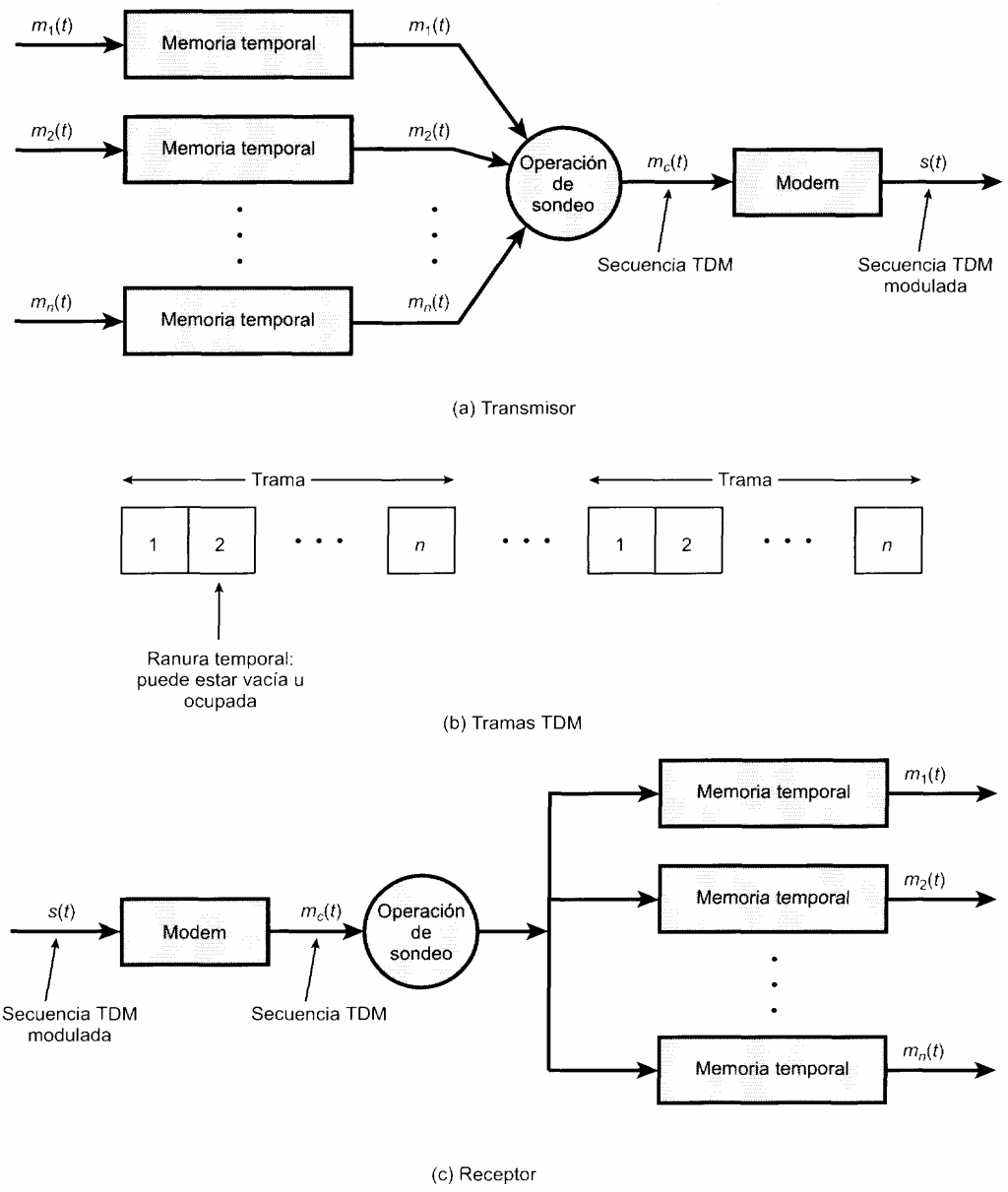


Figura 8.6. Sistema TDM síncrono.

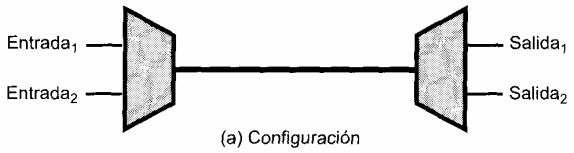
punto, para lo cual se considerarán dos mecanismos clave en el control del enlace de datos: control de flujo y control de errores. Es claro que el control de flujo no es necesario por lo que se refiere al multiplexor y al demultiplexor (Figura 8.1). La velocidad de datos es fija en la línea del multiplexor, estando éste y el demultiplexor diseñados para operar a esta velocidad. Pero supóngase que una de las líneas de salida está conectada a un dispositivo que es incapaz de aceptar datos temporalmente. ¿Debería cesar la transmisión de tramas TDM? Definitivamente no, ya que las restantes líneas de salida están esperando a recibir datos en instantes de tiempo predeterminados. La solución consiste en que el dispositivo de sali-

da que se ha saturado detenga el flujo de datos proveniente del correspondiente dispositivo de entrada. Así, el canal en cuestión transmitirá ranuras vacías durante algún tiempo pero las tramas en su conjunto mantendrán la misma velocidad de transmisión.

El razonamiento es el mismo para del control de errores. No se debería solicitar la retransmisión de una trama TDM completa si ocurriera un error en uno de los canales. Los dispositivos que utilizan los otros canales no querrían una retransmisión ni sabrían que algún otro dispositivo en otro canal la ha solicitado. De nuevo la solución consiste en aplicar el control de errores para cada canal de forma independiente.

El control de flujo y el control de errores pueden aplicarse para cada canal independientemente usando un protocolo de control de enlace de datos como HDLC. En la Figura 8.7 se muestra un ejemplo simplificado. Se suponen dos fuentes de datos, cada una de las cuales utiliza HDLC. Una de ellas transmite una secuencia de tramas HDLC de tres octetos de datos cada una y la otra fuente transmite tramas HDLC con cuatro octetos de datos. Por sencillez, y aunque es más frecuente la mezcla de bits, supóngase que se usa multiplexación por mezcla de caracteres. Obsérvese lo que sucede. Los octetos de las tramas HDLC de las dos fuentes se transmiten juntos a través de la línea multiplexada. Al lector puede resultarle incómodo inicialmente este diagrama dado que en cierto sentido las tramas HDLC han perdido su integridad. Por ejemplo, cada secuencia de comprobación de trama (FCS) en la línea se aplica a un conjunto distinto de bits. Incluso la FCS está dividida. No obstante, todas las piezas se ensamblan correctamente antes de que se reciban en el dispositivo correspondiente al otro extremo del protocolo HDLC. En este sentido, la operación de multiplexación/demultiplexación es transparente para las estaciones conectadas; es como si existiese un enlace dedicado para cada par de estaciones comunicadas.

En la Figura 8.7 se necesita un refinamiento. Ambos extremos de la línea tienen que ser una combinación multiplexor/demultiplexor con una línea *full-duplex* entre ellos. Así pues, cada canal consta de dos conjuntos de ranuras, una en cada sentido de la transmisión. Los dispositivos individuales conectados en cada extremo pueden, en parejas, usar HDLC para controlar su propio canal. Los multiplexores/demultiplexores no necesitan preocuparse de estas cuestiones.



(a) Configuración

Entrada$_1$ •••••••••• F_1 f_1 f_1 d_1 d_1 d_1 C_1 A_1 F_1 f_1 f_1 d_1 d_1 d_1 C_1 A_1 F_1

Entrada$_2$•••• F_2 f_2 f_2 d_2 d_2 d_2 d_2 C_2 A_2 F_2 f_2 f_2 d_2 d_2 d_2 d_2 C_2 A_2 F_2

(b) Cadena de datos de entrada

••• f_2 F_1 d_2 f_1 d_2 f_1 d_2 d_1 d_2 d_1 C_2 d_1 A_2 C_1 F_2 A_1 f_2 F_1 f_2 f_1 d_2 f_1 d_2 d_1 d_2 d_1 d_2 d_1 C_2 C_1 A_2 A_1 F_2 F_1

(c) Cadenas de datos multiplexada

Leyenda: F = campo delimitador
A = campo de direcciones
C = campo de control
d = un octeto del campo de datos
f = un octeto del campo FCS

Figura 8.7. Uso del control de enlace de datos en canales TDM.

Delimitación de tramas

Ya se ha visto que no es preciso un protocolo de control de enlace para gestionar el enlace TDM. No obstante, es necesaria una delimitación básica. Dado que no se han especificado indicadores o caracteres SYNC para delimitar las tramas TDM, es necesario algún método para asegurar la sincronización de éstas. Es clara la importancia de mantener la sincronización de trama ya que si la fuente y el destino se desincronizan se perderán los datos de todos los canales.

Quizás el mecanismo más usual para llevar a cabo la delimitación de tramas sea el conocido como delimitación por dígitos añadidos. En este esquema, generalmente, se incluye un bit de control en cada trama TDM. A modo de «canal de control», en cada trama se usa una combinación predefinida de bits. Un ejemplo típico es el patrón de bits alternantes 101010..., cuya aparición resulta poco probable en un canal de datos. De este modo, para sincronizar, el receptor compara los bits de entrada en una determinada posición de la trama con el patrón esperado. Si no coinciden, se compara con los bits sucesivos hasta que se encuentre la combinación de bits y éste persista a lo largo de varias tramas. Una vez realizada la sincronización, el receptor continúa la monitorización del canal de bits de delimitación. Si desaparece el patrón el receptor debe llevar a cabo de nuevo el proceso de búsqueda.

Inserción de bits

Quizás el problema más difícil en el diseño de un multiplexor por división en el tiempo síncrono sea la sincronización de las distintas fuentes de datos. Si cada fuente dispone de un reloj independiente, cualquier variación entre los relojes puede causar la pérdida del sincronismo. En algunos casos puede suceder también que las velocidades de datos de las secuencias de entrada no estén relacionadas por un número racional simple. En ambos casos resulta efectiva la técnica conocida como inserción de bits. En ella, la velocidad de salida del multiplexor, excluyendo los bits de delimitación, es mayor que la suma de las velocidades de entrada instantáneas máximas. La capacidad extra se emplea en la inclusión de pulsos o bits adicionales sin significado en cada señal de entrada hasta que su velocidad alcance a la de una señal de reloj generada localmente. Los pulsos insertados lo son en posiciones fijas dentro del formato de trama del multiplexor de manera que puedan ser identificados y eliminados en el demultiplexor.

Ejemplo

Un ejemplo, extraído de [COUC97], ilustra el uso de TDM síncrona para multiplexar fuentes analógicas y digitales (Figura 8.8). Considérese la existencia de 11 fuentes a multiplexar en un enlace:

- Fuente 1: analógica, con 2 kHz de ancho de banda.
- Fuente 2: analógica, con 4 kHz de ancho de banda.
- Fuente 3: analógica, con 2 kHz de ancho de banda.
- Fuentes 4-11: digitales síncronas a 7.200 bps.

En primer lugar se convierten a digital las fuentes analógicas haciendo uso de la técnica PCM. Recuérdese del Capítulo 5 que PCM se fundamenta en el teorema de muestreo, el cual establece que una señal se debe muestrear a una velocidad igual a dos veces su ancho de banda. Por tanto, la velocidad de muestreo para las fuentes 1 y 3 será de 4.000 muestras por segundo, y de 8.000 muestras por segundo para la fuente 2. Estas muestras, de naturaleza analógica (PAM), se deben cuantificar o digitalizar. Supóngase que se usan 4 bits para cada muestra analógica. Por comodidad, estas tres fuentes se multiplexarán en primer lugar. A una velocidad de sondeo de 4 kHz se toma por cada ciclo una muestra PAM de las fuentes 1 y 3 de forma alternativa y dos muestras PAM de la fuente 2. Estas cuatro muestras se mezclan y convierten a muestras PCM de 4 bits. Se genera así un total de 16 bits a razón de 4.000 veces por segundo, dando lugar a una velocidad compuesta de 64 kbps.

Para las fuentes digitales se usa inserción de bits con objeto de que cada fuente alcance una velocidad de 8 kbps para una velocidad conjunta de 64 kbps. Una trama puede constar de varios ciclos de 32

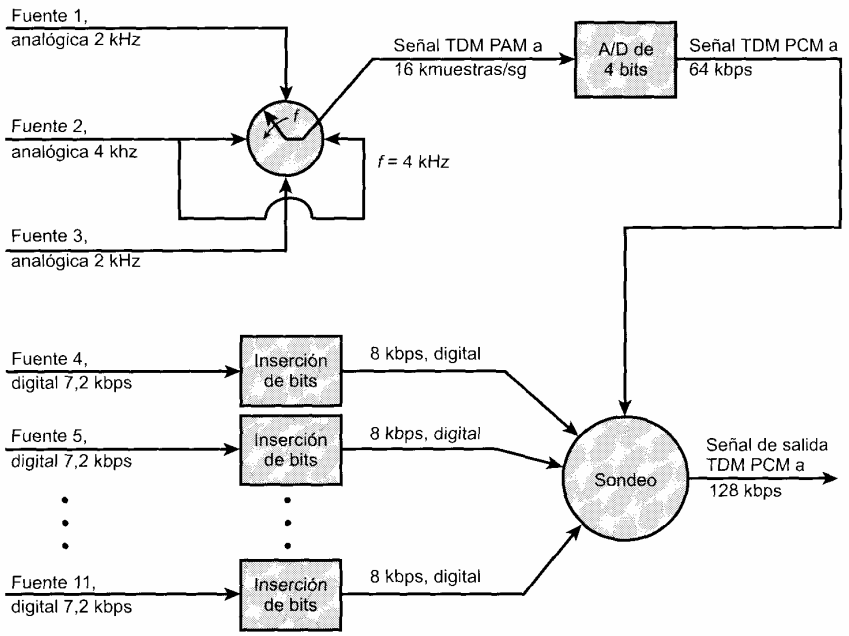


Figura 8.8. TDM para fuentes analógicas y digitales [COUC97].

bits, constando cada uno de ellos de 16 bits PCM y dos bits correspondientes a cada una de las ocho fuentes digitales.

SISTEMAS CON PORTADORA DIGITAL

El sistema de transmisiones de larga distancia de los Estados Unidos y del resto del mundo se diseñó para transmitir señales de voz a través de enlaces de transmisión de alta capacidad tales como fibra óptica, cable coaxial y microondas. Parte de la evolución de estas redes de telecomunicaciones hacia la tecnología digital ha consistido en la adopción de estructuras de transmisión TDM síncrona. En los Estados Unidos, AT&T desarrolló una jerarquía de estructuras TDM con diferentes capacidades; esta estructura se ha adoptado también en Canadá y en Japón. Una jerarquía análoga, aunque por desgracia no idéntica, fue adoptada internacionalmente bajo los auspicios de la ITU-T (Tabla 8.3).

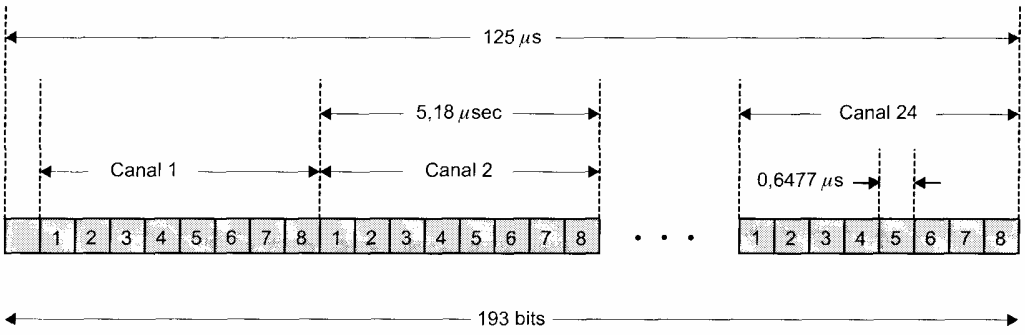
Tabla 8.3. Estándares TDM norteramericanos e internacionales.

Norteamérica			Internacional (ITU-T)		
Nomenclatura	**Número de canales de voz**	**Velocidad (Mbps)**	**Nivel**	**Número de canales de voz**	**Velocidad (Mbps)**
DS-1	24	1,544	1	30	2,048
DS-1C	48	3,152	2	120	8,448
DS-2	96	6,312	3	480	34,368
DS-3	672	44,736	4	1.920	139,264
DS-4	4.032	274,176	5	7.680	565,148

La base de la jerarquía TDM (en Norteamérica y Japón) es el formato de transmisión DS-1 (Figura 8.9), en el que se multiplexan 24 canales. Cada trama contiene 8 bits por canal más un bit de delimitación; es decir, 24 × 8 + 1 = 193 bits. Para transmisiones de voz se aplican las siguientes reglas. Cada canal contiene una palabra de datos de voz digitalizada. La señal de voz analógica original se digitaliza haciendo uso de la técnica de modulación por codificación de pulso (PCM) a una velocidad de 8.000 muestras por segundo. Por tanto, cada canal y, en consecuencia, cada trama se debe repetir 8.000 veces por segundo. Con una trama de longitud 193 bits se dispone por tanto de una velocidad de 8.000 × 193 = 1,544 Mbps. En cinco de cada seis tramas se utilizan muestras PCM de 8 bits. Cada seis tramas, cada uno de los canales contiene una palabra PCM de 7 bits más un *bit de señalización*. Los bits de señalización forman una secuencia para cada canal de voz que contiene información de control de red y de encaminamiento. Por ejemplo, las señales de control se emplean para establecer una conexión o para finalizar una llamada.

El formato DS-1 se emplea también para proporcionar servicio de datos digitales. Por cuestiones de compatibilidad con la voz se usa la misma velocidad de 1,544 Mbps. En este caso existen 23 canales de datos. El canal de posición vigésimo cuarto se reserva para un carácter especial *sync* que permite una recuperación más rápida y fiable de la delimitación tras un error en la misma. En cada canal se usan 7 bits de datos por trama, indicando el octavo bit si el canal, en esa trama, contiene datos de usuario o de control del sistema. Con 7 bits por canal, y dado que cada trama se repite 8.000 veces por segundo, se obtiene una velocidad de datos por canal de 56 kbps. Se pueden conseguir velocidades inferiores a través de la utilización de una técnica conocida como multiplexación de baja velocidad. En esta técnica se dedica un bit adicional de cada canal para indicar qué velocidad se va a proporcionar. Esto da una capacidad total por canal de 6 × 8.000 = 48 kbps. Esta capacidad se utiliza para multiplexar cinco canales a 9,6 kbps, diez canales a 4,8 kbps o veinte canales a 2,4 kbps. Por ejemplo, si se usa el canal 2 para proporcionar un servicio a 9,6 kbps, entonces hasta cinco subcanales de datos compartirán este subcanal. Los datos de cada subcanal aparecen como seis bits en el canal 2 cada cinco tramas.

Finalmente, el formato DS-1 se puede ser usar para transportar una mezcla de canales de voz y de datos. En este caso se utilizan los 24 canales, no existiendo octeto *sync*.



Notas

1. El primer bit es de delimitación, usado en la sincronización.
2. Canales de voz:
   - PCM 8 bits usado en cinco de cada seis tramas.
   - PCM 7 bits usado en una de cada seis tramas; el bit 8 de cada canal es de señalización.
3. Canales de datos:
   - El canal 24 se emplea para señalización sólo en algunos esquemas.
   - Los bits del 1 al 7 se usan para el servicio a 56 kbps.
   - Los bits 2-7 se usan para servicios a 9,6 kbps, 4,8 kbps y 2,4 kbps.

Figura 8.9. Formato de transmisión DS-1.

Por encima de la velocidad de 1,544 Mbps proporcionada por DS-1 se obtienen niveles superiores de multiplexación mediante la mezcla de bits procedentes de entradas DS-1. Por ejemplo, el sistema de transmisión DS-2 combina cuatro entradas DS-1 en una cadena de 6,312 Mbps. Los datos de las cuatro fuentes se mezclan a razón de 12 bits cada vez. Obsérvese que $1{,}544 \times 4 = 6{,}176$ Mbps. La capacidad restante se emplea para bits de delimitación y de control.

INTERFAZ USUARIO-RED EN RDSI

RDSI permite a un usuario multiplexar tráfico procedente de varios dispositivos a través de una misma línea de una red RDSI (red digital de servicios integrados). Se definen dos interfaces: una básica y otra primaria.

Acceso básico RDSI

En la interfaz entre el abonado y el equipo terminal de red se intercambian los datos mediante transmisión *full-duplex*. Para ello se utiliza una línea física independiente para cada sentido. La especificación de codificación de línea para la interfaz exige el uso del esquema de codificación pseudoternario[2], donde el uno binario se representa por la ausencia de tensión y el cero binario mediante un pulso positivo o negativo de 750 mV $\pm$ 10 %. La velocidad es 192 kbps.

La estructura del acceso básico consta de dos canales B de 64 kbps y un canal D de 16 kbps. Estos canales, que producen una carga de 144 kbps, se multiplexan sobre una interfaz usuario-red de 192 kbps. La capacidad restante se usa con distintos fines de delimitación y sincronización.

El canal B es el canal básico de usuario, pudiéndose utilizar para transmitir datos digitales (por ejemplo, una conexión de un computador personal), voz digital codificada PCM (por ejemplo, una conexión de teléfono) u otro tipo de tráfico que quepa en un canal de 64 kbps. En cualquier momento se puede establecer una conexión lógica independiente para cada canal B con destinos RDSI distintos. El canal D se puede usar para una conexión de transmisión de datos a una velocidad inferior, usándose también para transportar información de control necesaria para establecer y terminar las conexiones de canal B. La transmisión a través del canal D consiste en una secuencia de tramas LAPD.

Como en cualquier esquema de multiplexación por división en el tiempo síncrona (TDM), la transmisión de acceso básico se estructura en tramas de longitud fija que se repiten. En este caso, cada trama tiene una longitud de 48 bits; a una velocidad de 192 kbps las tramas se deben repetir a razón de una trama cada 250 μs. En la Figura 8.10 se muestra la estructura de la trama; la trama superior se transmite por parte del equipo terminal de abonado (TE, terminal equipment) hacia la red (NT network terminal); la trama inferior se transmite desde el NT hacia el TE.

Cada trama de 48 bits incluye 16 bits de cada uno de los dos canales B y 4 bits del canal D. Los bits restantes tienen la siguiente interpretación. Consideremos en primer lugar la estructura de trama en la dirección TE a NT. Cada trama comienza con un bit de delimitación (F) que se transmite siempre como un pulso positivo. Este bit está seguido por un bit de compensación DC (L) al que se asigna un pulso negativo. La combinación F-L sirve para sincronizar al receptor indicándole el comienzo de la trama. La especificación establece que, tras estas dos primeras posiciones de bit, la primera ocurrencia de un bit cero se codificará mediante un pulso negativo. Después de esto se aplican las reglas pseudoternarias. Los ocho bits siguientes (B1) son del primer canal B, los cuales están seguidos por otro bit de compensación DC (L). A continuación viene un bit del canal D, seguido por su bit de compensación. Seguidamente aparece el bit de delimitación auxiliar (F_A) que vale cero salvo cuando se usa en una estructura multitrama. A continuación sigue otro bit de compensación (L), ocho bits (B2) del segundo canal B y otro bit de compensación (L). Todo esto va seguido por bits del canal D, del primer canal B, del canal D

[2] Véase Sección 5.1.

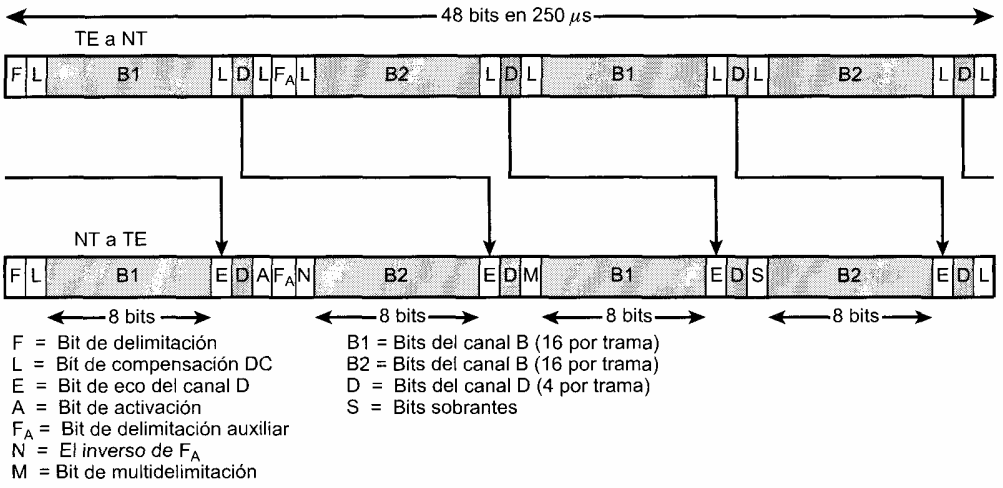


Figura 8.10. Estructura de trama para el acceso básico en RDSI.

de nuevo, del segundo canal B y del canal D otra vez, donde cada grupo de bits de canal va seguido por un bit de compensación.

La estructura de trama desde el NT hacia el TE es similar a la de la transmisión en el sentido TE a NT. Los nuevos bits que se indican a continuación reemplazan a algunos de bits de compensación DC. El bit de eco del canal D (E) es una retransmisión por parte del NT de los bits D más recientes recibidos desde el TE; el objetivo de este eco se explicará más adelante. El bit de activación (A) se emplea para activar o desactivar al TE, posibilitando al dispositivo conectarse o, cuando no exista actividad, pasar a modo de bajo consumo de potencia. El bit N se fija normalmente a uno binario, pudiéndose usar éste y el bit M para multidelimitación. El bit S se reserva para requisitos futuros de normalización.

El bit en el sentido TE a NT sirve para resolver contenciones, lo que ocurre cuando varios terminales comparten una única línea física (es decir, una línea multipunto). Existen dos tipos de tráfico:

- **Tráfico de canal B:** no se precisa funcionalidad adicional para controlar el acceso a los dos canales B dado que cada canal está dedicado en todo momento a un TE concreto.
- **Tráfico de canal D:** el canal D está disponible para todos los dispositivos de abonado tanto para señalización de control como para transmisión de paquetes, por lo que existe posibilidad de utilizar este canal para otra conexión adicional. Existen dos subtipos:
  - — Tráfico de entrada: el esquema de direccionamiento del nivel de enlace (LAPD) es suficiente para dar salida a cada unidad de datos hacia el destino apropiado.
  - — Tráfico de salida: el acceso se debe regular de modo que sólo transmita un dispositivo al mismo tiempo. Éste es el objetivo del algoritmo de resolución de contención.

El algoritmo de resolución de contención del canal D tiene los siguientes elementos:

- Cuando un dispositivo de abonado no tiene tramas LAPD que transmitir, transmite una serie de unos binarios sobre el canal D. Esto corresponde, haciendo uso del esquema de codificación pseudoternario, a la ausencia de señal en la línea.
- El NT, al recibir un bit del canal D, devuelve el valor binario como un bit de eco del canal D.
- Cuando un terminal está listo para transmitir una trama LAPD, escucha la secuencia de bits de eco del canal D de entrada. Si detecta una cadena de bits 1 de longitud igual a un umbral de valor X_i puede transmitir; en otro caso, el terminal supone que hay otro terminal transmitiendo y espera.
- Puede suceder que varios terminales monitoricen la cadena de eco y comiencen a transmitir al

mismo tiempo, provocando una colisión. Para solucionar este problema el TE transmisor monitoriza los bits E y los compara con sus bits D transmitidos. Si se detecta alguna diferencia, el terminal cesa la transmisión y vuelve al estado de escucha.

Las características eléctricas de la interfaz (por ejemplo, un bit 1 significa ausencia de señal) son tales que cualquier equipo de usuario que transmita un bit 0 prevalecerá sobre un equipo de usuario que transmita un bit 1 al mismo tiempo. Este convenio asegura a un dispositivo la finalización con éxito de su transmisión.

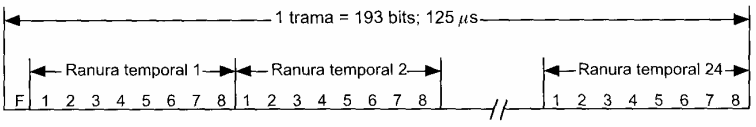
El algoritmo contempla un procedimiento de primitivas de prioridad basado en el umbral de valor X_i. La información de señalización tiene prioridad sobre la información de usuario. En cada una de estas dos clases de prioridad una estación comienza con una prioridad normal, reduciéndose ésta tras una transmisión. Esta prioridad menor se mantiene hasta que todos los otros terminales hayan tenido la oportunidad de transmitir. Los valores de X_i son los siguientes:

- **Información de señalización**
  Prioridad normal $X_1 = 8$
  Prioridad inferior $X_1 = 9$
- **Datos de usuario**
  Prioridad normal $X_2 = 10$
  Prioridad inferior $X_2 = 11$

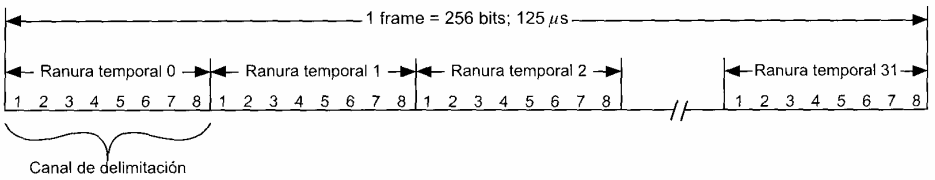
Acceso primario RDSI

La interfaz primaria, al igual que la básica, multiplexa varios canales a través de un único medio de transmisión. En el caso de la interfaz primaria sólo se permite una configuración punto a punto. Generalmente, la interfaz permite la utilización de una PBX digital o de otro dispositivo concentrador que controle varios TE y proporcione servicio TDM síncrono para acceso RDSI. En el acceso primario se definen dos velocidades: 1,544 Mbps y 2,048 Mbps.

La interfaz RDSI a 1,544 Mbps se fundamenta en la estructura de transmisión norteamericana DS-1, usada en el servicio de transmisión T1. En la Figura 8.11a se ilustra el formato de trama para esta velocidad de transmisión. La secuencia de bits se organiza en tramas repetitivas de 193 bits, las cuales cons-



(a) Interfaz a 1,544 Mbps



(b) Interfaz a 2,048 Mbps

Figura 8.11. Formatos de trama para el acceso primario RDSI.

tan de 24 subdivisiones o ranuras temporales de 8 bits más un bit de delimitación usado con fines de sincronización y de gestión. Las mismas ranuras temporales consideradas en las distintas tramas sucesivas constituyen un canal. A una velocidad de 1,544 Mbps las tramas se repiten cada 125 μs; es decir, a razón de 8.000 tramas por segundo. Así, cada canal soporta 64 kbps. Normalmente, la estructura de transmisión se usa para dar cabida a 23 canales B y un canal D a 64 kbps.

La codificación de línea para la interfaz a 1,544 Mbps es AMI (Alternate Mark Inversion) usando B8ZS.

La interfaz RDSI a 2,048 Mbps se basa en la estructura de transmisión europea a esa misma velocidad. En la Figura 8.11b se muestra el formato de trama para esta velocidad de bits. La secuencia de bits se estructura en tramas consecutivas de 256 bits, cada una de las cuales consta de 32 ranuras temporales de 8 bits. La primera ranura se usa con fines de delimitación y sincronización, mientras que las 31 ranuras restantes se usan para albergar canales de usuario. A una velocidad de 2,048 Mbps, las tramas se repiten cada 125 μs, lo que equivale a 8.000 tramas por segundo. Así pues, cada canal permite 64 kbps. Generalmente, la estructura de transmisión da cabida a 30 canales B y un canal D.

Para la interfaz a 2,048 Mbps se utiliza el esquema de codificación de línea AMI con HDB3.

SONET/SDH

La red óptica síncrona (SONET, synchronous optical network) es una interfaz de transmisión óptica propuesta originalmente por BellCore y normalizada por ANSI. ITU-T ha publicado en la recomendación G.707[3] una versión compatible denominada Jerarquía Digital Síncrona (SDH, synchronous digital hierarchy). SONET se ideó para proporcionar una especificación que aproveche las ventajas que proporciona la transmisión digital de alta velocidad a través de fibra óptica.

JERARQUÍA DE SEÑAL

La especificación SONET define una jerarquía de velocidades de datos digitales normalizadas (Tabla 8.4). En el nivel más bajo, denominado STS-1 («synchronous transport signal level 1») u OC-1 («optical ca-

Tabla 8.4. Jerarquía de señal en SONET/SDH.

Nomenclatura SONET	Nomenclatura ITU-T	Velocidad (Mbps)	Velocidad de información útil (Mbps)
STS-1/OC-1		51,84	50,112
STS-3/OC-3	STM-1	155,52	150,336
STS-9/OC-9		466,56	451,008
STS-12/OC-12	STM-4	622,08	601,344
STS-18/OC-18		933,12	902,016
STS-24/OC-24		1.244,16	1.202,688
STS-36/OC-36		1.866,24	1.804,032
STS-48/OC-48	STM-16	2.488,32	2.405,376
STS-96/OC-96		4.876,64	4.810,752
STS-192/OC-192	STM-64	9.953,28	9.621,504

[3] En adelante usaremos el término SONET para referirnos a ambas especificaciones, señalándose explícitamente las diferencias cuando éstas existan.

rrier level 1»)[4], la velocidad es 51,48 Mbps. Esta velocidad se puede usar para transportar una sola señal DS-3 o un grupo de señales a velocidad inferior tales como DS1, DS1C, DS2 y otras velocidades ITU-T (por ejemplo 2,048 Mbps).

Se pueden combinar varias señales STS-1 para formar una señal STS-N. La señal se crea mezclando octetos de *N* señales STS-1 mutuamente sincronizadas.

Para la jerarquía digital síncrona de la ITU-T la velocidad menor es 155,52 Mbps, y se denomina STM-1. Ésta se corresponde con STS-3 de SONET. El motivo de esta discrepancia es que STM-1 es la señal de más baja velocidad que puede alojar una señal de nivel 4 de la ITU-T (139,264 Mbps).

Formato de tramas

El bloque básico en SONET es la trama STS-1, que consta de 810 octetos y se transmite a razón de una cada 125 μs, dando lugar a una velocidad total de 51,84 Mbps (Figura 8.12a). La trama se puede ver desde un punto de vista lógico como una matriz de 9 filas de 90 octetos cada una, transmitiéndose por filas de izquierda a derecha y de arriba abajo.

Las tres primeras columnas (3 octetos × 9 filas = 27 octetos) de la trama son octetos suplementarios. Nueve de ellos están dedicados a información suplementaria relacionada con las secciones y los otros 18 se dedican a información suplementaria de línea. En la Figura 8.13a se muestra la disposición de los octetos suplementarios, definiéndose los distintos campos en la Tabla 8.5.

El resto de la trama es información útil, también denomina carga útil. Ésta incluye una columna de información suplementaria relacionada con la ruta, que no ocupa necesariamente la primera columna disponible; la información suplementaria de línea contiene un puntero que indica dónde comienza la información suplementaria de ruta. En la Figura 8.13b se muestra la disposición de los octetos suplementarios de ruta, definiéndose éstos en la Tabla 8.5.

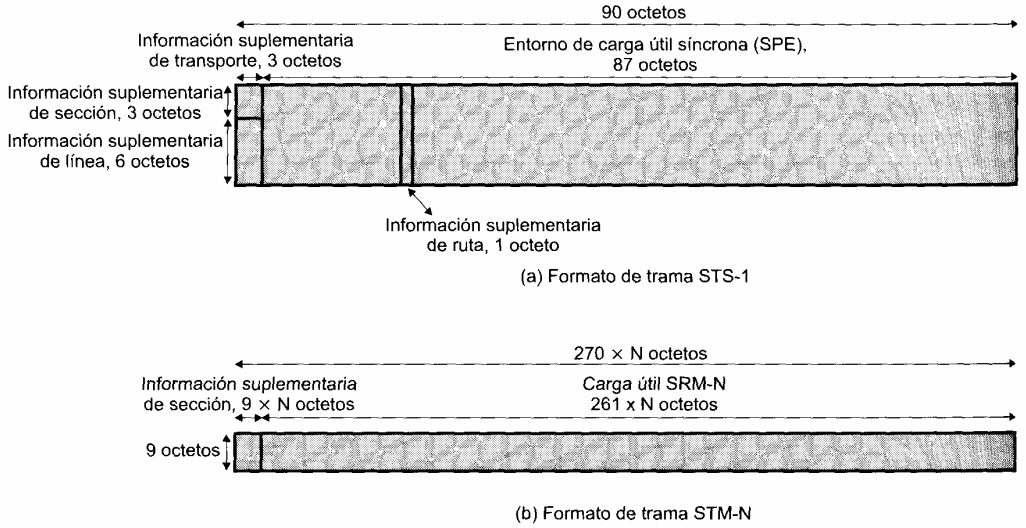


Figura 8.12. Formatos de trama SONET/SDH.

[4] Una velocidad OC-N es el equivalente a una señal eléctrica STS-N. Los dispositivos de usuario finales transmiten y reciben señales eléctricas, las cuales deben convertirse a y desde señales ópticas para transmisión a través de fibras ópticas.

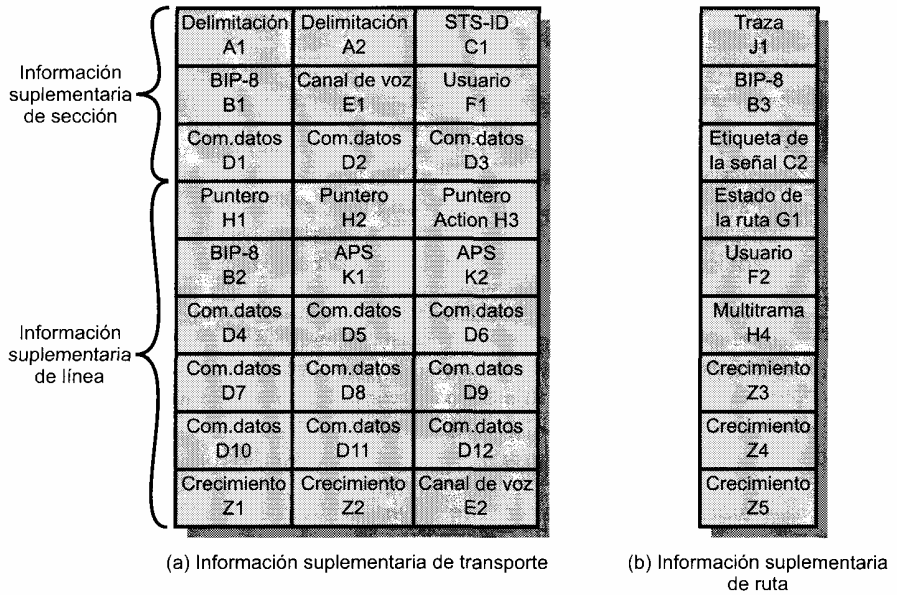


Figura 8.13. Octetos de información suplementaria en STS-1 de SONET.

La Figura 8.12b muestra el formato general para tramas de velocidad superior usando la nomenclatura de la ITU-T.

Tabla 8.5. Bits de información suplementaria en STS-1.

Información suplementaria de sección	
A1, A2:	Octetos de delimitación = F6,28 HEX; usados para sincronizar el comienzo de cada trama.
C1:	STS-1 ID identifica el número STS-1 (de 1 a N) para cada STS-1 en un multiplexor STS-N.
B1:	Octeto de paridad de la mezcla de bits («bit-interleaved parity»); se usa paridad par sobre la trama STS-1 anterior tras la mezcla; el bit *i*-ésimo de este octeto contiene el resultado de una operación de paridad par entre los bits de posición *i*-ésima de todos los octetos de la trama previa.
E1:	Este octeto a nivel de sección proporciona 64 kbps PCM; canal de voz de 64 kbps opcional a usar entre equipos terminales, concentradores y terminales remotos.
F1:	Canal a 64 kbps independiente para necesidades de usuario.
D1-D3:	Canal de comunicaciones de datos a 192 kbps para alarmas, mantenimiento, control y administración entre secciones.
Información suplementaria de línea	
H1-H3:	Octetos de puntero para el alineamiento de trama y ajuste de la frecuencia de los datos correspondientes a la carga útil.
B2:	Paridad de la mezcla de bits para monitorizar errores a nivel de línea.
K1, K2:	Dos octetos reservados para la señalización entre equipos de conmutación con protección automática a nivel de línea; se utiliza un protocolo orientado a bit que proporciona protección de errores y gestión del enlace óptico SONET.
D4-D12:	Canal de comunicaciones de datos a 576 kbps para alarmas, mantenimiento, control, monitorización y administración a nivel de línea.
Z1, Z2:	Reservados para uso futuro.
E2:	Canal de voz PCM a 64 kbps para a nivel de línea.

Tabla 8.5. *(Continuación)*

Información suplementaria de ruta	
J1:	Canal a 64 kbps usado para enviar repetidamente una cadena de longitud fija de 64 octetos de modo que un terminal receptor pueda verificar continuamente la integridad de una ruta; el contenido del mensaje es programable por el usuario.
B3:	Paridad de mezcla de bits a nivel de ruta, calculada sobre todos los bits del SPE previo.
C2:	Etiqueta de la señal de ruta STS que se utiliza para distinguir entre señales equipadas y no equipadas. *No equipadas* significa que la conexión de línea está completa pero no existen datos acerca de la ruta para enviar. En las señales equipadas, la etiqueta puede indicar una correspondencia específica para la información útil STS, necesaria para que los terminales receptores la interpreten correctamente.
G1:	Octeto de estado enviado desde el equipo de destino de la ruta al equipo origen de la misma para comunicar su estado así como las prestaciones de los errores en la ruta.
F2:	Canal de 64 kbps para el usuario de la ruta.
H4:	Indicador de multitrama para cargas útiles que requieran tramas de mayor longitud que una sola STS; los indicadores de multitrama se emplean cuando se empaquetan canales a velocidades inferiores (afluentes virtuales) en el SPE.
Z3-Z5:	Reservados para usos futuros.

8.3. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO ESTADÍSTICA

CARACTERÍSTICAS

En un multiplexor por división en el tiempo síncrono es usual que se desaprovechen muchas de las ranuras temporales dentro de una trama. Una aplicación típica de la TDM síncrona es la conexión de varios terminales a un puerto compartido de computador. Incluso en el caso de que todos los terminales se estén utilizando activamente, la mayor parte del tiempo no existe transferencia de datos en ningún terminal.

Una alternativa a la técnica TDM síncrona es TDM estadística. El multiplexor estadístico explota esta propiedad usual en la transmisión de datos mediante la reserva dinámica bajo demanda de las ranuras o divisiones temporales. Al igual que en TDM síncrona, el multiplexor estadístico tiene varias líneas de entrada/salida por un lado y una línea multiplexada de velocidad superior por otro. Cada línea de entrada/salida tiene asociada una memoria temporal. En el caso del multiplexor estadístico hay n líneas de entrada/salida, pero sólo k, con $k < n$, ranuras temporales disponibles en cada trama TDM. La función de entrada del multiplexor consiste en sondear las memorias de almacenamiento de entrada aceptando datos hasta que se complete una trama, enviándola posteriormente. A la salida, el multiplexor recibe la trama y distribuye las ranuras temporales de datos a las memorias temporales de salida correspondientes.

Dado que la técnica TDM estadística presenta la ventaja de que los dispositivos conectados no transmiten durante todo el tiempo, la velocidad de la línea multiplexada es menor que la suma de las velocidades de los dispositivos conectados. Así, un multiplexor estadístico puede usar una velocidad inferior para dar servicio a un número de dispositivos igual al soportado por un multiplexor síncrono. O dicho de otra forma, si un multiplexor estadístico y uno síncrono usan un enlace a la misma velocidad, el multiplexor estadístico puede dar servicio a más dispositivos.

En la Figura 8.14 se comparan las técnicas TDM síncrona y estadística. En la figura se consideran cuatro fuentes de datos así como los datos generados en cuatro intervalos de tiempo (t_0, t_1, t_2, t_3). En el caso del multiplexor síncrono se tiene una velocidad de salida efectiva de cuatro veces la velocidad de cualquiera de los dispositivos de entrada. Durante cada intervalo, los datos se toman de las cuatro fuen-

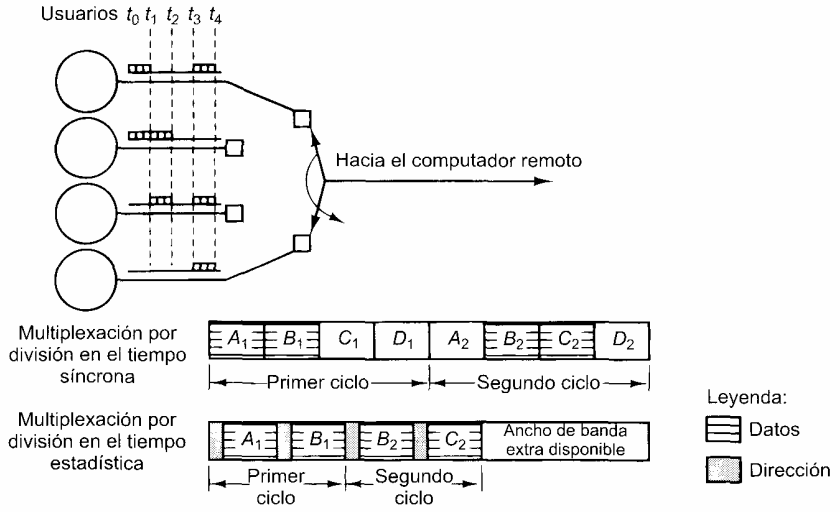


Figura 8.14. Comparación de las técnicas TDM síncrona y estadística.

tes y posteriormente se envían. Por ejemplo, en el primer intervalo las fuentes C y D no producen datos, de modo que dos de las cuatro ranuras temporales transmitidas por el multiplexor se encuentran vacías.

Por el contrario, el multiplexor estadístico no envía ranuras temporales vacías mientras haya datos que enviar. Así, durante el primer intervalo sólo se envían la ranuras de *A* y *B*. Ahora bien, con este esquema se pierde el significado posicional de las ranuras. Es decir, no se sabe a priori qué fuente de datos utilizará cada ranura. Luego, dado que los datos se reciben desde y se distribuyen hacia las líneas de entrada/salida de forma impredecible, se precisa información de direccionamiento para asegurar que el envío se realiza de forma apropiada. Por tanto, en el caso de la técnica TDM estadística existe más información suplementaria por ranura ya que cada una de ellas transporta una dirección además de los datos propiamente dichos.

La estructura de trama usada por un multiplexor estadístico repercute en las prestaciones finales del mismo. Es claro que resulta deseable minimizar la cantidad de bits suplementarios con objeto de mejorar la eficiencia. En general, un sistema TDM estadístico usa un protocolo síncrono tal como HDLC. Dentro de una trama HDLC, la trama de datos debe contener bits de control para el proceso de multiplexación. En la Figura 8.15 se muestran dos formatos posibles. En el primer caso sólo se incluye una fuente de datos por trama. Esta fuente se identifica mediante una dirección. La longitud del campo de datos es variable, marcándose su final por el final de toda la trama. Este esquema puede funcionar adecuadamente para baja carga pero resulta bastante ineficiente en condiciones de alta carga.

Una forma de mejorar la eficiencia consiste en permitir que se empaqueten varias fuentes de datos en una misma trama. En este caso es necesario, sin embargo, algún procedimiento para especificar la longitud de los datos de cada una de las fuentes. De este modo, la subtrama TDM estadística consta de una secuencia de campos de datos, cada uno de ellos etiquetado con una dirección y una longitud. Pueden usarse varias técnicas para hacer aún más eficiente esta aproximación. El campo de dirección se puede reducir a través del uso de direcciones relativas; es decir, cada dirección especifica el número de la fuente actual relativa a la anterior, módulo el número total de fuentes. Así, por ejemplo, en lugar de un campo de dirección de 8 bits bastaría con uno de 4 bits.

Otra mejora es el uso de una etiqueta de dos bits con el campo de longitud. Un valor de 00, 01 ó 10 corresponden con un campo de datos de uno, dos o tres octetos, no siendo necesario considerar un campo de longitud. Un valor 11 indicaría que se incluye el campo de longitud.

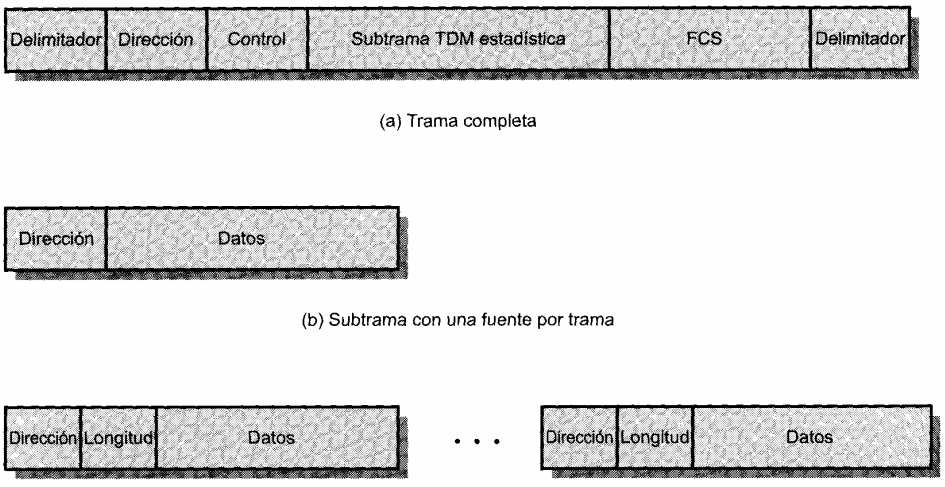


Figura 8.15. Formatos de trama en TDM estadística.

PRESTACIONES

Ya se ha mencionado que la velocidad de salida en un multiplexor estadístico es menor que la suma de las velocidades de las entradas. Esto está permitido dado que se supone que la cantidad media de entrada es menor que la capacidad de la línea multiplexada. El problema de este enfoque es que, aunque la entrada conjunta promedio puede ser menor que la capacidad de la línea multiplexada, puede haber periodos pico en los que la entrada exceda la capacidad.

La solución a este problema consiste en incluir una memoria temporal en el multiplexor para almacenar temporalmente el exceso de datos de entrada. En la Tabla 8.6 se da un ejemplo del comportamiento de este tipo de sistemas. Se suponen 10 fuentes, cada una de ellas con una capacidad de 1.000 bps, y que la entrada media por fuente es el 50 % del máximo. Así, en promedio, la carga de entrada es 5.000 bps. Se consideran dos casos: multiplexores con capacidad de salida de 5.000 bps y de 7.000 bps. Las entradas en la tabla mencionada muestran el número de bits de entrada procedentes de cada uno de los 10 dispositivos por cada milisegundo y la salida del multiplexor. Cuando la entrada excede la salida, el exceso se debe almacenar temporalmente.

Existe un compromiso entre el tamaño de la memoria temporal usada y la velocidad de la línea. Sería deseable usar tanto la memoria como la velocidad menores posibles, pero una reducción en uno de estos parámetros requiere el incremento del otro. Téngase en cuenta que el deseo de reducir el tamaño de la memoria temporal no se debe al coste de ésta —la memoria es barata—, sino al hecho de que a más cantidad de memoria mayor es el retardo. Por tanto, el compromiso real está entre el tiempo de respuesta del sistema y la velocidad de la línea multiplexada. En esta sección se presentan algunas medidas aproximadas para evaluar este compromiso. Estas medidas son suficientes para la mayoría de las situaciones.

Definamos los siguientes parámetros para un multiplexor por división en el tiempo estadístico:

I = número de fuentes de entrada

R = velocidad de cada fuente, en bps

M = capacidad efectiva de la línea multiplexada, en bps

Tabla 8.6. Ejemplo de las prestaciones de un multiplexor estadístico.

	Capacidad = 5.000 bps		Capacidad = 7.000 bps	
Entrada[a]	Salida	Exceso	Salida	Exceso
6	5	1	6	0
9	5	5	7	2
3	5	5	5	0
7	5	5	7	0
2	5	2	2	0
2	4	0	2	0
2	2	0	2	0
3	3	0	3	0
4	4	0	4	0
6	5	1	6	0
1	2	0	1	0
10	5	5	7	3
7	5	7	7	3
5	5	7	7	1
8	5	10	7	2
3	5	8	5	0
6	5	9	6	0
2	5	6	2	0
9	5	10	7	2
5	5	10	7	0

[a] Entrada = 10 fuentes, 1.000 bps/fuente; velocidad de entrada promedio = 50% del máximo.

α = fracción media de tiempo que transmite cada fuente, $0 < \alpha < 1$

$K = \dfrac{M}{IR}$ = razón entre la capacidad de la línea multiplexada y la entrada máxima total

El parámetro M se ha definido teniendo en consideración los bits suplementarios incluidos por el mutiplexor; es decir, M representa la velocidad máxima a la que se pueden transmitir los bits de datos.

El parámetro K es una medida de la compresión alcanzada por el multiplexor. Por ejemplo, para una capacidad M dada, si $K = 0{,}25$ se gestionan, utilizando la misma capacidad de enlace, cuatro veces más dispositivos que mediante un multiplexor por división en el tiempo síncrono. El valor de K se puede acotar por:

$$\alpha < K < 1$$

Un valor de $K = 1$ corresponde a un multiplexor por división en el tiempo síncrono, ya que el sistema tiene capacidad para servir todos los dispositivos de entrada al mismo tiempo. Si $K < \alpha$, la entrada excederá la capacidad del multiplexor.

Se pueden obtener algunos resultados considerando al multiplexor como una cola atendida por un solo servidor. Se alcanza una situación de cola cuando un servicio recibe un «cliente» y, al encontrarlo ocupado, tiene que esperar. El retardo sufrido por el cliente de un servicio es el tiempo de espera en la cola más el tiempo de servicio. El retardo depende del patrón de tráfico de llegada y de las características del servidor. En la Tabla 8.7 se resumen los resultados para una distribución de llegadas aleatorias (Poisson) y un tiempo de servicio constante. Este modelo se puede relacionar fácilmente con el multiplexor estadístico:

$$\lambda = \alpha IR$$

$$T_s = \frac{1}{M}$$

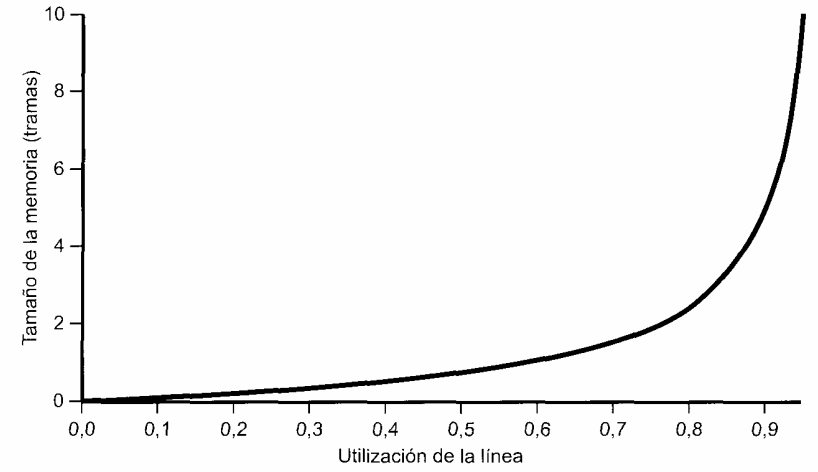
La velocidad de llegada promedio λ en bps es igual a la entrada potencial total (IR) multiplicada por la fracción de tiempo α con que transmite cada fuente. El tiempo de servicio T_s, en segundos, es el tiempo empleado en transmitir un bit, que es $1/M$. Obsérvese que

$$\rho = \lambda T_s = \frac{\alpha IR}{M} = \frac{\alpha}{K} = \frac{\lambda}{M}$$

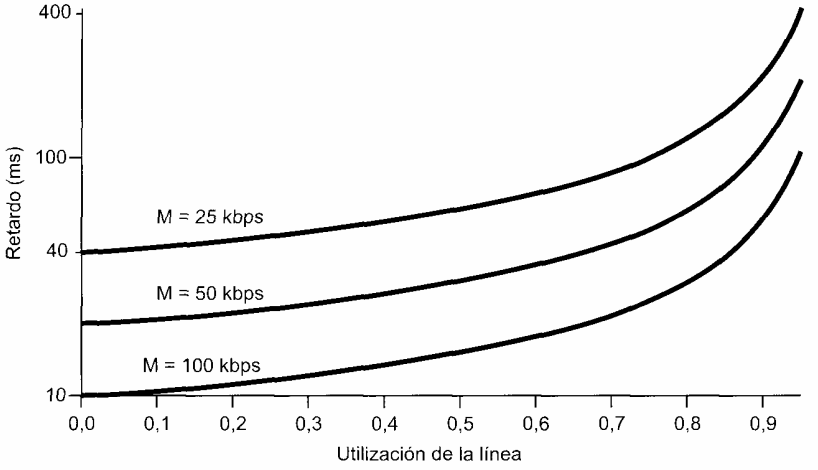
El parámetro ρ es la utilización o fracción de capacidad total del enlace utilizado. Por ejemplo, si la capacidad M es 50 kbps y $\rho = 0{,}5$, la carga del sistema es 25 kbps. El parámetro N en la Tabla 8.7 es una medida de la capacidad de memoria temporal utilizada por el multiplexor. Por último, T_r es una medida del retardo promedio sufrido por una fuente de entrada.

Tabla 8.7. Colas de un único servidor con tiempos de servicio constantes y distribución de llegadas de tipo poisson (aleatorias).

Parámetros
λ = número medio de llegadas por segundo T_s = tiempo de servicio para cada llegada ρ = utilización; fracción de tiempo que está ocupado el servidor N = número medio de «clientes» en el sistema (en espera y siendo servidos) T_r = tiempo de estancia; tiempo medio que un «cliente» pasa en el sistema (en espera y siendo servido) σ_r = desviación estándar de T_r
Fórmulas
$\rho = \lambda T_s$ $N = \frac{\rho^2}{2(1-\rho)} + \rho$ $T_r = \frac{T_s(2-\rho)}{2(1-\rho)}$ $\sigma_r = \frac{1}{1-\rho}\sqrt{\rho - \frac{3\rho^2}{2} + \frac{5\rho^3}{6} - \frac{\rho^4}{12}}$



(a) Tamaño medio de la memoria frente a utilización



(b) Retardo medio frente a utilización

Figura 8.16. Tamaño de la memoria temporal y retardo para un multiplexor estadístico.

La Figura 8.16 puede aclarar conceptualmente el compromiso entre el tiempo de respuesta del sistema y la velocidad de la línea multiplexada. Se supone que los datos se transmiten en tramas de 1.000 bits. En la parte (a) de la figura se representa el número medio de tramas que se deben almacenar temporalmente en función de la utilización media de la línea multiplexada. Así, si la carga de entrada media es de 5.000 bps, la utilización es del 100 % para una línea con una capacidad de 5.000 bps y en torno al 71 % para una línea de 7.000 bps de capacidad. En la parte (b) de la figura se muestra el retardo medio experimentado por una trama en función de la utilización y de la velocidad de datos. Se observa que a medida que crece la utilización lo hacen también los requisitos de almacenamiento temporal y el retardo. Resulta claramente no deseable una utilización por encima del 80 %.

Obsérvese que el tamaño promedio para la memoria temporal sólo depende de ρ, y no directamente de M. Por ejemplo, considérense los dos siguientes casos:

Caso I	Caso II
l = 10 R = 100 bps α = 0,4 M = 500 bps	l = 100 R = 100 bps α = 0,4 M = 5.000 bps

En ambos el valor de ρ es 0,8 y el tamaño medio de la memoria temporal es N = 2,4. Así, proporcionalmente, para multiplexores que gestionan un número elevado de fuentes se requiere una menor cantidad de memoria por fuente. En la Figura 8.16b se muestra también que el retardo promedio, para una utilización constante, será menor a medida que aumente la capacidad del enlace.

Hasta ahora se ha considerado la longitud promedia de cola y, en consecuencia, el tamaño medio de la memoria temporal necesaria. Es claro que existirá un límite máximo para el tamaño de memoria temporal disponible. La variación del tamaño de la cola aumenta con la utilización. Así, a mayor nivel de utilización mayor será la memoria necesaria para gestionar el exceso. Incluso así, existe posibilidad de que la memoria temporal se desborde. En la Figura 8.17 se muestra la fuerte dependencia de la probabilidad de desbordamiento de la memoria temporal con la utilización. Esta figura, junto con la Figura 8.16, sugiere que no es deseable una utilización por encima del 0,8.

8.4. LÍNEA DE ABONADO DIGITAL ASIMÉTRICA

La parte que supone un mayor desafío en la implementación y desarrollo de una red digital pública de área amplia de alta velocidad es el enlace entre el abonado y la red: la línea de abonado digital. Dada la existencia de miles de millones de abonados potenciales en todo el mundo, la sola idea de llevar a cabo

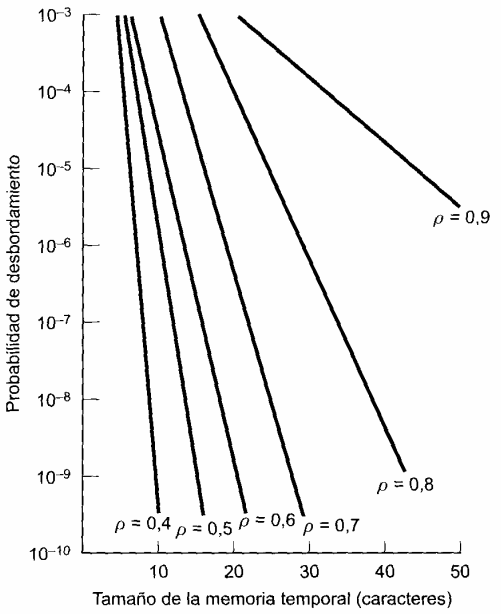


Figura 8.17. Probabilidad de desbordamiento de la memoria temporal en función de su tamaño.

la instalación de un nuevo cable para cada uno de los usuarios asusta. En lugar de ello, los diseñadores de red han estudiado distintas formas de aprovechar el cable de par trenzado ya instalado y que enlaza con redes telefónicas prácticamente a todos los consumidores particulares y de empresa. Estos enlaces fueron instalados para transportar señales de voz en un ancho de banda de cero a 4 kHz. Sin embargo, los cables son capaces de transmitir señales con un espectro mucho más amplio – 1MHz o más.

ADSL es la más conocida de una nueva familia de tecnologías modem diseñada para permitir transmisión de datos digitales de alta velocidad a través de cable telefónico convencional. ADSL está siendo ofrecida por varios proveedores y se encuentra definida en una normalización ANSI. En esta sección se verá en primer lugar el diseño completo de ADSL, tras lo cual se presentarán los fundamentos de la tecnología subyacente conocida como DMT.

DISEÑO ADSL

El término *asimétrico* se refiere al hecho de que ADSL proporciona más capacidad de transmisión en el enlace descendente (desde la oficina central del proveedor hacia el usuario) que en el ascendente (desde el usuario hacia el proveedor). ADSL se orientó originalmente hacia las necesidades de recursos previstas en aplicaciones de vídeo bajo demanda y servicios relacionados. A pesar de que este tipo de aplicaciones no se ha materializado, la demanda de acceso a Internet de alta velocidad ha crecido desde la aparición de la tecnología ADSL. En general, el usuario precisa mayor capacidad en el enlace descendente que para la transmisión ascendente. La mayor parte de las transmisiones realizadas por un usuario son del tipo de pulsaciones de teclado o transmisión de mensajes cortos de correo electrónico, mientras que el tráfico de entrada, especialmente el tráfico web, puede conllevar grandes cantidades de datos que incluyen imágenes e incluso vídeo. Es por ello que la tecnología ADSL resulta muy apropiada para las necesidades de transmisión en Internet.

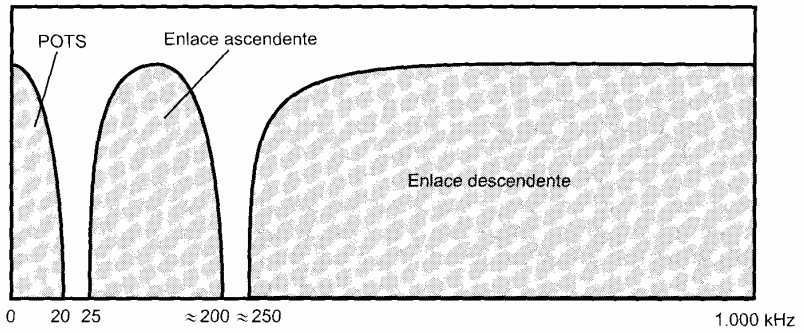
ADSL hace uso de modulación por división en frecuencias (FDM) de una forma novedosa para aprovechar la capacidad de 1 MHz de que dispone el cable de par trenzado. Existen tres elementos en la estrategia ADSL (Figura 8.18):

- Reserva de los 25 kHz inferiores para voz, conocido como POST («Plain Old Telephone Service»). La voz se transmite sólo en la banda 0-4 kHz, sirviendo el ancho de banda adicional para evitar la producción de diafonía entre los canales de voz y de datos.
- Utilización de cancelación de eco[5] o de FDM para dar cabida a dos bandas, una ascendente y otra banda descendente a frecuencia más elevada.
- Uso de FDM en las bandas ascendente y descendente. En este caso, una secuencia de bits dada se divide en varias secuencias paralelas y cada una de ellas se transmite en una banda de frecuencias distinta.

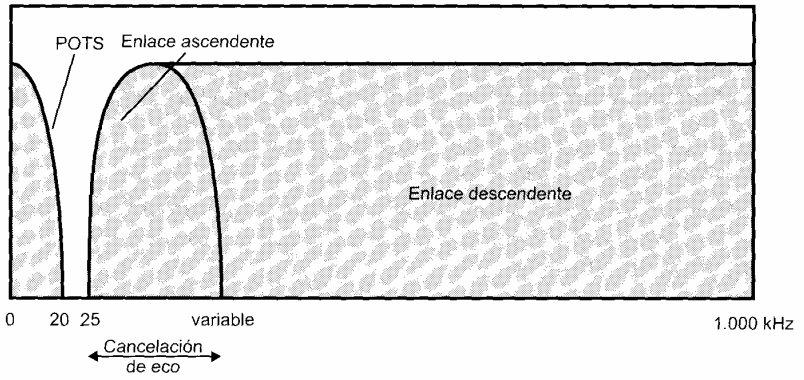
Cuando se usa cancelación de eco, la banda de frecuencia correspondiente al canal ascendente se solapa con la porción inferior del canal descendente. Este hecho presenta dos ventajas en comparación con el empleo de bandas de frecuencia distintas para los enlaces ascendente y descendente.

- La atenuación aumenta con la frecuencia. Con la utilización de cancelación de eco, la mayor parte del ancho de banda del enlace descendente se encuentra en la zona «adecuada» del espectro.
- El diseño del procedimiento de cancelación de eco es más flexible para modificar la capacidad de la transmisión ascendente. Aunque este canal se puede extender hacia frecuencias superiores sin llegar a caer dentro del ancho de banda del canal descendente, lo que se hacer es aumentar el área de solapamiento.

[5] La cancelación de eco es una técnica de procesamiento de señal que permite la transmisión de señales digitales en ambos sentidos de forma simultánea a través de una misma línea de transmisión. En esencia, un transmisor debe eliminar de la señal que recibe el eco debido a su propia transmisión con objeto de recuperar la señal enviada por el otro extremo.



(a) Multiplexación por división en frecuencias



(b) Cancelación de eco

Figura 8.18. Configuración de canales ADSL.

La desventaja del uso de la cancelación de eco es la necesidad de la existencia de lógica de cancelación de eco en ambos extremos de la línea.

El esquema ADSL permite distancias de hasta 5,5 km en función del diámetro del cable y de la calidad de éste. Esto resulta suficiente para dar servicio en torno al 95 por ciento de todas las líneas de abonado de Estados Unidos y del mismo orden en otros países.

MULTITONO DISCRETO

La técnica de multitono discreto (DMT) consiste en hacer uso de varias señales portadora a diferentes frecuencias, de modo que se envían algunos de los bits en cada canal. El ancho de banda disponible (ascendente o descendente) se divide en varios subcanales de 4 kHz. En el proceso de iniciación, el modem DMT envía señales de test sobre los subcanales con el fin de determinar la relación señal-ruido en cada uno de ellos. Realizado el test, el modem asigna más bits de datos a los canales con mejor calidad de transmisión de señal y un número de bits menor para aquellos canales de calidad inferior. En la Figura 8.19 se ilustra este proceso. Cada subcanal puede transportar datos a una velocidad de entre 0

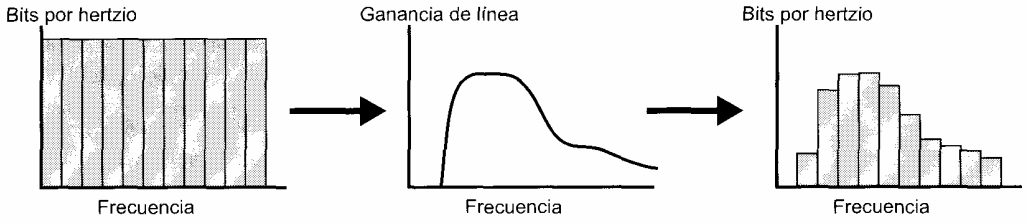


Figura 8.19. Reserva de bits DMT por canal.

y 60 kbps. La figura muestra una situación típica en la que existe un aumento de la atenuación y, por tanto, un decremento en la relación señal-ruido a altas frecuencias. En consecuencia, los subcanales de frecuencia superior transportan menos datos.

En la Figura 8.20 se ofrece un diagrama general de la transmisión DMT. Tras el proceso de inicio, la secuencia de bits a transmitir se divide en varias subsecuencias, una para cada subcanal que transportará datos. La suma de las velocidades de las subsecuencias es igual a la velocidad total. A continuación, cada subsecuencia se convierte en una señal analógica mediante la técnica de modulación en amplitud por cuadratura (QAM) descrita en el Capítulo 5. Este esquema funciona adecuadamente dada la capacidad de QAM para asignar a cada una de las señales transmitidas un número diferente de bits. Cada señal QAM ocupa una banda de frecuencia diferente, de modo que estas señales se pueden combinar sin más que sumarlas para dar lugar a la señal compuesta a transmitir.

Los diseños ADSL/DMT actuales utilizan 256 subcanales descendentes. En teoría, con cada subcanal de 4 kHz que transporta 60 kbps sería posible transmitir a una velocidad de 15,36 Mbps. En cambio, en la práctica, el deterioro de la transmisión impide la consecución de esta velocidad. Las implementaciones actuales operan en el rango 1,5-9 Mbps dependiendo de la distancia de la línea y de la calidad de ésta.

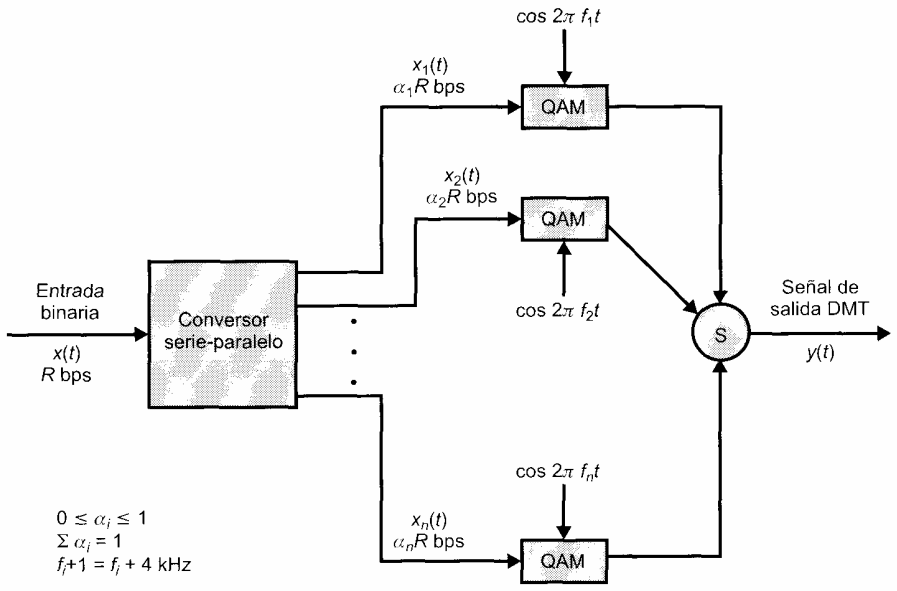


Figura 8.20. Transmisor DMT.

8.5. xDSL

ADSL es uno de los numerosos esquemas de reciente aparición para proporcionar una transmisión digital de alta velocidad del bucle de abonado. En la Tabla 8.8 se resumen y comparan algunos de los más importantes de estos nuevos esquemas, que se denominan de forma genérica xDSL.

LÍNEA DE ABONADO DIGITAL DE ALTA VELOCIDAD

HDSL se desarrolló a finales de los años 80 por BellCore con objeto de ofrecer una forma más efectiva, desde el punto de vista del coste, para el envío de datos a la velocidad proporcionada por T1 (1,544 Mbps). La línea estándar T1 usa codificación AMI, que ocupa un ancho de banda de alrededor de 1,5 MHz. Debido a la aparición de estas altas frecuencias, las características de atenuación limitan el uso de T1 para distancias en torno a 1 km entre repetidores. Por tanto, para muchas de las líneas de abonado se precisan uno o más repetidores, lo cual encarece la instalación y su mantenimiento.

En HDSL se hace uso del esquema de codificación 2B1Q para poder alcanzar una velocidad de datos de hasta 2 Mbps a través de dos líneas de par trenzado dentro de un ancho de banda que se extiende sólo hasta 196 kHz aproximadamente. Para conseguir esto se trabaja con distancias en torno a 3,7 km.

LÍNEA DE ABONADO DIGITAL DE LÍNEA SIMPLE

Aunque HDSL resulta atractiva para reemplazar las líneas T1 existentes, no es posible para abonados particulares ya que en HDSL se precisan dos pares trenzados y estos abonados disponen generalmente de un solo par. Así, SDSL se desarrolló para proporcionar a través de una única línea de par trenzado el mismo tipo de servicio que HDSL proporciona con dos. Como en el caso de HDSL, en SDSL se usa la técnica de codificación 2B1Q. Se emplea cancelación de eco para conseguir transmisión *full-duplex* a través de un único par.

Tabla 8.8. Comparación de las técnicas xDSL.

	ADSL	HDSL	SDSL	VDSL
Bits/segundo	de 1,5 a 9 Mbps en descendente de 16 a 640 kbps en ascendente	1,544 o 2,048 Mbps	1,544 o 2,048 Mbps	de 13 a 52 Mbps en descendente de 1,5 a 2,3 Mbps en ascendente
Modo	Asimétrico	Simétrico	Simétrico	Asimétrico
Pares de cobre	1	2	1	1
Distancia (UTP de calibre 24)	de 3,7 a 5,5 km	3,7 km	3,0 km	1,4 km
Señalización	Analógica	Digital	Digital	Analógica
Código de línea	CAP/DMT	2B1Q	2B1Q	DMT
Frecuencia	de 1 a 5 MHz	196 kHz	196 kHz	10 MHz
Bits/ciclo	Variable	4	4	Variable

UTP = par trenzado sin apantallar.

LÍNEA DE ABONADO DIGITAL DE MUY ALTA VELOCIDAD (VDSL)

Uno de los más recientes esquemas xDSL es VDSL. Muchos de los detalles de esta especificación de señalización se encuentran aún por definir en el momento de la escritura de este texto. El objetivo de VDSL es proveer un esquema similar a ADSL a una velocidad muy superior a costa de disminuir la distancia permitida. La técnica de señalización para VDSL será probablemente DMT/QAM.

VDSL no utiliza cancelación de eco pero proporciona bandas separadas para los diferentes servicios, siendo la asignación provisional para cada uno de ellos la siguiente:

- POTS: 0-4 kHz
- RDSI: 4-80 kHz
- Enlace ascendente: 300-700 kHz
- Enlace descendente: $\geqslant 1$ MHz

8.6. LECTURAS Y SITIOS WEB RECOMENDADOS

En [BELL90] y [FREE98] puede encontrarse un estudio sobre los sistemas de transmisión TDM y FDM. Por su parte, en [STAL99] se tratan en mayor profundidad las interfaces RDSI y SONET.

El texto [CIOF97] proporciona un excelente estudio sobre ADSL; un buen artículo sobre este tema es también [MAXW96]. Finalmente, se recomiendan [HAWL97] y [HUMP97] por el tratamiento de las técnicas xDSL que en ellos se hace.

BELL90 Bellcore (Bell Communications Research). *Telecommunications Transmission Engineering*. Three volumes. 1990.

CIO97 Cioffi, J. «Asymmetric Digital Subscriber Lines.» in Gibson, J., ed. *The Communications Handbook*. Boca Raton, FL: CRC Press, 1997.

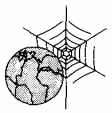
HAWL97 Hawley, G. «Systems Considerations for the Use of xDSL Technology for Data Access.» *IEEE Communications Magazine*, March 1997.

HUMP97 Humphrey, M., y Freeman, J. «How xDSL Supports Broadband Services to the Home.» *IEEE Network*, January/March 1997.

FREE98 Freeman, R. *Telecommunications Transmission Handbook*. New York: Wiley, 1998.

MAXW96 Maxwell, K. «Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years.» *IEEE Communications Magazine*, October 1996.

STAL99 Stallings, W. *ISDN and Broadband ISDN, with Frame Relay and ATM*. Upper Saddle River, NJ: Prentice Hall, 1999.



SITIOS WEB RECOMENDADOS

- **Foro ADSL:** incluye una FAQ e información técnica sobre especificaciones del Foro ADSL.
- **ADSL universal:** página principal del Universal ADSL Working Group, consorcio industrial que promueve el acceso ADSL de alta velocidad a bajo coste por parte de usuarios particulares.
- **Foro de interoperabilidad SONET:** presenta productos, tecnología y estándares actuales.
- **Página principal de SONET:** enlaces de interés, artículos especializados, informes oficiales y preguntas planteadas habitualmente (FAQ, frequently asked questions).

8.7. PROBLEMAS

8.1. Se multiplexa y transmite la información correspondiente a cuatro señales analógicas a través de un canal telefónico con una banda de paso de 400 a 3.100 Hz. Cada una de las señales analógicas en banda base está limitada en banda hasta 500 Hz. Diseñe un sistema de comunicaciones (a nivel de diagrama de bloques) que permita la transmisión de estas cuatro fuentes a través del canal telefónico haciendo uso de:

a) Multiplexación por división en frecuencias con subportadoras SSB (banda lateral única, «single sideband»).

b) Multiplexación por división en el tiempo usando PCM.
Muestre los diagramas de bloques del sistema completo en ambos casos, incluyendo las partes de transmisión, canal y recepción. Incluya los anchos de banda de las señales en los distintos puntos del sistema.

8.2. Parafraseando a Lincoln, «... todo el canal durante algún tiempo, parte del canal durante todo el tiempo...». Relacione esta frase con la Figura 8.2.

8.3. Considere un sistema de transmisión que hace uso de multiplexación por división en frecuencias. ¿Qué factores de coste se verán afectados al añadir uno o más pares de estaciones al sistema?

8.4. En TDM síncrona es posible entremezclar los bits, considerando para ello un bit de cada canal en el ciclo. Si los canales usan un código de auto-reloj (es decir, la señal de reloj está contenida en el propio código) para facilitar la sincronización, ¿podría esta mezcla de bits introducir problemas dado que no existe una secuencia continua de bits procedente de una fuente?

8.5. ¿Por qué se pueden eliminar los bits de comienzo y de parada cuando se usa mezcla de caracteres en TDM síncrona?

8.6. Explique desde el punto de vista del control de enlace de datos y de la capa física cómo se realizan el control de flujo y el control de errores en la multiplexación por división en el tiempo síncrona.

8.7. Uno de los 193 bits en el formato de transmisión DS-1 se usa para sincronización de trama. Explique su funcionamiento.

8.8. ¿Cuál es la velocidad de datos de la señal de control para cada canal de voz en el formato DS-1?

8.9. Se multiplexan y transmiten 24 señales de voz a través de un par trenzado. ¿Cuál es el ancho de banda necesario en FDM? Suponiendo una eficiencia del ancho de banda (relación entre la velocidad de datos y el ancho de banda de la transmisión, ya explicada en el Capítulo 5) de 1 bps/Hz, ¿cuál es el ancho de banda necesario para TDM haciendo uso de PCM?

8.10. Dibuje un diagrama de bloques similar al de la Figura 8.8 para un sistema TDM PCM que dé cabida a cuatro entradas digitales síncronas a 300 bps y una entrada analógica con un ancho de banda de 500 Hz. Suponga que las muestras analógicas se codifican en palabras PCM de 4 bits.

8.11. Se utiliza un multiplexor por división en el tiempo con mezcla de caracteres para combinar las secuencias de datos procedentes de varios terminales asíncronos a 110 bps para transmisión de datos sobre una línea digital de 2.400 bps. Cada terminal envía caracteres asíncronos de 7 bits de datos, 1 bit de paridad, 1 bit de comienzo y 2 bits de parada. Suponga que se envía un carácter de sincronización cada 19 caracteres de datos y que al menos el 3 por ciento de la capacidad de la línea se reserva para la inserción de pulsos con objeto de acomodar las variaciones de velocidad de los distintos terminales.

a) Determine el número de bits por carácter.

b) Determine el número de terminales que puede servir el multiplexor.

c) Obtenga un posible patrón de delimitación para el multiplexor.

8.12. Encuentre el número de dispositivos, especificados a continuación, que puede atender una línea TDM de tipo T1 si el 1 % de la capacidad de la línea se reserva con fines de sincronización.

a) Terminales teletipo de 110 bps.

b) Terminales de computador de 300 bps.

c) Terminales de computador de 1.200 bps.

d) Puertos de salida de computador a 9.600 bps.

e) Líneas de voz PCM de 64 kbps.

¿Cómo variaría este número si cada una de las fuentes estuviese operativa en promedio el 10 % del tiempo?

8.13. Se multiplexan 10 líneas a 9.600 bps haciendo uso de TDM. Ignorando los bits suplementarios, ¿cuál es la capacidad total requerida para TDM síncrona? Suponiendo que deseamos limitar la utilización media de línea a 0,8, y suponiendo que cada línea está ocupada el 50 por ciento del tiempo, ¿cuál es la capacidad necesaria en TDM estadística?

8.14. Se definen los siguientes parámetros para un multiplexor por división en el tiempo estadístico:

F = longitud de la trama en bits
OH = información suplementaria en una trama, en bits
L = carga útil de datos en la trama en bps
C = capacidad del enlace, en bps

a) Exprese F en función de los otros parámetros. Explique por qué se puede ver F más como una variable que como una constante.

b) Represente gráficamente F frente a L para C = 9,6 kbps y para valores de OH = 40, 80 y 120. Comente los resultados y compárelos con los de la Figura 8.16.

c) Dibuje F en función de L para OH = 40 y para valores de C = 9,6 kbps y 8,2 kbps. Comente los resultados y compárelos con los de la Figura 8.16.

8.15. Una compañía tiene dos sedes: la oficina central y una fábrica situada a unos 25 km de la primera. La fábrica tiene cuatro terminales a 300 bps que se comunican con los servicios informáticos del computador central mediante líneas alquiladas de calidad telefónica. La compañía está planteándose instalar equipos TDM de modo que sólo se precise una línea. ¿Qué factores de coste deben considerarse en la toma de la decisión?

8.16. En TDM estadística puede existir un campo de longitud. ¿Qué alternativa se puede considerar a la inclusión de este campo? ¿Qué problema podría ocasionar esta solución y cómo se puede resolver?

8.17. En TDM síncrona, las líneas de entrada/salida servidas por los dos multiplexores pueden ser síncronas o asíncronas aunque el canal entre los multiplexores debe ser síncrono. ¿Existe alguna inconsistencia en esta afirmación? Razone la respuesta.

8.18. Suponga que está diseñando un sistema TDM, digamos DS-489, para dar servicio a 30 canales de voz usando muestras de 6 bits y una estructura similar a DS-1. Determine la velocidad requerida.

PARTE III

REDES DE ÁREA AMPLIA

CUESTIONES A TRATAR EN LA TERCERA PARTE

La Parte II se dedicó a la transferencia de datos entre dispositivos que están directamente conectados, generalmente por una línea punto a punto. Frecuentemente, sin embargo, esta disposición no es práctica, y entonces se necesita una red de comunicación de datos para transmitir información entre dispositivos, ya sea porque los dispositivos estén muy alejados o porque deban interconectarse una gran cantidad de ellos. Las redes de comunicaciones pueden clasificarse como sigue:

- Redes de conmutación:
  - Redes de conmutación de circuitos.
  - Redes de conmutación de paquetes, incluyendo retransmisión de tramas y ATM.
- Redes de difusión:
  - Redes en bus.
  - Redes en anillo.
  - Redes en estrella.

Las redes de área amplia utilizan técnicas de conmutación, y se discuten en la Parte III. La mayoría de redes de área local usan técnicas de difusión, y son analizadas en la Parte IV.

ESQUEMA DE LA PARTE III

CAPÍTULO 9. CONMUTACIÓN DE CIRCUITOS

Nuestro tratamiento de la tecnología y de la arquitectura de redes de conmutación de circuitos se inicia con el funcionamiento interno de un sencillo conmutador. Esto está en contraste con las redes de conmutación de paquetes, que son la mejor explicación para el comportamiento colectivo de un conjunto de conmutadores que componen una red. Así, el Capítulo 9 comienza examinando los conceptos de conmutación digital, incluyendo conmutación por división en el espacio y en el tiempo. Después se discuten conceptos relacionados con redes de conmutación de circuitos multimodo, desde el punto de vista del encaminamiento y señalización de control.

CAPÍTULO 10. CONMUTACIÓN DE PAQUETES

Hay dos principales problemas técnicos asociados con las redes de conmutación de paquetes:

- **Encaminamiento:** debido a que las estaciones fuente y destino de los datos no están directamente conectadas, la red debe encaminar cada paquete, de nodo a nodo, a través de la red.
- **Control de congestión:** la cantidad de trafico introducida y transmitida a través de la red debe ser regulada para lograr eficiencia, estabilidad y prestaciones adecuadas.

Los temas claves del diseño del enrutamiento se discuten en el Capítulo 10; el análisis se basa en ejemplos de redes específicas. Las consideraciones sobre congestión se difieren al Capítulo 12. Además, se describe una interfaz estándar clave para la conmutación de paquetes, la X25.

CAPÍTULO 11. ATM Y RETRANSMISIÓN DE TRAMAS

El Capítulo 11 se centra en la tecnología de transmisión fundamento de banda ancha ISDN: el modo de transferencia asíncrono (ATM, Asynchronous Transfer Mode). Este modo se utiliza ampliamente también en aplicaciones distintas de la de su uso como parte de la ISDN de banda ancha. En esencia ATM es una tecnología de conmutación de paquetes, pero más moderna y eficiente que la conmutación de paquetes clásica, y está proyectado para admitir velocidades de datos muy elevadas. Este capítulo comienza con una descripción del protocolo y formato ATM. Después se discute el tema de la capa física en relación con la transmisión de celdas ATM y la Capa de Adaptación ATM (AAL, ATM Adaptation Layer). Finalmente se discute la tecnología de retransmisión de tramas.

CAPÍTULO 12. CONTROL DE CONGESTIÓN EN REDES DE DATOS

Un problema de diseño crítico en conmutación de datos es el control de congestión. El capítulo se inicia con una explicación de la naturaleza de la congestión en redes de datos, y de tanto la importancia como la dificultad de controlar la congestión. El resto del capítulo se focaliza en la congestión y control de tráfico en redes ATM. Éste es uno de los aspectos más complejos de ATM y actualmente es el objetivo de investigaciones intensivas. Este capítulo resume aquellas técnicas que han sido aceptadas por tener una amplia utilidad en entornos ATM. El capítulo también analiza el control de congestión en retransmisión de tramas y contiene una discusión general del control de congestión en redes tradicionales de conmutación de paquetes.

CAPÍTULO 9

Conmutación de circuitos

- La conmutación de circuitos se usa en redes telefónicas públicas y es la base de redes privadas implementadas con líneas alquiladas y que utilizan conmutadores de circuitos in-situ. La técnica de conmutación de circuitos se desarrolló para tráfico de voz aunque también puede gestionar tráfico de datos, si bien su uso en este último tipo de aplicaciones resulta en ocasiones ineficiente.
- En la conmutación de circuitos se establece un canal de comunicaciones dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión. Ésta es transparente: una vez establecida parece como si los dispositivos estuviesen directamente conectados.
- Diversos aspectos importantes de las redes de conmutación de circuitos han cambiado de forma drástica con el incremento de la complejidad y digitalización de las redes de telecomunicaciones públicas. Así, esquemas simples de encaminamiento jerárquico han sido reemplazados por otros no jerárquicos más flexibles y potentes. Esto evidencia el cambio adoptado en la arquitectura subyacente, lo cual permite un incremento en la eficiencia y en la flexibilidad. Los métodos de señalización de control intracanal se han reemplazados por técnicas de señalización por canal común más complejas y de mayor velocidad.

Desde la invención del teléfono, la conmutación de circuitos ha sido la tecnología dominante en las comunicaciones de voz, y así ha seguido siendo con la llegada de la RDSI. Este capítulo comienza con una introducción al concepto de redes de comunicación conmutadas, pasando seguidamente a presentar las características principales de las redes de conmutación de circuitos.

9.1. REDES CONMUTADAS

Para la transmisión de datos[1] a larga distancia, más allá de un entorno local, la comunicación se realiza generalmente mediante la transmisión de datos desde el origen hasta el destino a través de una red de nodos de conmutación intermedios. Este diseño de red conmutada se usa también a veces para implementar redes LAN (local area networks). El contenido de los datos no es del interés de los nodos de conmutación, sino que el propósito de estos últimos es proporcionar un servicio de conmutación que posibilite el intercambio de datos entre nodos hasta que alcancen su destino. En la Figura 9.1 se muestra una red sencilla, en la que los dispositivos finales que desean comunicarse se denominan *estaciones*. Éstas pueden ser computadores, terminales, teléfonos u otros dispositivos de comunicación. Por su parte, a los dispositivos de conmutación cuyo objetivo es proporcionar la comunicación se les denomina *nodos*. Los nodos están conectados entre sí mediante enlaces formando una topología dada. Cada estación se conecta a un nodo, llamándose *red de comunicaciones* al conjunto de todos los nodos.

Los tipos de redes estudiados en este capítulo, así como en los tres siguientes, se denominan *redes de comunicación conmutadas*. Los datos que entran a la red procedentes de una estación se encaminan hacia el destino mediante su conmutación de nodo en nodo. Por ejemplo, en la Figura 9.1 los datos desde la estación A con destino la estación F se envían al nodo 4. Éstos se pueden encaminar hasta el destino a través de los nodos 5 y 6 o bien vía los nodos 7 y 6. Diversas consideraciones se pueden realizar acerca de las redes de comunicación conmutadas:

[1] Este término se usa aquí en un sentido muy general para referirnos a voz, imágenes y vídeo, así como datos ordinarios (datos numéricos o texto por ejemplo).

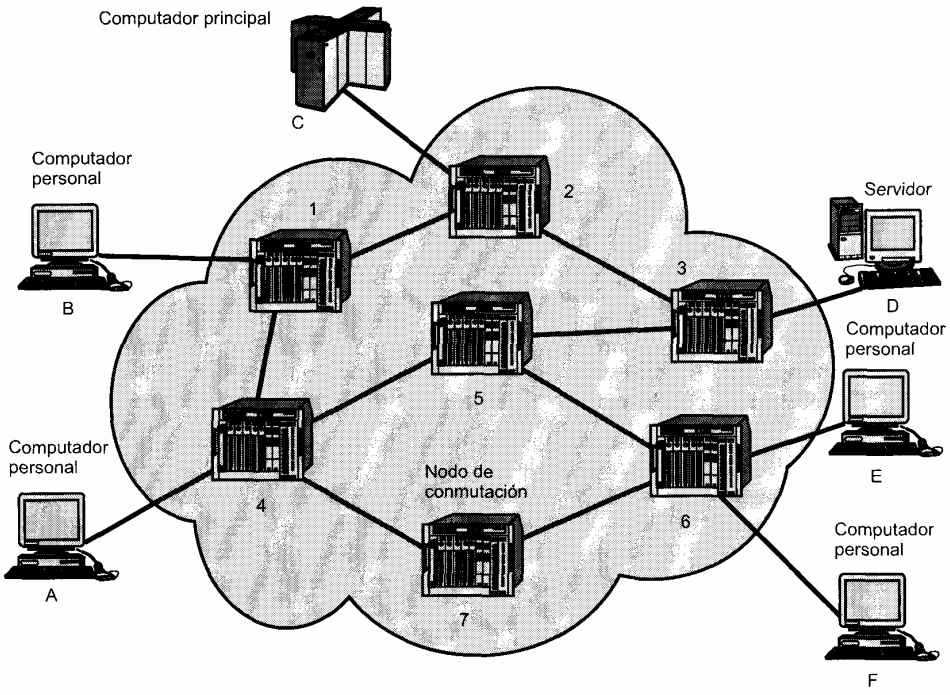


Figura 9.1. Red de conmutación simple.

1. Algunos nodos sólo se conectan con otros nodos (por ejemplo, los nodos 5 y 7), siendo su única tarea la conmutación interna (en la red) de los datos. Otros nodos tienen también conectadas una o más estaciones, de modo que además de sus funciones de conmutación estos nodos aceptan datos desde y hacia las estaciones conectadas a ellos.
2. Los enlaces entre nodos están normalmente multiplexados, utilizándose multiplexación por división en frecuencias (FDM) o por división en el tiempo (TDM).
3. Generalmente, la red no está completamente conectada; es decir, no existe un enlace directo entre cada posible pareja de nodos. Sin embargo, siempre resulta deseable tener más de un camino posible a través de la red para cada par de estaciones. Esto mejora la fiabilidad o seguridad de la red.

En las redes conmutadas de área amplia se emplean dos tecnologías diferentes: conmutación de circuitos y conmutación de paquetes. Estas dos tecnologías difieren en la forma en que los nodos conmutan la información entre enlaces en el camino desde el origen hasta el destino. En este capítulo se verá en detalle la conmutación de circuitos, dejándose el estudio de la técnica de conmutación de paquetes para el Capítulo 10. Por su parte, en el Capítulo 11 se presentarán dos tecnologías derivadas de la conmutación de paquetes: ATM y retransmisión de tramas («frame relay»).

9.2. REDES DE CONMUTACIÓN DE CIRCUITOS

Las comunicaciones mediante la conmutación de circuitos implican la existencia de un camino o canal de comunicaciones dedicado entre dos estaciones, que es una secuencia de enlaces conectados entre nodos de la red. En cada uno de los enlaces físicos se dedica un canal lógico para cada conexión estableci-

da. La comunicación vía la conmutación de circuitos implican tres fases, que se pueden explicar haciendo referencia a la Figura 9.1.

1. **Establecimiento del circuito.** Antes de transmitir señal alguna, se establece un circuito extremo a extremo (estación a estación). Por ejemplo, la estación A envía una solicitud al nodo 4 pidiendo una conexión con la estación E. Generalmente, el enlace entre A y 4 es una línea dedicada, por lo que esa parte de la conexión existe ya. El nodo 4 debe encontrar el siguiente enlace de la ruta para alcanzar el nodo 6. En función de la información de encaminamiento y de las medidas de disponibilidad y, quizás, el coste, el nodo 4 selecciona el enlace hacia el nodo 5, reserva un canal libre del enlace (utilizando FDM o TDM) y envía un mensaje a E solicitando la conexión. Tras esto queda establecido un camino dedicado desde A hasta 5 a través de 4. Dado que pueden existir varias estaciones conectadas al nodo 4, éste debe ser capaz de establecer rutas internas desde varias estaciones a múltiples nodos. El resto del proceso es similar. El nodo 5 reserva un canal hasta el nodo 6 y asigna internamente este canal al que viene desde el nodo 4. El nodo 6 completa la conexión con E, para lo cual se realiza un test con objeto de determinar si E está ocupada o, por el contrario, se encuentra lista para aceptar la conexión.
2. **Transferencia de datos.** Tras el establecimiento del circuito se puede transmitir la información desde A hasta E a través de la red. Los datos pueden ser analógicos o digitales dependiendo de la naturaleza de la red. Debido a la tendencia actual de migración hacia redes digitales completamente integradas, la utilización de transmisiones digitales (binarias) tanto de voz como de datos se está convirtiendo en el método de comunicaciones predominante. El camino del ejemplo está constituido por el enlace A-4 (conmutación interna a través de 4), el canal 4-5 (conmutación interna a través de 5), el canal 5-6 (conmutación interna a través de 6) y el enlace 6-E. Normalmente, la conexión es *full-duplex*.
3. **Desconexión del circuito.** Tras la fase de transferencia de datos, la conexión finaliza por orden de una de las dos estaciones involucradas. Las señales se deben propagar a los nodos 4, 5 y 6 para que éstos liberen los recursos dedicados a la conexión que se cierra.

Obsérvese que el canal de conexión se establece antes de que comience la transmisión de datos, por lo que la capacidad del canal se debe reservar entre cada par de nodos en la ruta y cada nodo debe ser capaz de conmutar internamente para gestionar la conexión solicitada. En definitiva, los conmutadores deben contar con la inteligencia necesaria para realizar estas reservas y establecer una ruta a través de la red.

La conmutación de circuitos puede llegar a ser bastante ineficiente. La capacidad del canal se dedica permanentemente a la conexión mientras dura ésta, incluso si no se transfieren datos. Aunque no se alcanza el 100 %, la utilización puede ser bastante alta para una conexión de voz. Por su parte, para comunicaciones entre un terminal y un computador, es posible que el canal esté libre durante la mayor parte de la conexión. Desde el punto de vista de las prestaciones, existe un retardo previo a la transferencia de las señales debido al establecimiento de la llamada. No obstante, una vez establecido el circuito la red es transparente para los usuarios. La información se transmite a una velocidad fija sin otro retardo que el de propagación a través de los enlaces de transmisión, siendo despreciable el retardo introducido por cada nodo de la ruta.

La conmutación de circuitos fue desarrollada para el tráfico de voz, pero en la actualidad se usa también para el tráfico de datos. El mejor ejemplo conocido de una red de conmutación de circuitos es el de la red telefónica pública (Figura 9.2), la cual es en la actualidad un conjunto de redes nacionales interconectadas para ofrecer un servicio internacional. Aunque fue ideada e implementada inicialmente para ofrecer un servicio de telefonía analógica a los abonados, en la actualidad opera con una gran cantidad de tráfico de datos vía modem y está siendo convertida progresivamente en una red digital. Otra aplicación bien conocida de la conmutación de circuitos son las centralitas privadas (PBX, Private Branch Exchange), que se usan para conectar los teléfonos dentro de un edificio u oficina. Este tipo de redes se utiliza usualmente en compañías u organizaciones para conectar sus diferentes delegaciones o sedes. Una red de este tipo consta normalmente de una serie de PBX, cada una de las cuales se sitúa en

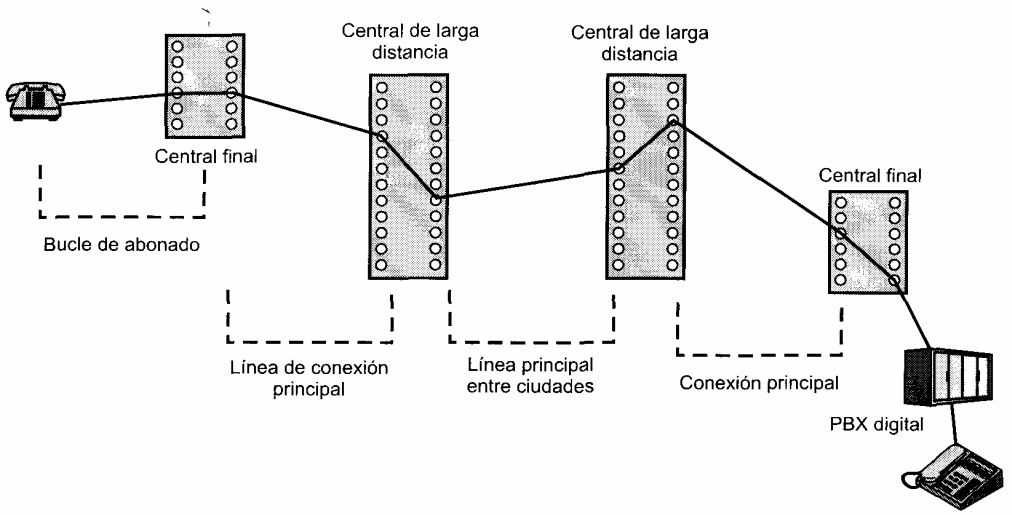


Figura 9.2. Ejemplo de conexión sobre una red pública de conmutación de circuitos.

una dependencia e interconectadas entre sí a través de líneas alquiladas a alguno de los proveedores de servicios de telecomunicaciones, como, por ejemplo, AT&T. Un último ejemplo de aplicación de la conmutación de circuitos es la conmutación de datos. Ésta es similar a las PBX, pero en este caso se interconectan dispositivos de procesamiento de datos digitales tales como terminales y computadores.

Una red pública de telecomunicaciones se puede describir a través de los cuatro componentes que forman su arquitectura:

- **Abonados:** son los dispositivos que se conectan a la red. La mayoría de los dispositivos de abonado en redes de telecomunicaciones públicas continúan siendo en la actualidad los teléfonos, si bien el porcentaje de tráfico de datos crece año tras año.
- **Bucle local:** es el enlace entre el abonado y la red, también denominado *bucle de abonado* o *línea de abonado*. En casi todas las conexiones de bucle local se hace uso de cable de par trenzado. La longitud del bucle local está normalmente comprendida en el rango que va desde unos pocos kilómetros hasta varias decenas de ellos.
- **Centrales:** son los centros de conmutación de la red. Aquellos centros de conmutación a los que se conectan directamente los abonados se denominan *centrales finales*. Generalmente, una central final da servicio a varios miles de abonados en un área geográfica localizada. Existen por encima de 19.000 centrales finales en los Estados Unidos, por lo que es claramente imposible en la práctica la existencia de un enlace directo entre cada dos centrales finales cualesquiera; esto requeriría del orden de 2×10^8 enlaces. En lugar de ello se utilizan nodos de conmutación intermedios.
- **Líneas principales:** son los enlaces entre centrales. Las líneas principales transportan varios circuitos de voz haciendo uso de FDM o de TDM síncrona. Con anterioridad, al conjunto de estas líneas se le denominaba *sistema de transporte*.

Los abonados se conectan directamente a una central final, que conmuta el tráfico entre abonados y entre un abonado y otras centrales de larga distancia. Las otras centrales son responsables de encaminar y conmutar el tráfico entre centrales finales. Esta distinción se muestra en la Figura 9.3. Para comunicar entre sí dos abonados que están conectados a la misma central final se establece un circuito en la forma descrita anteriormente. Si los abonados están conectados a dos centrales finales diferentes, el circuito establecido entre ellos consistirá en una concatenación de circuitos a través de una o más centrales intermedias. En la figura se establece una conexión entre las líneas *a* y *b* simplemente mediante un circuito a

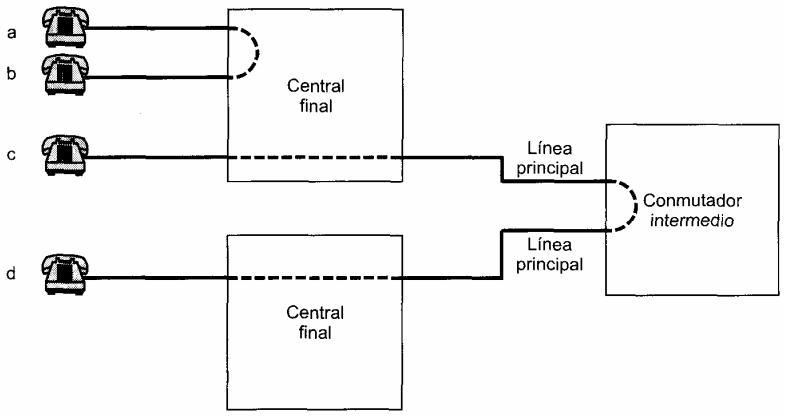


Figura 9.3. Establecimiento de un circuito.

través de la central final. Por su parte, la conexión entre *c* y *d* es más compleja. En este caso, la central final de *c* establece una conexión entre la línea *c* y un canal sobre una línea principal TDM al conmutador intermedio. En este conmutador, el canal se conecta a un canal de un enlace TDM a la central final de *d*. En esta central final, el canal se conecta con la línea *d*.

La tecnología de conmutación de circuitos se desarrolló para las aplicaciones de tráfico de voz. Uno de los aspectos clave del tráfico de voz es que no debe haber prácticamente retardo en la transmisión ni, por supuesto, variaciones en el mismo. La velocidad de transmisión de la señal se debe mantener constante, ya que, tanto la emisión como la recepción se realizan a la misma velocidad. Estos requisitos son necesarios para permitir una conversación humana normal. Es más, la calidad de la señal recibida debe ser suficientemente elevada para proporcionar, como mínimo, inteligibilidad.

La conmutación de circuitos está ampliamente extendida, ocupando una posición predominante debido a que es adecuada para la transmisión analógica de señales de voz. En el mundo digital actual resultan más relevantes sus limitaciones. No obstante, a pesar de sus inconvenientes, la conmutación de circuitos continúa siendo una atractiva alternativa tanto para redes de área local como para redes de área amplia. Una de sus ventajas principales es la transparencia: una vez que se ha establecido el circuito, éste parece una conexión directa entre las dos estaciones conectadas, no siendo necesaria la inclusión de lógica de red especial en las estaciones.

9.3. CONCEPTOS DE CONMUTACIÓN DE CIRCUITOS

Para comprender mejor la tecnología de conmutación de circuitos, consideremos un ejemplo del funcionamiento de un solo nodo conmutado. Una red diseñada en torno a un único nodo de conmutación de circuitos consiste en un conjunto de estaciones conectadas a una unidad central de conmutación. El conmutador central establecerá un canal dedicado entre cualesquiera dos dispositivos que deseen comunicarse. En la Figura 9.4 se muestran los elementos principales de una red de un solo nodo como la mencionada. Las líneas discontinuas dentro del conmutador simbolizan las conexiones que se encuentran activas en un momento dado.

La parte central de todo sistema moderno es el **conmutador digital**, cuya función es proporcionar una ruta transparente entre cualesquiera dos dispositivos conectados. El camino es transparente en el sentido de que parece como si existiese una conexión directa entre los dispositivos. Generalmente, la conexión debe permitir transmisión *full-duplex*.

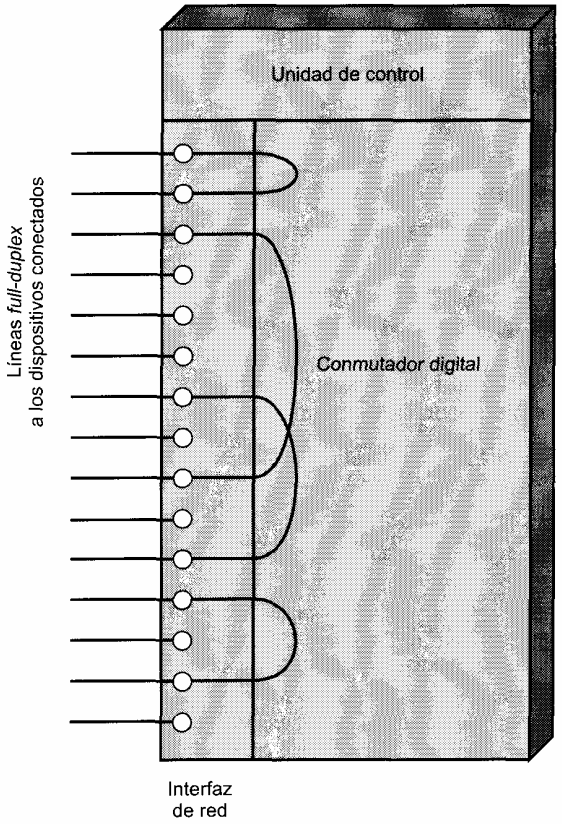


Figura 9.4. Elementos de un nodo de conmutación de circuitos.

El elemento de **interfaz de red** incluye las funciones y el hardware necesarios para conectar dispositivos digitales, tales como dispositivos de procesamiento de datos y teléfonos digitales, a la red. Los teléfonos analógicos también se pueden conectar si la interfaz de red contiene la lógica necesaria para convertir la señal a digital. Las líneas principales a otros conmutadores digitales transportan señales TDM y facilitan los canales para la construcción de redes de varios nodos.

La **unidad de control** realiza tres tareas generales. En primer lugar establece conexiones, lo cual se realiza generalmente bajo demanda (es decir, ante la solicitud de un dispositivo conectado a la red). Para establecer la conexión, la unidad de control debe gestionar y confirmar la petición, determinar si la estación de destino está libre y construir una ruta a través del conmutador. En segundo lugar, la unidad de control debe mantener la conexión. Dado que el conmutador digital utiliza una aproximación por división en el tiempo, esta segunda tarea puede precisar un control continuo de los elementos de conmutación. No obstante, los bits de la comunicación se transfieren de forma transparente (desde el punto de vista de los dispositivos del nodo). Por último, la unidad de control debe liberar la conexión, bien en respuesta a una solicitud generada por una de las partes o por razones propias.

Una característica importante de un dispositivo de conmutación de circuitos es si es *bloqueante* o *no bloqueante*. El bloqueo ocurre cuando la red no puede conectar a dos estaciones debido a que todos los posibles caminos entre ellas están siendo ya utilizados.

Una red bloqueante es aquella en la que es posible el bloqueo. Por su parte, una red no bloqueante se caracteriza porque permite que todas las estaciones se conecten simultáneamente (por parejas) y garantiza el servicio a todas las solicitudes de conexión posibles siempre que el destino esté libre. La configu-

ración bloqueante resulta generalmente aceptable cuando una red sólo admite tráfico de voz, ya que se espera que la mayor parte de las llamadas telefónicas sean de corta duración y que, por tanto, sólo una fracción de los teléfonos estarán ocupados todo el tiempo. Sin embargo, estas suposiciones pueden no ser válidas cuando se trata de dispositivos de procesamiento de datos. Por ejemplo, para una aplicación de entrada de datos, un terminal puede estar continuamente conectado a un computador durante horas. Por tanto, para aplicaciones de datos se necesita una configuración no bloqueante o «casi no bloqueante» (es decir, con una probabilidad de bloqueo muy baja).

Reconsideremos ahora el estudio de las técnicas de conmutación internas a un nodo de conmutación de circuitos.

CONMUTACIÓN POR DIVISIÓN EN EL ESPACIO

La conmutación por división en el espacio se desarrolló originalmente para entornos analógicos, desplazándose posteriormente al contexto digital. Los principios fundamentales de un conmutador son los mismos tanto si se usa para transportar señales analógicas como para el transporte de señales digitales.

Como su nombre indica, un conmutador por división en el espacio es aquel en el que las rutas de señal que se establecen son físicamente independientes entre sí (divididas en el espacio). Cada conexión necesita el establecimiento de un camino físico a través del conmutador que se dedique únicamente a la transferencia de señales entre los dos extremos. El bloque básico de un conmutador consiste en una matriz de conexiones metálicas (o puntos de cruce) o puertas semiconductoras que una unidad de control puede habilitar o deshabilitar.

En la Figura 9.5 se muestra una matriz de conexiones simple con 10 líneas de entrada/salida *full-duplex*. La matriz tiene 10 entradas y 10 salidas; cada estación se conecta a la matriz a través de una línea de entrada y otra de salida. La conexión entre cualesquiera dos líneas es posible habilitando el punto de cruce correspondiente. Obsérvese que es necesario un total de 100 conexiones. Los conmutadores matriciales presentan varias limitaciones:

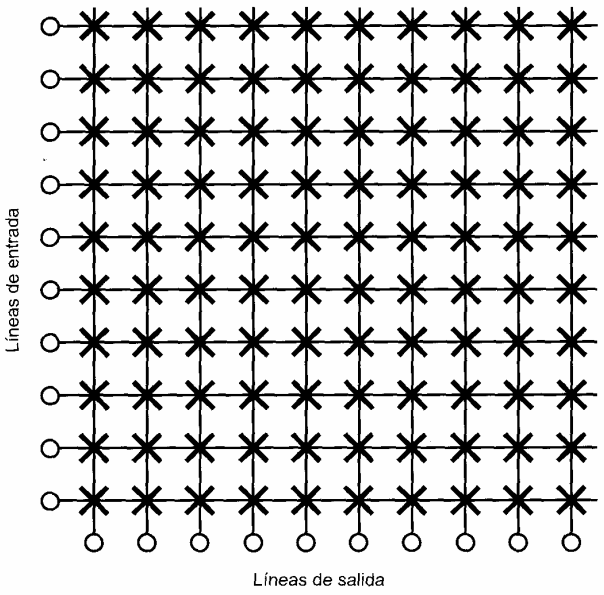


Figura 9.5. Conmutador por división en el espacio.

- El número de conexiones crece con el cuadrado del número de estaciones conectadas, lo cual resulta costoso para conmutadores grandes.
- La pérdida de un cruce impide la conexión entre los dos dispositivos cuyas líneas interseccionan en ese punto de cruce.
- Las conexiones se utilizan de forma ineficiente; incluso cuando todos los dispositivos conectados se encuentran activos, sólo está ocupada una pequeña fracción de los puntos de cruce.

Para superar estas limitaciones se emplean conmutadores multietapa. La Figura 9.6 es un ejemplo de conmutador de tres etapas. Esta solución presenta dos ventajas sobre una matriz de una sola etapa:

- El número de conexiones se reduce, aumentando la utilización de las líneas de cruce. En este ejemplo, el número total de interconexiones para 10 estaciones se reduce de 100 a 48.
- Existe más de una ruta a través de la red para conectar dos extremos, incrementándose así la seguridad de la red.

Evidentemente, una red multietapa necesita un esquema de control más complejo. Para establecer un camino en una red de una etapa sólo se necesita habilitar una única puerta. En una red multietapa se debe determinar una ruta libre a través de las etapas habilitando las puertas correspondientes.

Una cuestión importante acerca de un conmutador por división en el espacio multietapa es que puede ser bloqueante. Es claro a partir de la Figura 9.5 que una matriz de una sola etapa es no bloqueante; es decir, siempre hay un camino disponible para conectar una entrada con una salida. Como se muestra en la Figura 9.6, esto no es necesariamente verdad en el caso de un conmutador multietapa. En esta figura se resaltan en negrita las líneas ya en uso. En este estado, la línea de entrada 10, por ejemplo, no se puede conectar a las líneas de salida 3, 4 o 5, aun cuando todas ellas estuviesen disponibles. Un conmutador multietapa puede convertirse en no bloqueante aumentando el número o el tamaño de los conmutadores intermedios, si bien ello incrementará el costo.

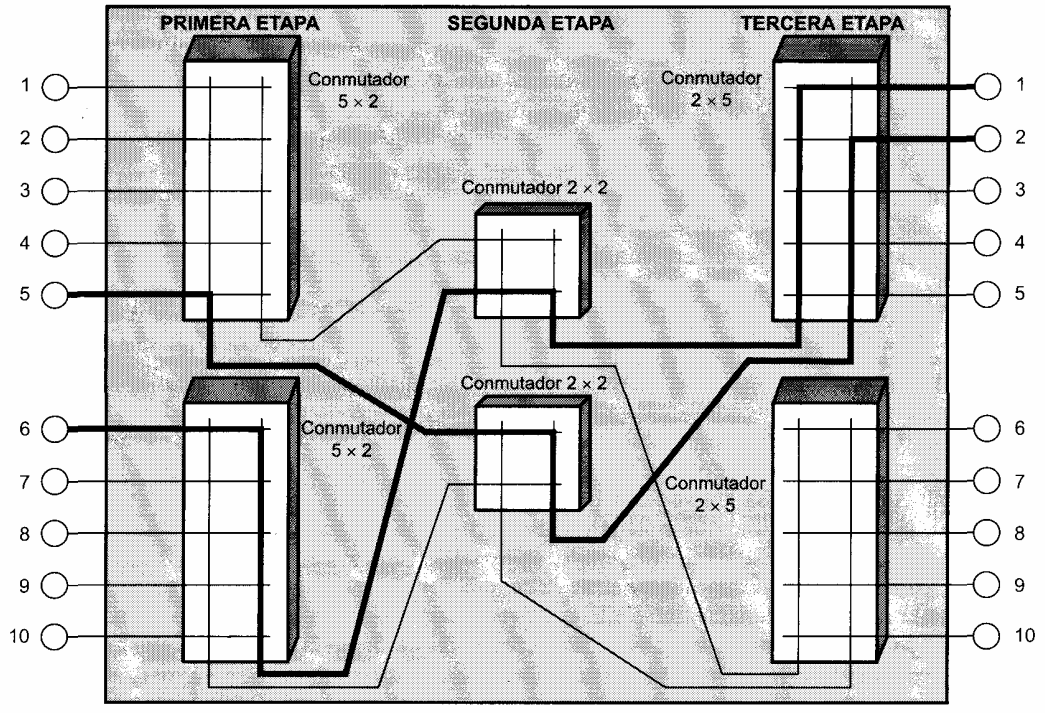


Figura 9.6. Conmutador por división en el espacio de tres etapas.

CONMUTACIÓN POR DIVISIÓN EN EL TIEMPO

La tecnología de conmutación tiene una larga historia, la mayor parte de la cual corresponde a la era analógica. Con la aparición de la voz digitalizada y las técnicas de multiplexación por división en el tiempo síncronas se posibilita la transmisión de la voz y de los datos mediante señales digitales. Esto ha dado lugar a un cambio drástico en el diseño y en la tecnología de los sistemas de conmutación.

En lugar de utilizar los sistemas relativamente torpes por división en el espacio, los sistemas digitales modernos se basan en el control inteligente de elementos de división en el espacio y de división en el tiempo.

Virtualmente todos los conmutadores de circuitos modernos emplean técnicas por división en el tiempo para el establecimiento y el mantenimiento de los circuitos. La conmutación por división en el tiempo involucra la fragmentación de una cadena de bits de menor velocidad en segmentos que compartirán una secuencia de velocidad superior con otras cadenas de bits. Los fragmentos individuales, o ranuras, se gestionan por parte de la lógica de control con el fin de encaminar los datos desde la entrada hacia la salida. Existen distintas variantes dentro de este concepto básico. Para proporcionar al lector una idea clara acerca de la conmutación por división en el tiempo se presenta a continuación una de las más técnicas más sencillas pero a la vez más populares, denominada *conmutación mediante bus TDM.*

La conmutación mediante bus TDM, y de hecho todas las técnicas de conmutación digital, se fundamenta en la utilización de la multiplexación por división en el tiempo síncrona (TDM). Como se vio en la Figura 8.6, la técnica TDM síncrona permite que varias cadenas de bits de baja velocidad compartan una línea de alta velocidad. Las entradas se muestrean por turnos. Las muestras en serie se organizan en ranuras (canales) para formar una trama recurrente de ranuras, siendo el número de ranuras por trama igual al número de entradas. Una ranura puede ser un bit, un octeto o un bloque de longitud mayor. Una cuestión importante a resaltar es que con TDM síncrona se conocen el origen y el destino para cada ranura.

En la Figura 9.7 se muestra una forma sencilla de cómo adaptar esta técnica para su utilización en conmutación. Cada dispositivo se conecta al conmutador a través de una línea *full-duplex.*

Estas líneas se conectan a un bus digital de alta velocidad a través de unas puertas controlables. A cada línea de entrada se le asigna una ranura temporal. La puerta de una línea se encuentra habilitada durante el periodo de la ranura asociada, permitiendo así que una ráfaga pequeña de datos se dirija hacia el bus. Durante esa misma ranura se encuentra habilitada también una de las puertas correspondiente a una de las líneas de salida. De este modo, durante esa ranura temporal, los datos se conmutan desde la línea de entrada hasta la línea de salida habilitadas. A través de las sucesivas ranuras se habilitan diferentes parejas de líneas de entrada/salida, permitiendo así numerosas conexiones sobre el bus compartido. Los dispositivos conectados al bus consiguen la operación *full-duplex* transmitiendo durante una ranura asignada y recibiendo durante otra. El otro extremo de la conexión es una pareja de entrada/salida para la que estas ranuras temporales tienen justo el significado contrario al anterior.

Veamos la temporización con más detalle. Consideremos en primer lugar la implementación no bloqueante dada en la Figura 9.7. Para un conmutador que atendiera, por ejemplo, a 100 dispositivos deben haber 100 ranuras temporales diferentes generándose de forma repetitiva, estando cada una de ellas asignada a una línea de entrada y a una de salida. La asignación de las líneas de entrada puede ser fija, mientras que las de salida varían para permitir distintas conexiones. Cuando comienza una ranura temporal, la línea de entrada designada (habilitada) puede insertar una ráfaga de datos en la línea, sobre la cual se propagará. Durante este tiempo, la línea de salida designada (habilitada) copia los datos, si es que los hay. Por tanto, la duración de la ranura debe ser igual al tiempo de transmisión de la entrada más el retardo de propagación desde la entrada hasta la salida sobre el bus. Para mantener uniforme la duración de las sucesivas ranuras, se define su longitud como el tiempo de transmisión más el retardo de propagación de extremo a extremo en el bus.

Para no perder información de las líneas de entrada, la razón de datos en el bus debe ser suficientemente elevada para que las ranuras completen el ciclo con suficiente rapidez. Por ejemplo, considérese

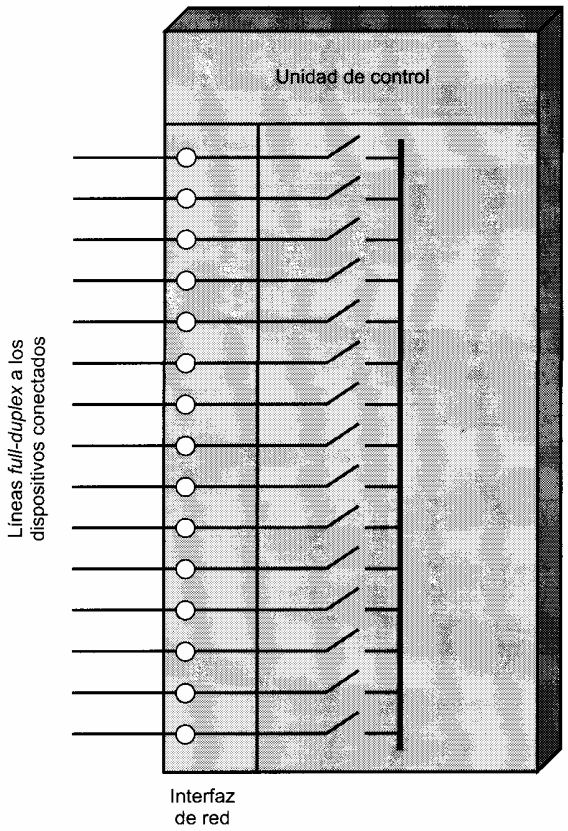


Figura 9.7. Conmutador mediante bus TDM.

un sistema que conecta 100 líneas *full-duplex* a 19,2 kbps. Los datos de entrada de cada línea se almacenan temporalmente en la puerta. Cada memoria temporal debe vaciarse al habilitar la puerta con suficiente rapidez para evitar rebosamientos. Así pues, la razón de datos en el bus para este ejemplo debe ser superior a 1,92 Mbps. La velocidad real debe ser suficientemente elevada para además tener en cuenta el tiempo invertido en la propagación.

Estas consideraciones determinan igualmente la capacidad de transporte de tráfico en un conmutador bloqueante. Para éstos no hay una asignación fija de líneas de entrada a ranuras temporales, sino que ésta se lleva a cabo bajo demanda. La velocidad de datos del bus establece cuántas conexiones se pueden establecer en un momento dado. Para un sistema con 200 dispositivos a 19,2 kbps y un bus a 2 Mbps, aproximadamente la mitad de los dispositivos se pueden conectar en cualquier momento.

El esquema de conmutación mediante bus TDM puede dar servicio a líneas con diferentes razones de datos. Por ejemplo, si una línea de 9.600 bps requiere una ranura por trama, una línea de 19,2 kbps precisará dos ranuras por trama. Por supuesto, sólo se pueden conectar líneas de la misma velocidad.

En la Figura 9.8 se ofrece un ejemplo que sugiere cómo se puede realizar el control de un conmutador mediante bus TDM. Supongamos que el tiempo de propagación en el bus es de 0,01 μs. El tiempo en el bus se organiza en tramas de 30,06 μs de duración, consistiendo cada trama en seis ranuras temporales de 5,01 μs. Una memoria de control indica qué puertas deben habilitarse durante cada ranura temporal. En este ejemplo se necesitarán seis palabras de memoria. Un controlador sondea la memoria a razón de un ciclo cada 30,06 μs. Durante la primera ranura temporal de cada ciclo se habilitan la puerta de entrada del dispositivo 1 y la puerta de salida al dispositivo 3, permitiendo así que los datos pasen del

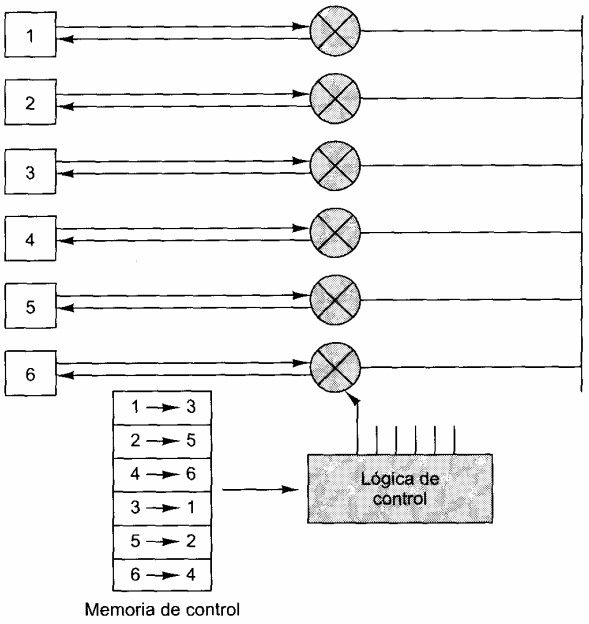


Figura 9.8. Control de un conmutador mediante bus TDM.

dispositivo 1 al dispositivo 3 a través del bus. Las palabras de memoria restantes se incluyen en las siguientes ranuras de tiempo y son tratadas en consecuencia. Mientras que la memoria de control contenga la información mostrada en la Figura 9.8, se mantendrán las conexiones entre 1 y 3, 2 y 5 y entre 4 y 6.

9.4. ENCAMINAMIENTO EN REDES DE CONMUTACIÓN DE CIRCUITOS

En una red grande de conmutación de circuitos, tal como la red telefónica de larga distancia de AT&T, muchas de las conexiones de circuitos necesitan una ruta que pase a través de más de un conmutador. Cuando se establece una llamada, la red debe encontrar una ruta desde el abonado llamante hasta el abonado llamado que pase a través de varios conmutadores y enlaces. Existen dos requisitos fundamentales para la arquitectura de red que tienen efecto sobre la estrategia de encaminamiento: *eficiencia* y *flexibilidad*. En primer lugar, es deseable minimizar la cantidad de equipos (conmutadores y enlaces) en la red teniendo en cuenta que debe ser capaz de aceptar toda la carga esperada. Las necesidades de carga se expresan usualmente en términos de *tráfico en horas punta*. Esto es sencillamente la carga promedio esperada durante los periodos de más actividad a lo largo del día. Desde un punto de vista práctico, es necesario ser capaz de gestionar esta cantidad de tráfico. Desde el punto de vista de costes, sería deseable gestionar esta carga con el menor equipamiento posible. Otro requisito es la flexibilidad. Aunque la red se puede dimensionar teniendo en cuenta el tráfico en horas punta, es posible que la carga supere temporalmente este nivel (por ejemplo, durante una gran tormenta). Puede darse también el caso de que, ocasionalmente, los conmutadores y las líneas fallen y se encuentren momentáneamente inaccesibles (puede que desgraciadamente coincidiendo con la propia tormenta). Sería deseable por tanto que la red proporcionase un nivel razonable de servicio incluso bajo tales circunstancias.

El punto clave de diseño que determina la naturaleza del compromiso entre eficiencia y flexibilidad es la estrategia de encaminamiento. Tradicionalmente, la función de encaminamiento en redes de telecomunicaciones públicas ha sido bastante simple.

Esencialmente, los conmutadores de una red se organizaban en una estructura en árbol o jerarquía. Se establecía una ruta a través del árbol comenzando en el abonado llamante hasta el primer nodo común, y después hasta el abonado llamado. Para proporcionar cierta flexibilidad a la red, se incluían en el árbol enlaces de alta capacidad adicionales para conectar entre sí centrales con altos volúmenes de tráfico. En general, esta aproximación es estática. La incorporación de enlaces de alta capacidad proporciona redundancia y una capacidad extra, pero persisten las limitaciones en términos de eficiencia y de flexibilidad. Dado que este esquema de encaminamiento no es capaz de adaptarse a condiciones cambiantes, la red debe diseñarse para dar servicio en condiciones típicas de alta carga. Para dar un ejemplo de los problemas a que da lugar esta aproximación, téngase en cuenta que las horas punta para el tráfico este-oeste no coinciden con las del tráfico norte-sur y plantean además diferentes demandas al sistema. Es difícil analizar los efectos de estas variaciones, que pueden dar lugar a un sobredimensionamiento y, en consecuencia, a ineficiencia. En términos de flexibilidad, la estructura jerárquica fija con enlaces adicionales puede responder pobremente ante la ocurrencia de fallos. Generalmente, en estos diseños la consecuencia de un fallo es la aparición de una congestión local importante cerca del lugar donde se origina el fallo.

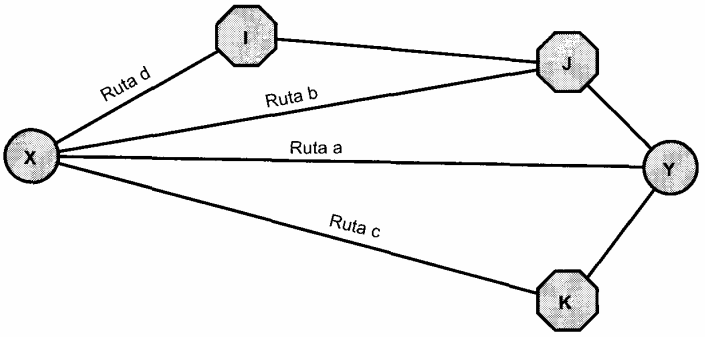
Para hacer frente a la creciente demanda de las redes de telecomunicaciones públicas, la práctica totalidad de los proveedores han pasado de una aproximación jerárquica estática a la adopción de una aproximación dinámica. En una aproximación de encaminamiento dinámica las decisiones de encaminamiento están influenciadas en cada instante de tiempo por las condiciones de tráfico actuales. Generalmente, los nodos de conmutación de circuitos mantienen una relación de igual a igual entre sí en lugar de una jerárquica como la de la aproximación estática. Todos los nodos están capacitados para realizar las mismas funciones. Esta arquitectura de encaminamiento es más compleja y, a la vez, más flexible. Más compleja porque la arquitectura no proporciona una ruta «natural» o conjunto de rutas basándose en la estructura jerárquica. Pero al mismo tiempo es más flexible debido a que hay más rutas alternativas.

Como ejemplo veamos una forma de encaminamiento en redes de conmutación de circuitos llamada **encaminamiento alternativo**. La esencia de los esquemas de encaminamiento alternativo reside en que las posibles rutas entre dos centrales finales se encuentran predefinidas. Es responsabilidad del conmutador origen seleccionar el camino adecuado para cada llamada. Cada conmutador dispone de un conjunto de rutas prefijadas en orden de preferencia para cada destino. Si existe una conexión directa entre dos conmutadores, ésta suele ser la elección preferida. Si no está disponible esta línea se prueba con la segunda alternativa, y así sucesivamente. Las secuencias de encaminamiento (conjunto de rutas intentadas) reflejan un análisis basado en patrones de tráfico conocidos y se diseñan para optimizar la utilización de los recursos de la red.

Si sólo se define una secuencia de encaminamiento para cada pareja origen-destino, el esquema se conoce como esquema de encaminamiento alternativo fijo. No obstante, es más frecuente el uso de un esquema de encaminamiento alternativo dinámico. En este caso se utiliza un conjunto diferente de rutas preplanificadas en instantes distintos de tiempo con objeto de aprovechar las distintas condiciones de tráfico en las diferentes zonas horarias y en los distintos periodos en un día. Por tanto, la decisión de encaminamiento se basa tanto en el estado del tráfico actual (una ruta se descartará si está ocupada) como en patrones de tráfico conocidos (que determinan la secuencia de rutas a considerar).

En la Figura 9.9 se muestra un ejemplo sencillo. El conmutador origen, X, tiene cuatro posibles rutas hacia el conmutador destino, Y. Siempre se intentará en primer lugar la ruta directa (a). Si este enlace no está disponible (ocupado o fuera de servicio), se intentarán las otras rutas en un orden dado dependiendo de la hora de que se trate. Por ejemplo, durante las mañanas del fin de semana la siguiente ruta en probarse será la b.

En las «Bell Operating Companies» se emplea una variante de la técnica de encaminamiento alternativo dinámico para proporcionar servicio telefónico local y regional [BELL90]; es la técnica conocida como encaminamiento multialternativo (MAR, multialternate routing). Este enfoque también se utiliza por AT&T en su red de larga distancia [ASH90] y se conoce como encaminamiento no jerárquico dinámico (DNHR, dynamic nonhierarchical routing).



Ruta a: X → Y
Ruta b: X → J → Y
Ruta c: X → K → Y
Ruta d: X → I → J → Y

= Central final

= Nodo de conmutación intermedio

(a) Topología

Periodo de tiempo	Primera ruta	Segunda ruta	Tercera ruta	Cuarta y última ruta
Mañana	a	b	c	d
Tarde	a	d	b	c
Noche	a	d	c	b
Fin de semana	a	c	b	d

(b) Tabla de encaminamiento

Figura 9.9. Rutas alternativas desde la central final X hasta la central final Y.

9.5. SEÑALIZACIÓN DE CONTROL

En las redes de conmutación de circuitos, las señales de control constituyen el medio mediante el que se gestiona la red y por el que se establecen, mantienen y finalizan las llamadas. Tanto la gestión de las llamadas como la gestión de la red necesitan que se intercambie información entre el abonado y los conmutadores, entre los conmutadores entre sí y entre los conmutadores y el centro de gestión de red. En las grandes redes de telecomunicaciones se precisa un esquema de señalización de control relativamente complejo.

En esta sección se ofrece un breve resumen de la funcionalidad de las señales de control, estudiándose posteriormente la técnica base de las redes digitales integradas modernas, denominada señalización por canal común.

FUNCIONES DE SEÑALIZACIÓN

Las señales de control afectan a varios aspectos relativos al funcionamiento de la red, incluyendo tanto a los servicios de la red visibles por el abonado como a los procedimientos internos. A medida que la red se hace más compleja, crece necesariamente el número de funciones que se realizan a través de la señalización de control. Entre las funciones más importantes se encuentran las siguientes:

1. Comunicación audible con el abonado, que incluye el tono de marcar, el tono de llamada, la señal de ocupado, etc.
2. Transmisión del número marcado a las centrales de conmutación, que tratarán de establecer de una conexión.
3. Transmisión de información entre los conmutadores indicando que una llamada dada no se puede establecer.
4. Transmisión de información entre conmutadores indicando que una llamada ha finalizado y que la ruta puede desconectarse.
5. Generación de la señal que hace que el teléfono suene.
6. Transmisión de información con fines de tarifación.
7. Transmisión de información indicando el estado de los equipos y líneas principales de la red. Esta información se puede emplear con fines de encaminamiento y mantenimiento.
8. Transmisión de información utilizada para el diagnóstico y aislamiento de fallos en el sistema.
9. Control de equipos especiales tales como equipos para canales vía satélite.

Como ejemplo del empleo de la señalización de control considérese la secuencia de conexión telefónica típica desde una línea a otra en la misma central:

1. Ambos teléfonos deben estar libres (colgados) antes de la llamada. Ésta empieza cuando uno de los abonados coge el auricular (descuelga), lo cual se indica automáticamente al conmutador de la central final a la que está conectado.
2. El conmutador responde con un tono audible de marcar, señalizando al abonado que puede marcar el número deseado.
3. El abonado llamante marca el número, lo cual se comunica al conmutador como la dirección del abonado de destino.
4. Si el abonado llamado no está ocupado, el conmutador lo alerta acerca de la llamada entrante enviando una señal de llamada que provoca que el teléfono suene.
5. El conmutador proporciona realimentación al abonado llamante:
   a) Si el abonado destino no está ocupado, el conmutador devuelve un tono audible de llamada al abonado origen mientras que simultáneamente se envía la señal de llamada al abonado llamado.
   b) Si el destino está ocupado, el conmutador envía una señal audible de ocupado al llamante.
   c) Si la llamada no puede establecerse a través del conmutador, éste envía un mensaje audible de «reintento» al abonado llamante.
6. El destino acepta la llamada levantando el auricular (descolgando), lo que se comunica automáticamente al conmutador.
7. El conmutador corta la señal y el tono de llamada, estableciendo una conexión entre los dos abonados.
8. La conexión se libera cuando una de las dos partes cuelga.

Cuando el abonado llamado está conectado a un conmutador diferente al que está conectado el abonado origen, son necesarias las siguientes funciones de señalización en los enlaces que unen dos conmutadores:

1. El conmutador origen ocupa un enlace libre entre ambos conmutadores, envía una indicación de descolgar a través del enlace y solicita una registro al otro conmutador para comunicar la dirección destino.

2. El conmutador final envía una señal de descolgar seguida por una de colgar, conocida como «parpadeo» o «guiño». Esto indica que el registro está preparado.
3. El conmutador origen envía los dígitos de la dirección al conmutador final.

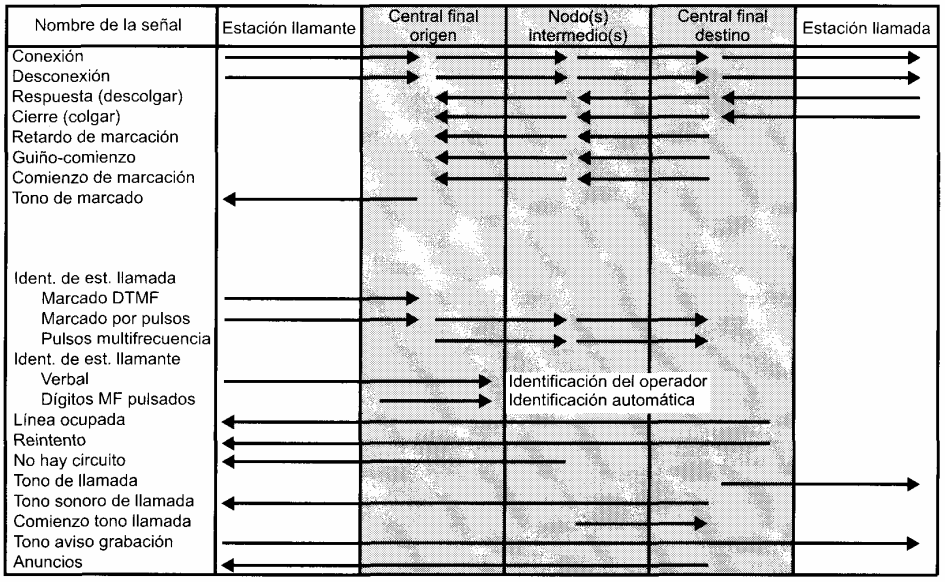
Este ejemplo ilustra algunas de las funciones realizadas por las señales de control. En la Tabla 9.1 se muestra un resumen algo más detallado. Las funciones realizadas por las señales de control se pueden agrupar básicamente las categorías de supervisión, de direccionamiento, de información sobre la llamada y de gestión de la red. En la Figura 9.10, basada en una figura dada en [FREE94], se indica el origen y el destino de algunas de las señales de control.

Desde un punto de vista funcional, la señalización también se puede clasificar en las cuatro categorías anteriores: de supervisión, de direccionamiento, de información sobre la llamada y de gestión de la red.

El término **supervisión** se emplea generalmente para referirnos a las funciones de control que tienen un carácter binario (verdadero/falso; activado/desactivado), tales como solicitud de servicio, respuesta, aviso y retorno a desocupado. Estas señales se encargan de informar acerca de la disponibilidad del abonado llamado y de los recursos de la red necesarios. Las señales de control de supervisión se usan para determinar si un recurso necesario está disponible y, si es así, reservarlo. También se utilizan para comunicar el estado de los recursos que se han solicitado.

Las señales de **direccionamiento** identifican al abonado. Inicialmente se genera una señal de dirección por parte de un abonado origen cuando marca un número de teléfono. La dirección resultante se puede propagar a través de la red para permitir el encaminamiento así como localizar y hacer que suene el teléfono del abonado destino.

El término **información sobre la llamada** se refiere a aquellas señales que proporcionan al abonado información acerca del estado de la llamada. En contraste con las señales de control interno entre conmutadores, estas señales se emplean para el establecimiento y cierre de la llamada. Estas señales inter-



Nota: Las líneas no continuas indican repetición de una señal en cada central, mientras que las líneas continuas indican la transmisión directa a través de oficinas intermedias.

Figura 9.10. Señalización de control en una red telefónica de conmutación de circuitos.

Tabla 9.1. Funciones de señalización.

DE SUPERVISIÓN

La señalización de supervisión proporciona un mecanismo de reserva de recursos para establecer una llamada. Se usa para iniciar una petición de establecimiento de llamada, para mantener o liberar una conexión establecida, para avisar a un abonado y para iniciar una llamada de cliente. Esta señalización conlleva el reconocimiento del estado ocupado o no de las líneas de abonado y de los enlaces entre centrales así como la transmisión de esta información al que realiza la llamada y al sistema de conmutación. Este tipo de señalización involucra tanto funciones de control como de estado.

De control

La señalización de supervisión se emplea para controlar el uso de los recursos. La capacidad de los enlaces y de los conmutadores se asigna a una conexión a través de las señales de supervisión. Estos recursos, una vez reservados, se mantienen durante toda la llamada y se liberan cuando termina.

De estado

La señalización de supervisión también comprende la información correspondiente al estado de una llamada establecida o sólo intentada. Esta información se envía a través de la red hacia el conmutador del abonado.

DE DIRECCIONAMIENTO

La señalización de direccionamiento proporciona el procedimiento para identificar a los abonados participantes en una llamada establecida o en un intento de llamada. Este tipo de señalización transporta información del tipo del número de teléfono del abonado que realiza la llamada o llamado y un código de área o de país o el código de acceso de un enlace PBX. Ello implica la transmisión de dígitos de un número de teléfono llamado desde un abonado a un sistema de conmutación o entre sistemas de conmutación. La señalización de direccionamiento incluye señales relacionadas con la estación y el encaminamiento.

Relativas a la estación

La señalización de direccionamiento se origina por parte del abonado que realiza la llamada. La señal se genera desde un teléfono en forma de secuencia de pulsos (marcador de dial) o como una secuencia de frecuencias de dos tonos (marcador con teclas). Para abonados digitales se deben usar señales de control digital.

Relativas al encaminamiento

Si en el establecimiento de la llamada se encuentran involucrados más de dos conmutadores, es necesario el uso de una señalización entre ellos. Esto incluye la señalización de direccionamiento, que una realiza la función de encaminamiento, y la señalización de supervisión, implicada en la reserva de recursos.

DE INFORMACIÓN SOBRE LA LLAMADA

Las señales de información de llamada se transmiten al que realizó la llamada para ofrecer tanto a éstos como a los operadores información relativa al establecimiento de una conexión a través de la red telefónica. Con este propósito se utilizan diversos tonos audibles. Estas señales se clasifican en: de aviso y de progreso.

De aviso

Las señales de alerta se proporcionan a un abonado que no participa en una llamada. Estas señales incluyen el timbre de llamada a un teléfono y el aviso al abonado cuyo teléfono está descolgado.

De progreso

Las señales de progreso de la llamada indican el estado de la llamada al abonado origen.

DE GESTIÓN DE LA RED

Las señales de gestión de red comprenden todas aquellas señales relativas al funcionamiento y gestión continuos de la red. Aquí se incluyen señales que hacen que se lleven a cabo funciones de control y señales que proporcionan información acerca del estado de la red.

De control

Las señales de control de gestión de la red se usan para controlar el proceso de selección de ruta (por ejemplo, para cambiar las rutas predefinidas de un conmutador) y para modificar las características funcionales de la red en respuesta a situaciones de sobrecarga y ocurrencia de fallos.

De estado

Las señales de estado de gestión de la red se emplean para proporcionar información de estado a los centros de gestión de red y a otros conmutadores. La información de estado incluye el volumen de tráfico, las condiciones de sobrecarga, las condiciones de error persistentes y los fallos.

nas a la red son mensajes eléctricos analógicos o digitales. En cambio, las señales de información sobre la llamada son tonos audibles que pueden ser oídos por el llamante o por un operador que disponga del equipo de teléfono apropiado.

Las señales de supervisión, de direccionamiento y de control de información sobre la llamada están directamente involucradas en el establecimiento y finalización de una llamada. Por el contrario, las señales de **gestión de la red** se utilizan para el mantenimiento, la resolución de problemas y el funcionamiento general de la red. Estas señales pueden tener forma de mensajes, como, por ejemplo, una lista de rutas predefinidas enviadas a una estación para la actualización de sus tablas de encaminamiento. Las señales de gestión de la red cubren un amplio abanico de funciones, y será esta clase de señales la que más se extenderá con la creciente complejidad de las redes conmutadas.

LOCALIZACIÓN DE LA SEÑALIZACIÓN

Es necesario considerar la señalización de control en dos contextos: la señalización entre el abonado y la red y la señalización dentro de la red. Generalmente, la señalización funciona de forma diferente en estos dos contextos.

La señalización entre un teléfono, o cualquier otro dispositivo de abonado, y la oficina de conmutación a la que se encuentra conectado se determina, en gran medida, por las características del dispositivo del abonado y por las necesidades del usuario. Las señales dentro de la red corresponden completamente a intercambios entre computadores. Esta señalización interna no se ocupa sólo de la gestión de llamadas del abonado, sino también de la gestión de la propia red. Así, para la señalización interna se necesita un conjunto de órdenes, respuestas y parámetros más complejo.

Dado que se utilizan dos técnicas de señalización diferentes, la central local de conmutación a la que está conectado el abonado debe proporcionar una correspondencia o traducción entre la técnica de señalización relativamente poco compleja usada por el abonado y la técnica de mayor complejidad utilizada internamente en la red.

SEÑALIZACIÓN POR CANAL COMÚN

La señalización de control tradicional en redes de conmutación de circuitos se ha realizado a través de la propia línea principal o intracanal. En la técnica de **señalización intracanal** se usa el mismo canal para transportar tanto las señales de control como la llamada propiamente dicha. Esta señalización comienza en el abonado origen y sigue la misma ruta que la llamada en sí.

Esto tiene la ventaja de que no se precisan servicios de transmisión adicionales para llevar a cabo la señalización; los recursos para transmisión de voz son compartidos por la señalización de control.

Existen dos formas de señalización intracanal: intrabanda y fuera de banda. La **señalización intrabanda** utiliza no sólo el mismo camino físico que la llamada a la que sirve, sino que usa también la misma banda de frecuencias que las señales de voz que se transmiten. Esta técnica de señalización presenta varias ventajas. Dado que las señales de control tiene las mismas propiedades electromagnéticas que las señales de voz, pueden llegar a los mismos lugares que éstas. Por tanto, no existe limitación alguna para el uso de la señalización intrabanda en cualquier punto de la red, incluso en aquellos sitios donde tiene lugar la conversión analógica a digital o digital a analógica. Además, es imposible establecer una llamada sobre un canal de voz con errores ya que las señales de control usadas en el establecimiento de la ruta tendrían que seguir el mismo camino.

La **señalización fuera de banda** aprovecha el hecho de que las señales de voz no utilizan completamente los 4 kHz de ancho de banda reservado para ellas, de modo que dentro de los 4 kHz se hace uso de una banda de señalización estrecha e independiente para el envío de las señales de control. La principal ventaja de esta aproximación radica en que las señales de control se pueden enviar tanto si hay como si no señales de voz en la línea, permitiéndose así la supervisión y el control continuos de la llamada. No obstante, en un esquema fuera de banda se necesita circuitería electrónica adicional para gestionar la

banda de señalización, y las velocidades de señalización son inferiores ya que la señal se ha confinado en un ancho de banda estrecho.

A medida que las redes de telecomunicaciones públicas se han hecho más complejas y ofrecen un conjunto de servicios más amplio, se hacen más evidentes las desventajas que presenta la señalización intracanal. En primer lugar, la velocidad de transferencia de información se encuentra bastante limitada. Con las señales intrabanda, un canal de voz en uso sólo puede ser utilizado por las señales de control cuando no hay señales de voz en el circuito. En la señalización fuera de banda se encuentra disponible un ancho de banda muy estrecho. Con estas limitaciones resulta difícil transmitir a tiempo el más simple de los mensajes de control. Sin embargo, se requiere un repertorio de señales de control más amplio y potente con el fin de aprovecharnos de los servicios potenciales y hacer frente a la creciente complejidad de las nuevas tecnologías de red.

Una segundo desventaja de la señalización intracanal es el retardo existente desde que un abonado introduce una dirección (marca el número) hasta que la conexión se establece. La necesidad de reducir este retardo es cada vez más importante en la medida en que las redes se están utilizando para nuevas aplicaciones. Por ejemplo, en las llamadas controladas por computador, tales como el procesamiento de transacciones, se transmiten mensajes relativamente cortos, por lo que el tiempo de establecimiento de llamada representa una parte importante del tiempo de transacción total.

Ambos problemas se pueden evitar mediante la **señalización por canal común**, en la que las señales de control se transmiten por rutas completamente independientes de los canales de voz (Tabla 9.2). Una ruta independiente para las señales de control puede transportar las señales de varios canales de abonado, siendo en consecuencia un canal de control común para todos estos canales de abonado.

El fundamento de la señalización por canal común se ilustra y compara con la señalización intracanal en la Figura 9.11. Como se puede observar, la ruta de señal para la señalización por canal común está físicamente separada de la ruta de voz u otras señales de abonado. El canal común se puede configurar con el ancho de banda necesario para transportar señales de control que lleven a cabo una gran variedad de funciones. Así, tanto el protocolo de señalización como la arquitectura de red que lo soporta son más complejos que en la señalización intracanal. Sin embargo, la reducción continua en los costes del hardware de los computadores hace que la señalización por canal común resulte cada vez más atractiva.

Tabla 9.2. Técnicas de señalización de control de redes de conmutación de circuitos.

	Descripción	**Comentario**
Intracanal		
Intrabanda	Se transmiten las señales de control en la misma banda de frecuencias usada por las señales de voz.	Es la técnica más sencilla. Es necesaria para las señales de información sobre la llamada y se puede usar para otras señales de control. La señalización intrabanda se puede utilizar sobre cualquier tipo de interfaz de línea de abonado.
Fuera de banda	Las señales de control se transmiten haciendo uso de los mismos recursos que las señales de voz, pero una parte diferente de la banda de frecuencias.	A diferencia de la señalización intrabanda, la señalización fuera de banda proporciona una supervisión continua durante toda la conexión.
Por canal común	Las señales de control se transmiten sobre canales de señalización dedicados a las señales de control, y son comunes a varios canales de voz.	Se reduce el tiempo de establecimiento de llamada en comparación con los métodos de señalización intracanal. Resulta también más adaptable a las nuevas necesidades funcionales.

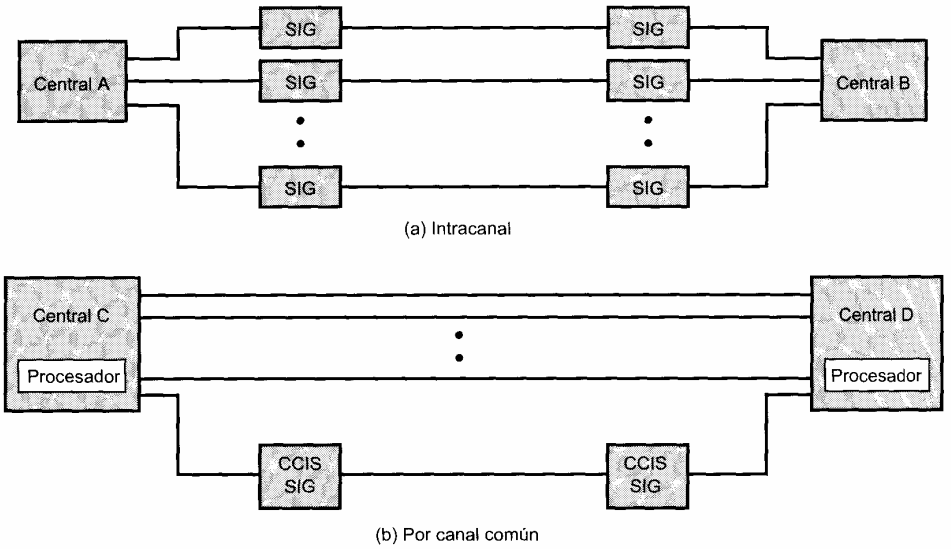


Figura 9.11. Señalización intracanal y por canal común.

Las señales de control son mensajes que se transfieren entre los conmutadores y entre el conmutador y el centro de gestión de red. De este modo, la parte de señalización de control de la red es, en efecto, una red distribuida de computadores que transporta mensajes cortos.

Existen dos modos de funcionamiento en la señalización por canal común (Figura 9.12). En el **modo asociado** el canal común sigue los pasos, a lo largo de toda la línea, a los grupos de enlace entre conmutadores a los que sirve entre los dos extremos. Las señales de control viajan en canales diferentes a los de las señales de abonado y, dentro de un mismo conmutador, las señales de control se encaminan directamente hacia un procesador de señales de control. Un modo más complejo, aunque más potente, es el **modo no asociado**. En este modo se hace crecer la red a través de la adición de nodos llamados puntos de transferencia de señal. En este caso no existe una asignación o correspondencia ni definitiva ni sencilla entre los canales de control y los grupos de enlace. En efecto, en este modo existen ahora dos redes separadas con enlaces entre ellas de modo que la parte de control de la red puede realizar sus funciones a través de los nodos de conmutación que están dando servicio a las llamadas de abonado. La gestión de la red resulta más fácil en el modo no asociado ya que los canales de control se pueden asignar a tareas de una manera más flexible. El modo no asociado es el usado en RDSI.

Con la señalización intracanal, las señales de control de un conmutador dado se generan en un procesador de control y posteriormente se conmutan sobre el canal de salida correspondiente. En el receptor, las señales de control se deben conmutar desde el canal de voz al procesador de control. En la señalización por canal común, las señales de control se transfieren directamente desde un procesador al siguiente, sin ser asociadas a un canal de voz. Este procedimiento es el más sencillo y el menos susceptible a interferencias tanto accidentales como intencionadas entre la señal del abonado y las de control. Ésta es una de las razones principales que justifican el empleo de la señalización por canal común. Otra razón importante para ello es la reducción conseguida en el tiempo de establecimiento de la llamada. Considérese la secuencia de eventos para el establecimiento de la llamada en la señalización intracanal cuando están implicados más de un conmutador. Se enviará una señal de control desde un conmutador hasta el siguiente a través de la ruta correspondiente. En cada conmutador, la señal no se transferirá hacia el siguiente enlace de la ruta hasta que no se haya establecido el circuito asociado a través de dicho conmutador.

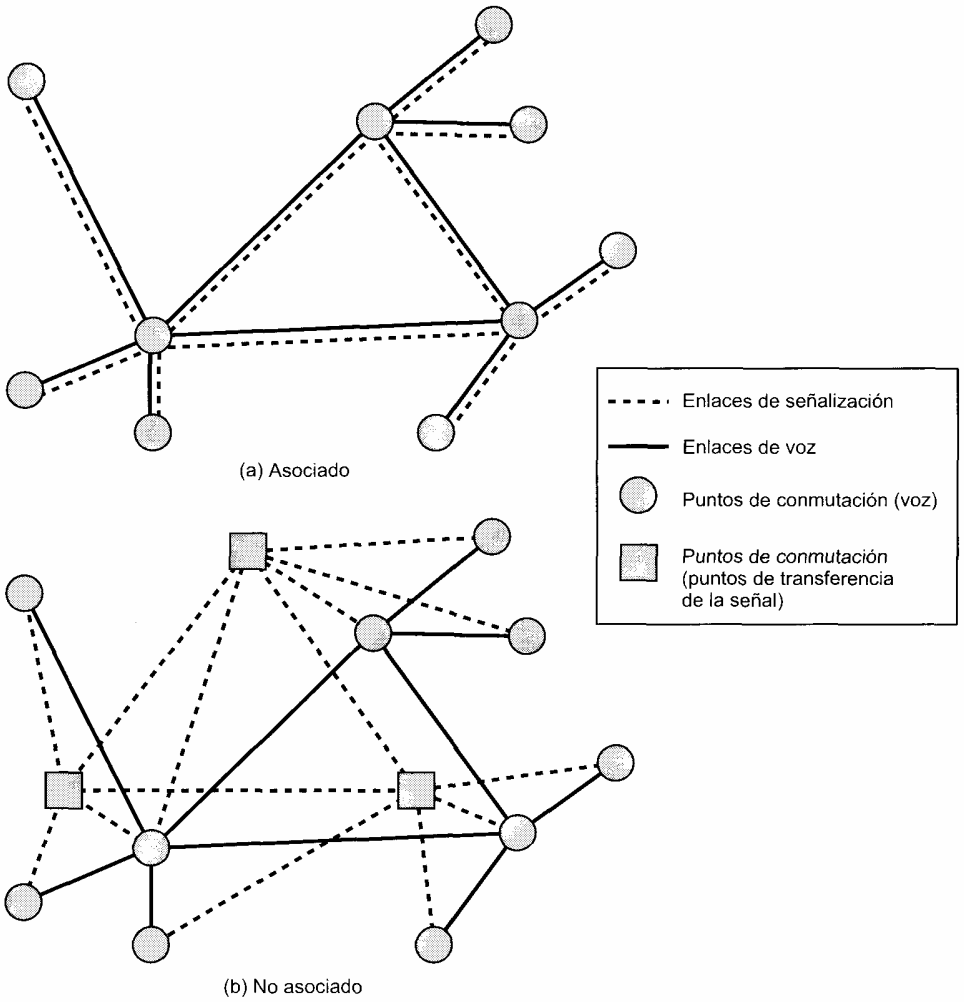


Figura 9.12. Modos de señalización por canal común [FREE96].

La retransmisión de información de control en la técnica de señalización por canal común se puede solapar con el procedimiento de establecimiento del circuito.

La señalización no asociada presenta una ventaja adicional: se pueden establecerse uno o más puntos centrales de control. Toda la información de control se puede encaminar a un centro de control de red, en el que se procesan las solicitudes y desde el que se envían las señales de control a los conmutadores que gestionan el tráfico de los abonados. De esta forma, las solicitudes se pueden procesar teniendo en cuenta una visión más global del estado de la red.

Desde luego, la señalización por canal común tiene algunas desventajas. Éstas están relacionadas en primer lugar con la complejidad de la técnica; sin embargo, la reducción de costes en el hardware digital y el creciente carácter digital de las redes de telecomunicaciones hacen que la señalización por canal común sea la tecnología apropiada.

Todo el estudio presentado a lo largo de esta sección se ha centrado en el uso de la señalización por canal común dentro de la red (es decir, para controlar los conmutadores). Incluso en el caso de que la

red esté completamente controlada mediante señalización por canal común, será necesaria alguna señalización intracanal para la comunicación con el abonado. Por ejemplo, el tono de marcar, la señal de indicación de llamada y la señal de ocupación deben ser señales intracanal dirigidas hacia el usuario. En una red telefónica sencilla, el abonado no tendrá acceso a la parte de la red señalizada por canal común, por lo que no tendrá que utilizar el protocolo correspondiente. Sin embargo, en redes digitales más sofisticadas, incluida la RDSI, se utiliza un protocolo de señalización por canal común entre el abonado y la red, que se hace corresponder con el protocolo de señalización interno.

SISTEMA DE SEÑALIZACIÓN NÚMERO 7

La señalización por canal común es más flexible y potente que la señalización intracanal y está mejor preparada para satisfacer las necesidades de las redes digitales integradas. El esquema más ampliamente usado es el Sistema de Señalización Número 7 (SS7, signaling system number 7). Si bien SS7 ha sido específicamente diseñada para su uso en redes RDSI, se ideó con ánimo ser una norma abierta de señalización por canal común que se pudiera utilizar en diversas redes de conmutación de circuitos digitales. SS7 es el mecanismo que proporciona el control interno y la inteligencia esenciales a una red RDSI.

El objetivo de SS7 es proporcionar un sistema de señalización por canal común de propósito general estandarizado internacionalmente con las siguientes características principales:

- Optimizado para su utilización en redes digitales de telecomunicaciones con nodos digitales controlados por programa y que hacen uso de canales digitales a 64 kbps.
- Diseñado para satisfacer las necesidades, tanto actuales como futuras, de transferencia de información para control de llamadas, control remoto, gestión y mantenimiento.
- Diseñado con objeto de constituir un medio seguro para la transferencia de información en el orden correcto sin pérdidas ni duplicaciones.
- Apropiado para su uso en canales analógicos a velocidades inferiores a 64 kbps.
- Adecuado para enlaces terrestres y satélite punto a punto.

El ámbito de acción del protocolo SS7 es enorme dado que cubre todos los aspectos de la señalización de control en redes digitales complejas, incluyendo el encaminamiento seguro así como el envío de mensajes de control y del contenido orientado a aplicación de los mismos. En esta sección se ofrece un breve estudio del protocolo SS7.

En SS7 los mensajes de control se encaminan a través de la red para llevar a cabo la gestión de las llamadas (establecimiento, mantenimiento, terminación) y las funciones relativas a la gestión de la red. Estos mensajes son bloques o paquetes pequeños que se pueden encaminar a través de la red, de modo que aunque la red que está siendo controlada sea una red de conmutación de circuitos, la señalización de control se basa en la tecnología de conmutación de paquetes. De hecho, la red de conmutación de circuitos se recubre por una de conmutación de paquetes para llevar a cabo el control y funcionamiento de la primera.

SS7 define las funciones realizadas en la red de conmutación de paquetes pero no especifica ninguna implementación hardware concreta. Por ejemplo, todas las funciones de SS7 se pueden implementar en los nodos de conmutación de circuitos como funciones adicionales de los mismos; esta aproximación corresponde al modo de señalización asociado mostrado en la Figura 9.12a. En la Figura 9.12b se muestra como alternativa el uso de puntos de conmutación independientes para el transporte exclusivo de los paquetes de control y no el de los circuitos. Incluso en este caso los nodos de conmutación de circuitos necesitarían implementar partes del protocolo SS7 con el fin de poder recibir señales de control.

Elementos de la red de señalización

SS7 define tres entidades funcionales: puntos de señalización, puntos de transferencia de señal y enlaces de señalización. Un **punto de señalización** (SP) es un nodo de la red de señalización con capacidad de

gestión de mensajes de control SS7. Un SP puede ser un receptor de mensajes de control incapaz de procesar mensajes que no vayan destinados directamente a él. Los nodos de conmutación de circuitos de la red podrían ser, por ejemplo, los extremos origen o destino de una comunicación. Otro ejemplo de SP lo constituye un centro de control de red. Un **punto de transferencia de señal** (STP) es un punto de señalización capaz de encaminar mensajes de control; es decir, un mensaje recibido sobre un enlace de señalización se transfiere a otro enlace. Un STP podría consistir en un nodo de encaminamiento puro, pudiendo realizar también las funciones propias de un punto final (origen/destino) de comunicaciones. Finalmente, un **enlace de señalización** es un enlace de datos que conecta entre sí puntos de señalización.

En la Figura 9.13 se evidencia la distinción entre la función de señalización mediante conmutación de paquetes y la función de transferencia de información basada en conmutación de circuitos para el caso de una arquitectura de señalización no asociada. Se puede considerar la existencia de dos planos de operación. El **plano de control** es responsable del establecimiento y de la gestión de las conexiones, las cuales se solicitan por el usuario. El diálogo entre el usuario y la red se realiza entre el usuario y el conmutador local. Con este fin, el conmutador local funciona como un punto de señalización ya que debe llevar a cabo la conversión entre el diálogo con el usuario y los mensajes de control internos a la red que son los que realmente realizan las acciones solicitadas por el usuario (SS7). El protocolo SS7 se usa internamente a la red para establecer y mantener una conexión dada; este proceso puede involucrar uno o más puntos de señalización y de transferencia de señal. Una vez se ha establecido la conexión, la información se transfiere desde un usuario hasta el otro, extremo a extremo, en el **plano de información**. Para ello se establece un circuito desde el conmutador local de un usuario hasta el del otro, habiéndose realizado quizás el encaminamiento a través de uno o más nodos de conmutación de circuitos denominados *centros de tránsito*. Todos estos nodos (conmutadores locales, centros de tránsito) son también puntos de señalización, ya que son capaces de enviar y recibir mensajes SS7 para establecer y gestionar la conexión.

Estructuras de la red de señalización

Las redes complejas disponen generalmente tanto de puntos de señalización (SP) como de puntos de transferencia de señal (STP). Una red de señalización que incluye nodos SP y nodos STP puede considerarse que tiene una estructura jerárquica en la que los SP constituyen el nivel inferior y los STP representan el nivel superior. Estos últimos pueden dividirse a su vez en varios niveles STP. En la Figura 9.13 se muestra un ejemplo correspondiente a una red con un solo nivel de STP.

Varios son los parámetros que pueden influir en las decisiones relativas al diseño de la red y al número de niveles a considerar:

- **Capacidad de los STP:** incluye el número de enlaces de señalización que puede gestionar un STP, el tiempo de transferencia de los mensajes de señalización y la capacidad de mensajes.
- **Prestaciones de la red:** comprende el número de SP y los retardos de señalización.
- **Eficacia y seguridad:** mide la capacidad de la red para proveer servicios ante la ocurrencia de fallos en los STP.

Cuando se consideran las restricciones de la red desde el punto de vista de las prestaciones, parece más adecuada la consideración de un solo nivel STP. Sin embargo, la consideración de los parámetros de eficacia y seguridad puede requerir un diseño con más de un nivel. La ITU-T sugiere las siguientes pautas:

- En una red de señalización jerárquica con un único nivel de STP:
  - — Cada SP que no sea simultáneamente un STP se conecta con al menos dos STP.
  - — El entramado de STP debe ser tan completo como sea posible, entendiendo por entramado completo aquel en el que existe un enlace directo entre cualesquiera dos STP.

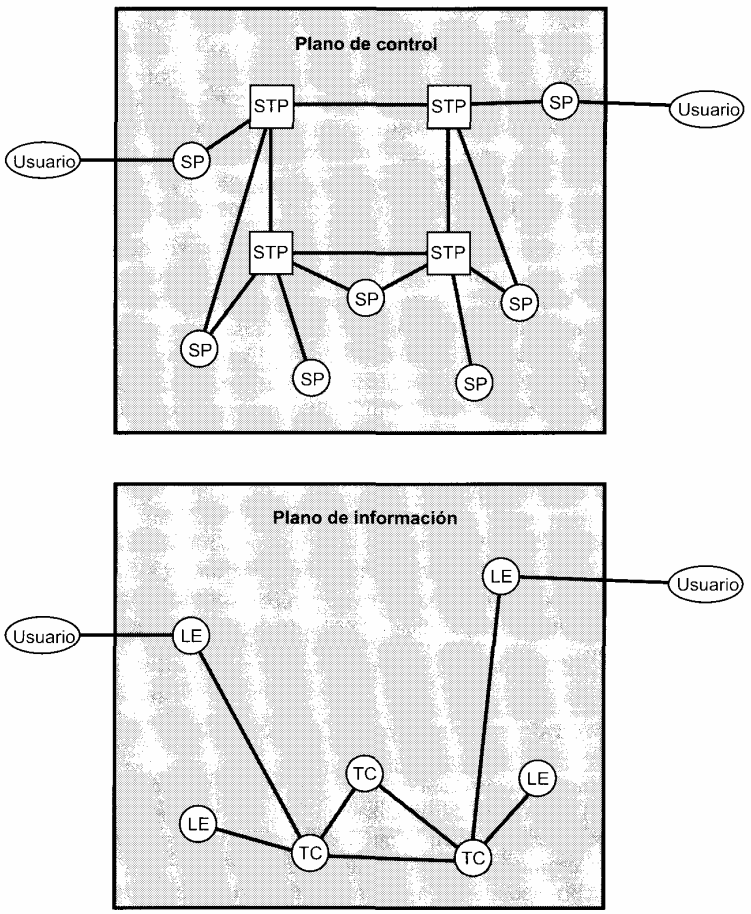


Figura 9.13. Puntos de señalización y de transferencia de información en SS7.

- En una red de señalización jerárquica con dos niveles de STP:
  - — Cada SP que no sea al mismo tiempo un STP se conecta con al menos dos STP del nivel inferior.
  - — Cada STP del nivel inferior se conecta con al menos dos STP del nivel superior.
  - — Los STP del nivel superior forman un entramado completo.

El diseño jerárquico en dos niveles de STP es generalmente tal que el nivel inferior se dedica a la gestión del tráfico correspondiente a una región geográfica particular de la red, mientras que el nivel superior gestiona el tráfico entre regiones.

9.6. LECTURAS RECOMENDADAS

Como conviene a su antigüedad, la conmutación de circuitos ha inspirado una voluminosa literatura. Dos buenos textos sobre este tema son [BELL91] y [FREE96]. En [GIRA90] se ofrece un estudio adecuado acerca del encaminamiento en redes de conmutación de circuitos. Por su parte, en [BOSS98] y [FREE98] se trata la señalización de control.

En [STAL97] se presenta en mayor detalle el protocolo SS7. Para un estudio en mayor profundidad de este protocolo resultan adecuados [BLAC97] y [RUSS95]. [BHAT97] proporciona también un tratamiento técnico detallado con especial énfasis en cuestiones de implementación práctica.

BELL91 Bellamy, J. *Digital Telephony*. New York: Wiley, 1991.

BHAT97 Bhatnagar, P. *Engineering Networks for Synchronization, CCS 7 and ISDN*. New York: IEEE Press, 1997.

BLAC97 Black, U. *ISDN and SS7: Architectures for Digital Signaling Networks*. Upper Saddle River, NJ: Prentice Hall, 1997.

BOSS98 Bosse, J. *Signaling in Telecommunication Networks*. New York: Wiley, 1998.

FREE96 Freeman, R. *Telecommunication System Engineering*. New York: Wiley, 1996.

FREE98 Freeman, R. *Telecomunications Transmission Handbook*. New York: Wiley, 1998.

GIRA90 Girard, A. *Routing and Dimensioning in Circuit-switching Networks*. Reading, MA: Addison-Wesley, 1990.

RUSS95 Russell, R. *Signaling System #7*. New York: McGraw-Hill, 1995.

STAL99 Stalling, W. *ISDN and Broadband ISDN, with Frame Relay and ATM*. Upper Saddle River, NJ: Prentice Hall, 1999.

9.7. PROBLEMAS

9.1. Suponga que la velocidad de propagación en un bus TDM es 0,8c, su longitud 10 m y la razón de datos 500 Mbps. ¿Cuántos bits se deberían transmitir en una ranura temporal para conseguir una utilización del bus del 99 %?

9.2. Considere una red telefónica sencilla consistente en dos centrales finales y un conmutador intermedio con un enlace *full-duplex* de 1 MHz entre cada una de las centrales y el conmutador intermedio. La utilización media de cada teléfono es de cuatro llamadas cada 8 horas en horario comercial, con una duración media por llamada de seis minutos. El diez por ciento de las llamadas son de larga distancia. ¿Cuál es el número máximo de teléfonos que puede soportar cada central?

9.3. ¿Sería posible realizar una implementación de SS7 basada en conmutación de circuitos en lugar de en conmutación de paquetes? ¿Cuáles serían las ventajas relativas de esta aproximación?

CAPÍTULO 10

Conmutación de paquetes

- La técnica de conmutación de paquetes se diseñó para ofrecer un servicio más eficiente que el proporcionado por la conmutación de circuitos. En la conmutación de paquetes, una estación realiza la transmisión de los datos en base a pequeños bloques llamados paquetes, cada uno de los cuales contiene una parte de los datos de usuario además de información de control necesaria para el adecuado funcionamiento de la red.
- Un elemento clave distintivo de las redes de conmutación de paquetes lo constituye el hecho de que el funcionamiento interno puede basarse en datagramas o en circuitos virtuales. En el caso de los circuitos virtuales internos se define una ruta entre dos puntos de comunicación finales o extremos, de modo que todos los paquetes para dicho circuito virtual siguen el mismo camino. Por su parte, en el caso de los datagramas internos, cada paquete se trata de forma independiente, por lo que paquetes con el mismo destino pueden seguir rutas diferentes.
- La función de encaminamiento de una red de conmutación de paquetes trata de encontrar la ruta de mínimo coste a través de la red, estando el parámetro de coste basado en el número de saltos, el retardo esperado u otras métricas. Los algoritmos de encaminamiento adaptable se fundamentan generalmente en el intercambio entre los nodos de información relativa a las condiciones de tráfico.
- X.25 es el protocolo estándar para la interfaz entre los sistemas finales y una red de conmutación de paquetes.

En torno a 1970 se ideó una nueva forma de arquitectura para comunicaciones de datos digitales de larga distancia: la conmutación de paquetes. Aunque la tecnología de esta técnica de conmutación ha evolucionado sustancialmente desde entonces, se ha de reseñar que (1) la tecnología básica en conmutación de paquetes es esencialmente la misma en la actualidad que la de las redes de principios de los años 70, y (2) la conmutación de paquetes continúa siendo una de las pocas tecnologías efectivas para comunicaciones de datos a larga distancia.

En este capítulo se presenta la tecnología de conmutación de paquetes. Se verá que muchas de las ventajas de esta tecnología (flexibilidad, compartimiento de recursos, robustez, efectividad) conllevan un coste. Una red de conmutación de paquetes es un conjunto distribuido de nodos de conmutación de paquetes, los cuales, idealmente, conocen siempre el estado de la red completa. Desgraciadamente, dado que los nodos están distribuidos, existe un tiempo de retardo entre la producción de un cambio en el estado de una parte de la red y la constatación de dicho cambio por parte de todos los nodos. Además, existe un coste adicional asociado a la comunicación de la información relativa al estado. En consecuencia, una red de conmutación de paquetes nunca funcionará «perfectamente», utilizándose complicados algoritmos para solventar el retardo temporal y los costes debidos al funcionamiento de la red. Estas mismas cuestiones aparecerán de nuevo cuando estudiemos la interconexión de redes en la Parte V del libro.

Este tema comienza con una introducción a los principios de las redes de conmutación de paquetes. A continuación se estudiará el funcionamiento interno de estas redes, presentándose los conceptos de circuito virtual y datagrama. Seguidamente se examinará la tecnología de encaminamiento. El tema concluye con una introducción a X.25, que es la interfaz estándar entre un sistema final y una red de conmutación de paquetes.

10.1. PRINCIPIOS DE CONMUTACIÓN DE PAQUETES

La red de telecomunicaciones de conmutación de circuitos de larga distancia se diseñó originalmente para el tráfico de voz, siendo aún hoy día la voz la responsable de la mayor parte del tráfico en estas redes. Una característica fundamental de las redes de conmutación de circuitos es que se dedican recursos internos de la red a una llamada particular; de este modo, para conexiones de voz, el circuito resultante alcanza un alto porcentaje de utilización dado que la mayor parte del tiempo está hablando un extremo o el otro. Sin embargo, a medida que las redes de conmutación de circuitos se han ido utilizando de forma creciente para conexiones de datos, se ponen de manifiesto dos problemas:

- En una conexión de datos usuario/estación típica (por ejemplo, un usuario de un computador personal conectado a un servidor de base de datos) la línea está desocupada la mayor parte del tiempo. Por tanto, la técnica de conmutación de circuitos resulta ineficiente para conexiones de datos.
- En una red de conmutación de circuitos la conexión ofrece una velocidad de datos constante, de modo que los dos dispositivos conectados debe transmitir y recibir a la misma velocidad. Esto limita la utilidad de la red para la interconexión de distintos tipos de computadores y estaciones de trabajo.

Para comprender cómo aborda estos problemas la conmutación de paquetes, veamos de forma breve cómo funciona esta técnica de conmutación. Los datos se transmiten en paquetes cortos, siendo 1.000 octetos un límite superior típico de la longitud de los mismos. Si un emisor tiene que enviar un mensaje de mayor longitud, éste se segmenta en una serie de paquetes (Figura 10.1). Cada paquete contiene una parte (o todas en el caso de que se trate de un mensaje corto) de los datos de usuario más cierta información de control. Esta información comprende, cómo mínimo, la información que necesita la red para encaminar el paquete a través de ella y alcanzar el destino deseado. En cada nodo de la ruta, el paquete se recibe, se almacena temporalmente y se envía al siguiente nodo.

Volvamos a la Figura 9.1, pero consideremos ahora que la red que en ella se muestra es una red de conmutación de paquetes. Supóngase que se envía un paquete desde la estación A a la estación E. El paquete incluirá información de control indicando que el destino es E. El paquete se envía desde A al nodo 4, el cual almacena el paquete, determina el siguiente nodo en la ruta (digamos 5) y pone en cola el paquete en ese enlace (enlace 4-5). Cuando el enlace está disponible, el paquete se transmite hacia el nodo 5, quien lo enviará hacia 6, y éste, finalmente, hacia E. Esta aproximación presenta varias ventajas frente a la conmutación de circuitos:

- La eficiencia de la línea es superior, ya que un único enlace entre dos nodos se puede compartir dinámicamente en el tiempo por varios paquetes. Los paquetes forman una cola y se transmiten sobre el enlace tan rápidamente como es posible. Por el contrario, en la conmutación de circuitos la capacidad temporal de un enlace se reserva a priori mediante la utilización de la técnica de

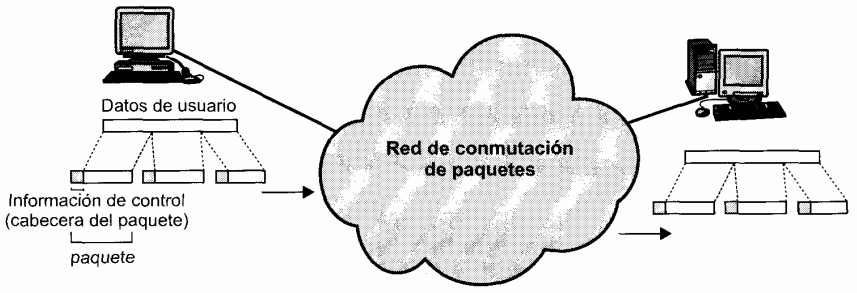


Figura 10.1. Uso de paquetes.

multiplexación por división en el tiempo síncrona, por lo que el enlace puede estar desocupado la mayor parte del tiempo dado que una parte de éste se dedica a una conexión sin datos.

- Una red de conmutación de paquetes puede realizar una conversión en la velocidad de los datos. Dos estaciones de diferentes velocidades pueden intercambiar paquetes ya que cada una se conecta a su nodo con su propia velocidad.
- Cuando aumenta el tráfico en una red de conmutación de circuitos, algunas llamadas se bloquean; es decir, la red rechaza la aceptación de solicitudes de conexión adicionales mientras no disminuya la carga de la red. En cambio, en una red de conmutación de paquetes éstos siguen aceptándose, si bien aumenta el retardo en la transmisión.
- Se puede hacer uso de prioridades, de modo que si un nodo tiene varios paquetes en cola para su transmisión, éste puede transmitir primero aquéllos con mayor prioridad. Estos paquetes experimentarán así un retardo menor que los de prioridad inferior.

TÉCNICA DE CONMUTACIÓN

Si una estación tiene que enviar un mensaje de longitud superior a la del tamaño máximo de paquete permitido a través de una red de conmutación de paquetes, ésta fragmenta el mensaje en paquetes y los envía, de uno en uno, hacia la red. La cuestión que surge es cómo gestiona la red esta secuencia de paquetes para encaminarlos a través de la red y entregarlos en el destino deseado. Existen dos aproximaciones usadas en las redes actuales: datagramas y circuitos virtuales.

En la técnica de **datagrama** cada paquete se trata de forma independiente, sin referencia alguna a los paquetes anteriores. Veamos las implicaciones de este enfoque. Supongamos que la estación A de la Figura 9.1 tiene que enviar a E un mensaje de tres paquetes. Transmite los paquetes 1, 2 y 3 al nodo 4, conteniendo cada uno de ellos la dirección del destino, E en este caso. El nodo 4 debe tomar una decisión de encaminamiento para cada paquete. El paquete 1 se recibe con destino a E, por lo que el nodo 4 podría enviar este paquete hacia el nodo 5 o hacia el nodo 7 como siguiente paso en la ruta. En este caso, el nodo 4 determina que su cola de paquetes hacia el nodo 5 es menor que la del nodo 7, de manera que pone en cola el paquete hacia el nodo 5. Igual para el paquete 2, pero en el caso del paquete 3 el nodo 4 observa que su cola hacia el nodo 7 es ahora más corta y, por tanto, envía el paquete 3 hacia este nodo. Así pues, aunque todos los paquetes tienen el mismo destino no todos siguen la misma ruta. En consecuencia, puede suceder que el paquete 3 se adelante al paquete 2, e incluso al 1, en el nodo 6. De esta forma, es posible que los paquetes se reciban en E en orden distinto al que se enviaron, siendo tarea de esta estación su reordenación. También es posible que un paquete se destruya en la red. Por ejemplo, si un nodo de conmutación de paquetes cae momentáneamente, pueden perderse todos los paquetes existentes en sus colas. Si sucediese esto con uno de los paquetes de nuestro ejemplo, el nodo 6 no tiene forma de saber que se ha perdido uno de los paquetes de la secuencia. De nuevo es misión de E detectar la pérdida de un paquete y ver la forma de recuperarlo. En esta técnica, cada paquete, tratado de forma independiente, se denomina datagrama.

En la técnica de **circuito virtual** se establece una ruta previa al envío de los paquetes. Por ejemplo, supongamos que A tiene uno o más mensajes que enviar a E. Primero envía un paquete especial de control, llamado Petición de Llamada («Call Request»), a 4 solicitando una conexión lógica a E. El nodo 4 decide encaminar la solicitud y todos los paquetes siguientes hacia 5, quien a su vez decide dirigirlos hacia 6, el cual envía finalmente el paquete Petición de Llamada a E. Si esta estación acepta la conexión, envía un paquete Llamada Aceptada («Call Accept») a 6. Este paquete se envía hacia A a través de los nodos 5 y 4. Las estaciones A y E pueden ya intercambiar datos sobre la ruta establecida. Dado que el camino es fijo mientras dura la conexión lógica, éste es similar a un circuito en redes de conmutación de circuitos y se le llama circuito virtual. Además de los datos, cada paquete contiene un identificador de circuito virtual en lugar de una dirección de destino. Cada nodo de la ruta preestablecida sabe hacia dónde dirigir los paquetes, no precisándose la toma de decisiones de encaminamiento. Así, cada uno de los paquete de datos de A a E atraviesa los nodos 4, 5 y 6, mientras que los paquetes

de E hacia A pasan por los nodos 6, 5 y 4. Eventualmente, una de las estaciones finaliza la conexión con un paquete Petición de Liberación («Clear Request»). Una estación puede disponer en un instante de tiempo dado de más de un circuito virtual hacia otra estación así como de circuitos virtuales a más de una estación.

La principal característica de la técnica de circuitos virtuales es que la ruta entre las estaciones se establece antes de la transferencia de los datos. Obsérvese que esto no significa que sea una ruta dedicada como en el caso de conmutación de circuitos. Un paquete continúa siendo almacenado en cada nodo y puesto en cola sobre una línea de salida, mientras que otros paquetes en otros circuitos virtuales pueden compartir el uso de la línea. La diferencia con la técnica de datagramas es que, con circuitos virtuales, el nodo no necesita tomar decisiones de encaminamiento para cada paquete, sino que ésta se toma una sola vez para todos los paquetes que usan dicho circuito virtual.

Si dos estaciones desean intercambiar datos durante un periodo de tiempo largo, existen ciertas ventajas al utilizar la técnica de circuitos virtuales. En primer lugar, la red puede ofrecer servicios sobre el circuito virtual, incluyendo orden secuencial y control de errores. El orden secuencial hace referencia al hecho de que, dado que los paquetes siguen la misma ruta, éstos se reciben en el mismo orden en que fueron enviados. El control de errores es un servicio que asegura que los paquetes no sólo se reciben en orden, sino que además son correctos. Por ejemplo, si un paquete en una secuencia del nodo 4 al 6 no llega a este último, o se recibe erróneamente, el nodo 6 puede solicitar al nodo 4 la retransmisión del paquete. Otra ventaja es que los paquetes viajan por la red más rápidamente haciendo uso de circuitos virtuales, ya que no es necesaria una decisión de encaminamiento para cada paquete en cada nodo.

Una ventaja del empleo de la técnica de datagrama es que no existe la fase de establecimiento de llamada. De esta forma, si una estación desea enviar sólo uno o pocos paquetes, el envío datagrama resultará más rápido. Otra ventaja del servicio datagrama es que, dado que es más rudimentario, resulta más flexible. Por ejemplo, si se produce congestión en una parte de la red, los datagramas entrantes se pueden encaminar siguiendo rutas lejanas a la zona de congestión. En la técnica de circuitos virtuales los paquetes siguen una ruta predefinida, por lo que es más difícil para la red solucionar la congestión. Una tercera ventaja es que el envío datagrama es inherentemente más seguro. Con la utilización de circuitos virtuales, si un nodo falla se perderán todos los circuitos virtuales que atraviesan ese nodo. Por el contrario, en el envío datagrama, si un nodo falla los paquetes siguientes pueden encontrar una ruta alternativa que no atraviese dicho nodo.

La mayor parte de las redes de conmutación de paquetes existentes en la actualidad hacen uso de circuitos virtuales para su funcionamiento interno. En cierta manera este hecho viene motivado por razones históricas, de modo que se posibilita a una red disponer de servicios fiables (en términos de orden secuencial) como en el caso de redes de conmutación de circuitos. Existen, sin embargo, varios proveedores de redes privadas de conmutación de paquetes que hacen uso de datagramas. Desde el punto de vista del usuario debería haber muy pocas diferencias en el funcionamiento externo de la transmisión mediante datagramas o mediante circuitos virtuales. Como se verá en la Parte V del texto, en la interconexión de redes es usual el funcionamiento basado en datagramas.

TAMAÑO DE PAQUETE

Como se muestra en la Figura 10.2, existe una relación importante entre el tamaño del paquete y el tiempo de transmisión. En este ejemplo se supone que existe un circuito virtual de la estación X a la estación Y a través de los nodos *a* y *b*. El mensaje a enviar es de 40 octetos, y cada paquete contiene 3 octetos de información de control situada al comienzo del mismo y conocida como cabecera. Si el mensaje completo se envía como un único paquete de 43 octetos (3 de cabecera y 40 octetos de datos), éste se envía primero desde la estación X hasta el nodo *a* (Figura 10.2a). Cuando se recibe el paquete completo, éste se puede transmitir de *a* a *b*. A su vez, cuando el paquete se recibe en *b*, se transfiere a la estación Y. Despreciando el tiempo de conmutación, el tiempo total de transmisión es de 129 veces el tiempo de duración de un octeto (43 octetos × 3 transmisiones del paquete).

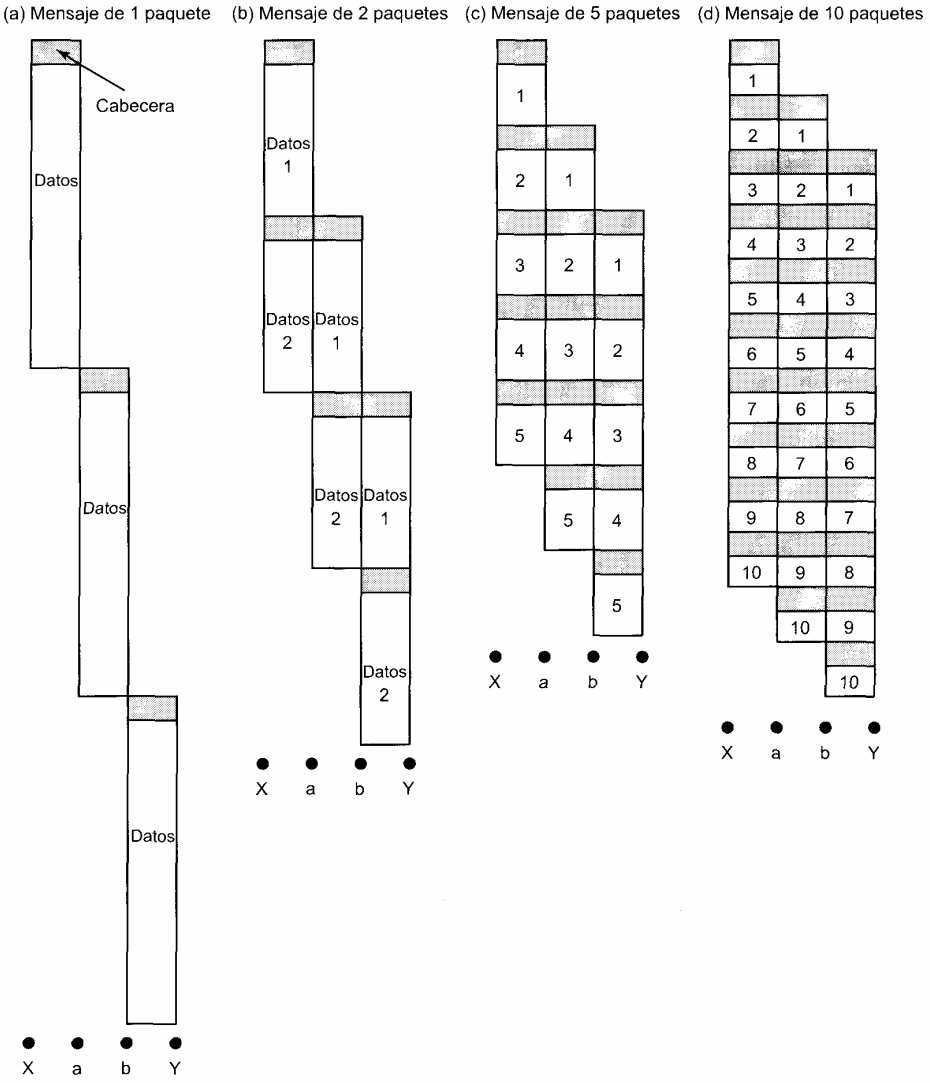


Figura 10.2. Efecto del tamaño de paquete en la transmisión.

Supongamos ahora que el mensaje se fragmenta en dos paquetes, cada uno con 20 octetos de mensaje y, claro está, 3 octetos de cabecera o de información de control. En este caso, el *nodo a* puede comenzar a transmitir el primer paquete tan pronto como se reciba desde X, sin esperar al segundo paquete. Debido a este solapamiento en la transmisión el tiempo total de ésta disminuye hasta 92 veces el tiempo de duración de un octeto. Troceando el mensaje en cinco paquetes, cada nodo intermedio puede comenzar la transmisión antes incluso, resultando superior el ahorro temporal conseguido: un total de 77 veces el tiempo de duración de un octeto. Sin embargo, tal como se ilustra en la Figura 10.2d, el proceso de usar un número de paquetes mayor y de tamaño más pequeño puede provocar un incremento, en lugar de una reducción, en el retardo. Esto se debe a que cada paquete contiene una cantidad fija de

datos de cabecera, y la existencia de más paquetes implica más cabeceras. Además, el ejemplo no muestra los retardos de procesamiento y puesta en cola en cada nodo, los cuales son también mayores cuantos más paquetes se usen para un mensaje dado. Sin embargo, veremos en el próximo capítulo que un tamaño de paquete excesivamente pequeño (53 octetos) puede dar lugar a un diseño de red eficiente.

COMPARACIÓN DE LAS TÉCNICAS DE CONMUTACIÓN DE CIRCUITOS Y DE PAQUETES

Una vez visto el funcionamiento interno de la técnica de conmutación de paquetes, a continuación se realizará una comparación de ella con la de conmutación de circuitos. En primer lugar nos centraremos en las prestaciones y después se examinarán otras características.

Prestaciones

En la Figura 10.3 se ofrece una sencilla comparación entre la conmutación de circuitos y las dos formas de conmutación de paquetes. Esta figura muestra la transmisión de un mensaje a través de cuatro nodos, desde una estación emisora conectada al nodo 1 hasta una estación de destino conectada al nodo 4. En esta figura se relacionan tres tipos de retardo:

- **Retardo de propagación:** es el tiempo que tarda la señal en propagarse desde un nodo hasta el siguiente. Este tiempo es generalmente despreciable, ya que la velocidad de las señales electromagnéticas a través de un cable, por ejemplo, es generalmente de 2×10^8 m/s.

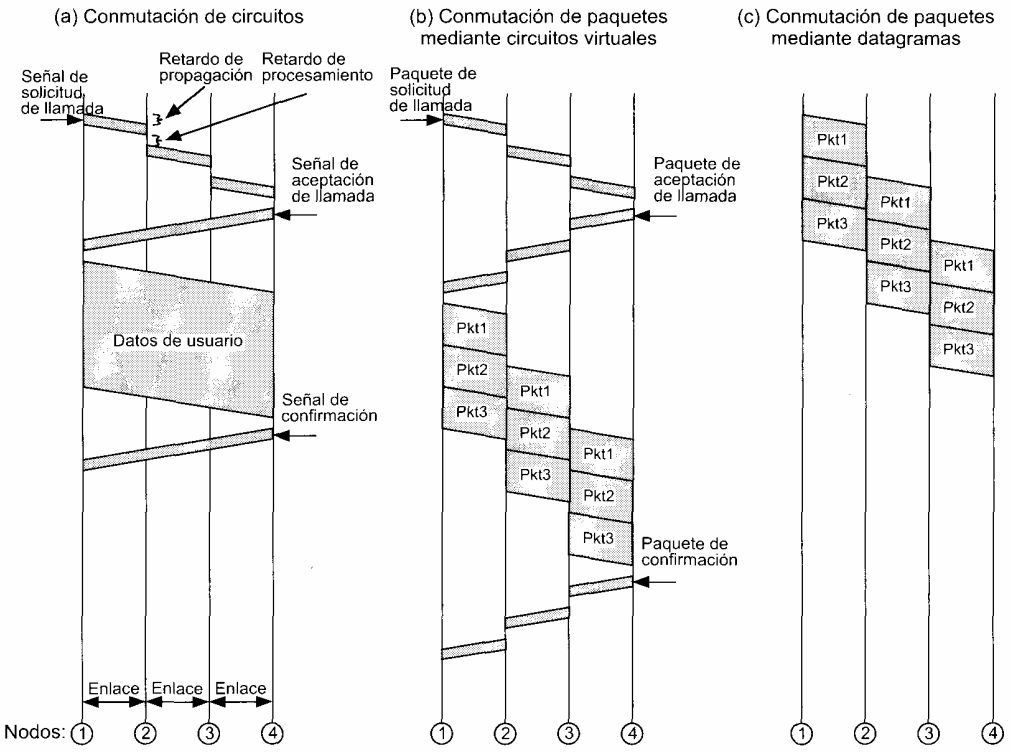


Figura 10.3. Eventos temporales en comutación de circuitos y en conmutación de paquetes.

- **Tiempo de transmisión:** es el tiempo que tarda un transmisor en enviar un bloque de datos. Por ejemplo, en una línea de 10 kbps se tarda 1 segundo en transmitir un bloque de datos de 10.000 bits.
- **Retardo de nodo:** es el tiempo que tarda un nodo en realizar los procesos necesarios para la conmutación de datos.

En conmutación de circuitos existe un cierto retardo antes de que se pueda enviar el mensaje. Primero se envía a través de la red una señal Petición de Llamada para establecer una conexión con el destino. Si la estación de destino no está ocupada, devuelve una señal Llamada Aceptada. Obsérvese la aparición de un retardo de procesamiento en cada nodo durante la solicitud de llamada, debido a la necesidad de establecer la ruta para la conexión. A la vuelta no se requiere procesamiento dado que la conexión está ya establecida. Una vez establecida la conexión, el mensaje se envía como un único bloque, sin retardos en los nodos de conmutación.

La técnica de conmutación de paquetes mediante circuitos virtuales parece muy similar a la de conmutación de circuitos. Un circuito virtual se solicita mediante el uso de un paquete Petición de Llamada, lo que provoca un retardo en cada nodo. El circuito virtual se acepta mediante un paquete Llamada Aceptada. Al contrario que en el caso de conmutación de circuitos, la aceptación de llamada también experimenta retardos en los nodos aunque la ruta del circuito virtual se encuentre ya establecida. La razón es que el paquete se pone en cola en cada nodo y debe esperar turno para su transmisión. Una vez establecido el circuito virtual, el mensaje se transmite en paquetes. Debería quedar claro que esta operación no puede ser más rápida, para redes comparables, que en el caso de la conmutación de circuitos. Este hecho de debe a que la conmutación de circuitos es esencialmente un proceso transparente, proporcionándose una velocidad de datos constante a través de la red. La conmutación de paquetes involucra cierto retardo en cada nodo de la ruta; peor aún, este retardo es variable y aumenta con la carga.

La técnica de conmutación de paquetes mediante datagramas no precisa un establecimiento de la llamada, de modo que para mensajes cortos resulta más rápida que la conmutación de paquetes mediante circuitos virtuales y, quizás, que la conmutación de circuitos. Sin embargo, dado que cada datagrama individual se encamina de forma independiente, el procesamiento de cada uno de ellos en cada nodo puede llegar a ser superior que en el caso de circuitos virtuales. Por tanto, para mensajes grandes, la técnica de circuitos virtuales puede ser mejor.

A partir de la Figura 10.3 se pueden comprender aproximadamente las prestaciones relativas de las distintas técnicas. Las prestaciones reales dependen de varios factores como el tamaño de la red, su topología, la carga y las características de cambios típicos.

Otras características

Además de las prestaciones existen numerosas características adicionales que se pueden tomar en consideración para llevar a cabo la comparación de las técnicas estudiadas. En la Tabla 10.1 se resumen las más importantes. Aunque algunas de ellas ya se han visto, a continuación se presentan unos breves comentarios adicionales.

Como se ha mencionado, la conmutación de circuitos es esencialmente un servicio transparente. Una vez que la conexión se ha establecido, se ofrece una velocidad de datos constante a las estaciones conectadas. Éste no es el caso de la conmutación de paquetes, en donde aparece generalmente un retardo variable y, en consecuencia, los datos no se reciben de forma constante. Además, en conmutación de paquetes mediante datagramas los datos pueden llegar en orden diferente al que fueron enviados.

Una consecuencia adicional de la transparencia es que no se precisa un coste extra para proveer de conmutación de circuitos. Una vez que se ha establecido la conexión, los datos analógicos o digitales van desde el origen hasta el destino. En conmutación de paquetes, los datos analógicos deben convertirse a digital antes de su transmisión; además, cada paquete incluye bits suplementarios relativos por ejemplo a la dirección de destino.

Tabla 10.1. Comparación de técnicas de conmutación en comunicaciones

Conmutación de circuitos	Conmutación de paquetes mediante datagramas	Conmutación de paquetes mediante circuitos virtuales
Ruta de transmisión dedicada	*Ruta no dedicada*	*Ruta no dedicada*
Transmisión de datos continua	Transmisión de paquetes	Transmisión de paquetes
Suficientemente rápida para aplicaciones interactivas	Suficientemente rápida para aplicaciones interactivas	Suficientemente rápida para aplicaciones interactivas
Los mensajes no se almacenan	Los paquetes se pueden almacenar hasta su envío	Los paquetes se almacenan hasta su envío
La ruta se establece para toda la conversación	La ruta se establece para cada paquete	La ruta se establece para toda la conversación
Existe retardo de establecimiento de la llamada; retardo de transmisión despreciable	Retardo de transmisión de paquetes	Existe retardo de establecimiento de la llamada y de transmisión de los paquetes
Uso de señal de ocupado si la parte llamada está ocupada	Se puede notificar al emisor acerca de que un paquete no se ha enviado	Se notifica al emisor sobre la denegación de conexión
La sobrecarga puede bloquear el establecimiento de la *llamada; no existe retardo en* las llamadas ya establecidas	La sobrecarga aumenta el retardo de paquete	La sobrecarga puede bloquear el establecimiento de la *llamada; aumenta el retardo* de paquete
Conmutación electromecánica o computerizada	Nodos de conmutación pequeños	Nodos de conmutación pequeños
El usuario es el responsable de la protección ante pérdidas del mensaje	La red puede ser la responsable de paquetes individuales	La red puede ser la responsable de secuencias de paquetes
No existe generalmente conversión de velocidad ni de código	Existe conversión de velocidad y de código	Existe conversión de velocidad y de código
Ancho de banda fijo	Uso dinámico del ancho de banda	Uso dinámico del ancho de banda
No existen bits suplementarios tras el establecimiento de la llamada	Uso de bits suplementarios en cada paquete	Uso de bits suplementarios en cada paquete

FUNCIONAMIENTO EXTERNO E INTERNO

Una de las características más importantes de una red de conmutación de paquetes es el uso de datagramas o de circuitos virtuales. Realmente, como se muestra en las Figuras 10.4 y 10.5, existen dos dimensiones de esta característica. En la interfaz entre una estación y un nodo de red, la red puede ofrecer tanto un servicio orientado a conexión como uno no orientado a conexión. En un servicio orientado a conexión la estación realiza una solicitud de llamada para establecer una conexión lógica con otra estación. Todos los paquetes enviados hacia la red se identifican como pertenecientes a una conexión lógica

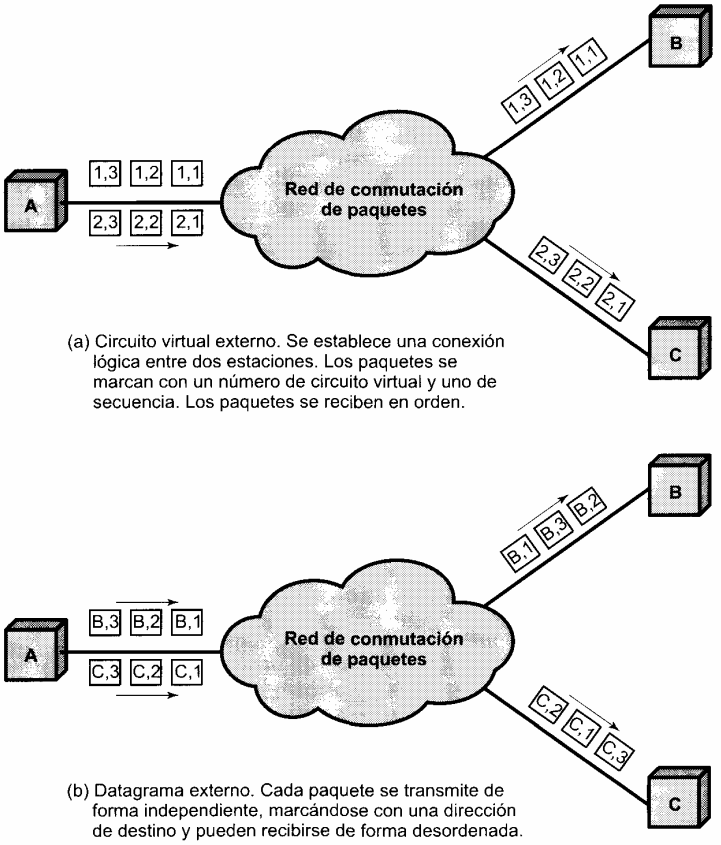


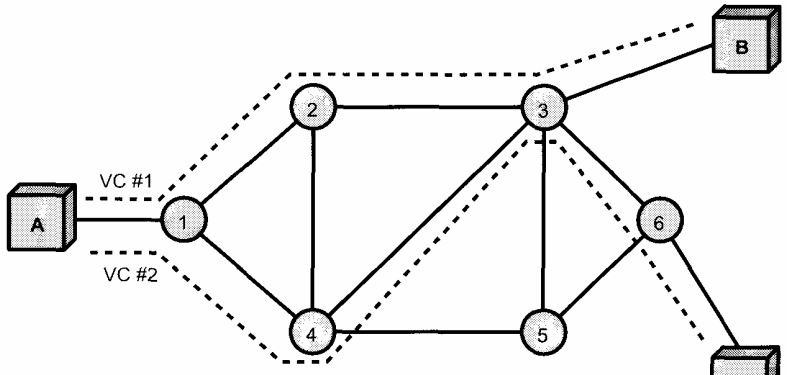
Figura 10.4. Operación de circuito virtual y de datagrama externos.

dada y se numeran secuencialmente de modo que la red los envía en este orden. La conexión lógica se denomina usualmente circuito virtual, mientras que el servicio orientado a conexión se conoce como **servicio de circuito virtual externo.** Desgraciadamente, como se verá, este servicio externo es distinto del concepto de **operación de circuito virtual interno.** Un ejemplo importante de un servicio de circuito virtual externo es X.25, que se estudiará en la Sección 10.3.

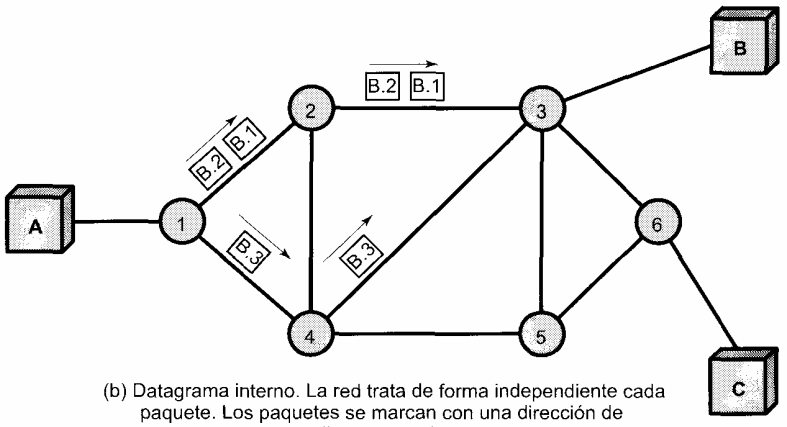
En un servicio no orientado a conexión la red gestiona los paquetes de forma independiente, pudiendo enviarlos desordenada o inadecuadamente. Este tipo de servicio se conoce a veces como **servicio de datagrama externo;** de nuevo, este concepto es distinto del de **operación de datagrama interno.** Internamente, la red puede construir (circuito virtual) o no (datagrama) una ruta fija entre el origen y el destino.

Estas decisiones de diseño interno y externo no necesitan ser coincidentes:

- **Circuito virtual externo, circuito virtual interno:** cuando el usuario solicita un circuito virtual se crea una ruta dedicada a través de la red, de forma que todos los paquetes siguen ese mismo camino.
- **Circuito virtual externo, datagrama interno:** la red gestiona cada paquete de forma separada, de modo que los distintos paquetes correspondientes a un mismo circuito virtual externo pueden



(a) Circuito virtual interno. Se define y se marca una ruta para los paquetes entre dos estaciones. Todos los paquetes de dicho circuito virtual siguen la misma ruta y se reciben en el destino en el mismo orden.



(b) Datagrama interno. La red trata de forma independiente cada paquete. Los paquetes se marcan con una dirección de destino y pueden recibirse desordenadamente en el nodo de destino.

Figura 10.5. Operación de circuito virtual y de datagrama internos.

seguir rutas diferentes. No obstante, si es necesario, la red almacena temporalmente los paquetes en el nodo de destino con objeto de enviarlos en el orden adecuado hacia la estación de destino.

- **Datagrama externo, datagrama interno:** cada paquete se trata de forma independiente tanto desde el punto de vista del usuario como desde el de la red.
- **Datagrama externo, circuito virtual interno:** el usuario externo no ve conexión alguna, limitándose a enviar paquetes a lo largo del tiempo. En cambio, la red establece una conexión lógica entre estaciones para el envío de paquetes, pudiéndose mantener esta conexión durante un largo periodo de tiempo con objeto de satisfacer futuras necesidades.

La cuestión que se plantea es si elegir circuitos virtuales o datagramas, tanto interna como externamente. Esto dependerá de los objetivos específicos en el diseño de la red de comunicaciones y de los factores de coste prioritarios. Ya se han realizado algunos comentarios acerca de las ventajas de la operación de datagrama interno frente a la de circuito virtual. Con respecto al servicio externo se pueden hacer las siguientes observaciones. El servicio datagrama, relacionado con la operación de datagrama interno, permite un uso eficiente de la red, no siendo necesario un nuevo establecimiento de llamada ni

el almacenamiento de los paquetes si se retransmite uno erróneo. Esta última característica resulta deseable para algunas aplicaciones en tiempo real. El servicio de circuito virtual permite un control del orden secuencial y de errores extremo a extremo. Este servicio resulta atractivo para aplicaciones orientadas a conexión tales como transferencia de ficheros y acceso a terminales remotos. En la práctica, el servicio de circuito virtual es mucho más común que el de datagrama, ya que la fiabilidad y la conveniencia de un servicio orientado a conexión resultan más atractivas que las ventajas del servicio datagrama.

10.2. ENCAMINAMIENTO

Uno de los aspectos más complejos y cruciales del diseño de redes de conmutación de paquetes es el encaminamiento. Este apartado comienza con una revisión de las principales características que se pueden usar para clasificar las estrategias de encaminamiento. Tras esto se discutirán algunas estrategias concretas.

Los principios descritos en esta sección son también aplicables al encaminamiento en la interconexión de redes discutida en la Parte V del libro.

CARACTERÍSTICAS

La función primordial de una red de conmutación de paquetes es aceptar paquetes procedentes de una estación emisora y enviarlos hacia una estación destino. Para ello se debe determinar una ruta o camino a través de la red, siendo posible generalmente la existencia de más de uno. Así pues, se debe realizar una función de encaminamiento. Los requisitos de esta función comprenden:

- Exactitud
- Simplicidad
- Robustez
- Estabilidad
- Imparcialidad
- Optimización
- Eficiencia

Las dos primeras características en la lista se explican por sí mismas. La robustez está relacionada con la habilidad de la red para enviar paquetes de alguna forma ante la aparición de fallos localizados y sobrecargas. Idealmente, la red puede reaccionar ante estas contingencias sin sufrir pérdidas de paquetes o caída de circuitos virtuales. La robustez puede implicar cierta inestabilidad. Las técnicas que reaccionan ante condiciones cambiantes presentan una tendencia no deseable a reaccionar demasiado lentamente ante determinados eventos o a experimentar oscilaciones inestables de un extremo a otro. Por ejemplo, la red puede reaccionar ante la aparición de congestión en un área desplazando la mayor parte de la carga hacia una segunda zona. Ahora será la segunda región la que estará sobrecargada y la primera infrautilizada, produciéndose un segundo desplazamiento del tráfico. Durante estos desplazamientos puede ocurrir que los paquetes viajen en bucles a través de la red.

También existe un compromiso entre imparcialidad y el hecho de que el encaminamiento trate de ser óptimo. Algunos criterios de funcionamiento pueden dar prioridad al intercambio de paquetes entre estaciones vecinas frente al intercambio realizado entre estaciones distantes, lo cual puede maximizar la eficiencia promedio pero será injusto para aquella estación que necesite comunicar principalmente con estaciones lejanas.

Finalmente, una técnica de encaminamiento implica cierto coste de procesamiento en cada nodo y, en ocasiones, también un coste en la transmisión, impidiéndose en ambos casos el funcionamiento eficiente de la red. Este coste debe ser inferior a los beneficios obtenidos por el uso de una métrica razonable tal como la mejora de la robustez o la imparcialidad.

Con estos requisitos en mente estamos en condiciones de evaluar los distintos elementos de diseño involucrados en una estrategia de encaminamiento. En la Tabla 10.2 se listan estos elementos. Algunos de los elementos se solapan o dependen de otros, pero un estudio acerca de ellos clarificará y permitirá organizar los conceptos de encaminamiento.

Tabla 10.2. Elementos de técnicas de encaminamiento en redes de conmutación de paquetes.

Criterios de funcionamiento	**Fuente de información de la red**
Número de saltos	Ninguna
Coste	Local
Retardo	Nodo adyacente
Eficiencia	Nodos a lo largo de la ruta
	Todos los nodos
Instante de decisión	
Paquete (datagrama)	**Tiempo de actualización de la información de la red**
Sesión (circuitos virtuales)	Continuo
	Periódico
Lugar de decisión	Cambio importante en la carga
Cada nodo (distribuido)	Cambio en la topología
Nodo central (centralizado)	
Nodo origen (fuente)	

Criterios de funcionamiento

La elección de una ruta se fundamenta generalmente en algún criterio de funcionamiento. El más simple consiste en elegir el camino con menor número de saltos (aquel que atraviesa el menor número de nodos) a través de la red[1]. Éste es un criterio que se puede medir fácilmente y que debería minimizar el consumo de recursos de la red. Una generalización del criterio de menor número de saltos lo constituye el encaminamiento de mínimo coste. En este caso se asocia un coste a cada enlace y, para cualesquiera dos estaciones conectadas, se elige aquella ruta a través de la red que implique el coste mínimo. Por ejemplo, en la Figura 10.6 se muestra una red en la que las dos líneas con flecha entre cada par de nodos representa un enlace entre ellos, y los números asociados representan el coste actual del enlace en cada sentido. El camino más corto (menor número de saltos) desde el nodo 1 hasta el 6 es 1-3-6 (coste = 5+5 = 10), pero el de mínimo coste es 1-4-5-6 (coste = 1 + 1 + 2 = 4). Los costes se asignan a los enlaces en función de los objetivos de diseño. Por ejemplo, el coste podría estar inversamente relacionado con la velocidad (es decir, a mayor velocidad menor coste) o con el retardo actual de la cola asociada al enlace. En el primer caso, la ruta de mínimo coste maximizaría la eficiencia, mientras que en el segundo se minimizaría el retardo.

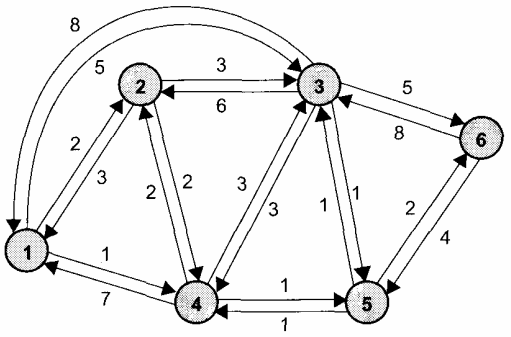


Figura 10.6. Ejemplo de red de conmutación de paquetes.

[1] El término *salto* se usa con cierta libertad en la bibliografía. La definición más común, usada en este texto, es que el número de saltos a lo largo de una ruta entre un origen y un destino dados es el número de nodos de la red (nodos de conmutación de paquetes, conmutadores ATM, dispositivos de encaminamiento, etc.) que encuentra un paquete a lo largo de dicha ruta. El número de saltos es igual a veces al número de enlaces, o terminales de grafo, atravesados. A partir de esta última definición se obtiene un valor superior en uno al conseguido mediante la definición aceptada en nuestro caso.

Tanto en la técnica de menor número de saltos como en la de mínimo coste, el algoritmo para determinar la ruta o camino óptimo entre dos estaciones es relativamente justo, siendo el tiempo de procesamiento aproximadamente el mismo en ambos casos. Dada su mayor flexibilidad, el criterio de mínimo coste es más utilizado que el de menor número de saltos.

Existen varios algoritmos de mínimo coste de uso común, los cuales se describen en el Apéndice 10A.

Instante y lugar de decisión

Las decisiones de encaminamiento se realizan de acuerdo con algún criterio de funcionamiento. Dos cuestiones importantes de esta decisión son el instante temporal y el lugar en que se toma la decisión.

El instante de decisión viene determinado por el hecho de que la decisión de encaminamiento de hace en base a un paquete o a un circuito virtual. Cuando la operación interna de la red es mediante datagramas, la decisión de encaminamiento se toma de forma individual para cada paquete. En el caso de circuitos virtuales internos, la decisión sólo se realiza en el momento en que se establece un circuito virtual dado, de modo que, en el caso más sencillo, todos los paquetes siguientes que usan ese circuito virtual siguen la misma ruta. En redes más complejas, la red puede cambiar dinámicamente la ruta asignada a un circuito virtual particular en respuesta a condiciones cambiantes (por ejemplo, sobrecarga o fallos en una parte de la red).

El término *lugar de decisión* hace referencia al nodo o nodos en la red responsables de la decisión de encaminamiento. El más común es el encaminamiento distribuido, en el que cada nodo de la red tiene la responsabilidad de seleccionar un enlace de salida sobre el que llevar a cabo el envío de los paquetes a medida que éstos se reciben. En el encaminamiento centralizado la decisión se toma por parte de algún nodo designado al respecto como puede ser un centro de control de red. El peligro de esta última aproximación es que el fallo del centro de control de la red puede bloquear el funcionamiento de la red; así, aunque la aproximación distribuida puede resultar más compleja es también más robusta. Una tercera alternativa empleada en algunas redes es la conocida como encaminamiento del origen. En este caso es la estación origen y no los nodos de la red quien realmente toma la decisión de encaminamiento, comunicándosela a la red. Esto permite al usuario fijar una ruta a través de la red de acuerdo con criterios locales al mismo.

El instante y el lugar de decisión son variables de diseño independientes. Por ejemplo, supongamos que el lugar de decisión en la Figura 10.6 es cada nodo y que los valores especificados son los costes en un instante de tiempo dado, los cuales pueden cambiar. Un paquete desde el nodo 1 al 6 podría seguir la ruta 1-4-5-6, estando cada enlace de la ruta determinado localmente por el nodo transmisor. Supongamos ahora que los valores cambian de forma que 1-4-5-6 ya no es el camino óptimo. En una red datagrama, el paquete siguiente puede seguir una ruta diferente, de nuevo determinada por cada nodo a lo largo del camino. En una red de circuitos virtuales, cada nodo recuerda la decisión de encaminamiento tomada cuando se estableció el circuito virtual, de modo que se limita a transmitir los paquetes sin tomar decisiones nuevas.

Fuente de información de la red y tiempo de actualización

La mayor parte de las estrategias de encaminamiento requieren que las decisiones se tomen en base al conocimiento de la topología de la red, la carga y el coste de los enlaces. Sorprendentemente, algunas estrategias como la de inundaciones y el encaminamiento aleatorio (descritas más adelante) no hacen uso de ninguna información para la transmisión de los paquetes.

En el encaminamiento distribuido, en el que la decisión de encaminamiento se toma en cada uno de los nodos, éstos hacen uso de información local como es el coste asociado los distintos enlaces de salida; también pueden utilizar información de los nodos adyacentes (directamente conectados), tal como la congestión experimentada en cada nodo. Finalmente, existen algoritmos de uso común que permiten al nodo obtener información de todos los nodos de una potencial ruta de interés. En el caso del encaminamiento centralizado, el nodo central hace uso generalmente de información procedente de todos los nodos.

Un concepto relacionado es el de tiempo de actualización de la información, el cual es función de la fuente de información y de la estrategia de encaminamiento. Es claro que si no se usa información (como en el método de inundaciones) no existe actualización. Si sólo se utiliza información local, la actualización es esencialmente continua ya que un nodo individual conoce siempre sus condiciones locales actuales. Para el resto de categorías de fuentes de información (nodos adyacentes, todos los nodos), el tiempo de actualización depende de la estrategia de encaminamiento. Para una estrategia de encaminamiento estático la información no se actualiza nunca, mientras que para una técnica adaptable la actualización se lleva a cabo periódicamente a fin de posibilitar la adaptación de la decisión de encaminamiento a las condiciones cambiantes de la red.

Como cabe esperar, cuanto mayor sea la información disponible y más frecuentemente se actualice, más probable será que las decisiones de encaminamiento tomadas por la red sean buenas. Eso sí, teniendo presente que la transmisión de esta información consumirá recursos de red.

ESTRATEGIAS DE ENCAMINAMIENTO

Existen numerosas estrategias de encaminamiento para abordar las necesidades de encaminamiento en redes de conmutación de paquetes. Muchas de ellas son aplicables también al encaminamiento en la interconexión de redes, estudiada en la Parte V del texto. En este apartado se presentan cuatro estrategias principales: estática, inundaciones, aleatoria y adaptable.

Encaminamiento estático

En el encaminamiento estático se configura una única y permanente ruta para cada par de nodos origen-destino en la red, pudiéndose utilizar para ello cualquiera de los algoritmos de encaminamiento de mínimo coste descritos en el Apéndice 10A. Las rutas son fijas, o al menos mientras lo sea la topología de la red. Así, los costes de enlace usados para el diseño de las rutas no pueden estar basados en variables dinámica tales como el tráfico, aunque sí podrían estarlo en tráfico esperado o en capacidad.

La Figura 10.7 sugiere cómo se pueden implementar rutas estáticas. Se crea una matriz de encaminamiento central, almacenada, por ejemplo, en un centro de control de red. Esta matriz especifica, para cada par de nodos origen-destino, la identidad del siguiente nodo en la ruta.

Obsérvese que no es necesario almacenar la ruta completa para cada par de nodos; es suficiente conocer, para cada pareja, cuál es el primer nodo en la ruta. Para comprender mejor este hecho supongamos que la ruta de mínimo coste desde X hasta Y comienza con el enlace X-A. Llamemos R_1 al resto de la ruta: parte desde A hasta Y, y definamos R_2 como la ruta de mínimo coste de A a Y. Si el coste de R_1 es mayor que el de R_2, la ruta X-Y mejorará al usar R_2 en lugar de R_1. Si el coste de R_1 es menor que el de R_2, entonces esta última ruta no es la de mínimo coste desde A hasta Y. Por tanto, $R_1 = R_2$. Así pues, en cada punto a lo largo del camino sólo es necesario conocer la identidad del nodo siguiente, no la ruta completa. En nuestro ejemplo, la ruta desde el nodo 1 al nodo 6 atraviesa en primer lugar el nodo 4. Consultando de nuevo la matriz se observa que la ruta del nodo 4 al 6 atraviesa el nodo 5. Por último, la ruta desde el nodo 5 hasta el 6 es un enlace directo a este último nodo. Por tanto, la ruta completa desde el nodo 1 al 6 es 1-4-5-6.

A partir de esta matriz se pueden crear y almacenar en cada nodo las tablas de encaminamiento asociadas. Siguiendo el razonamiento del párrafo anterior, cada nodo sólo necesitará almacenar una sola columna de la tabla de encaminamiento, indicándose en ella el nodo siguiente para cada destino.

En el encaminamiento estático no existe diferencia entre el uso de datagramas y de circuitos virtuales, ya que todos los paquetes procedentes de un origen dado y con un destino concreto siguen la misma ruta. La ventaja del encaminamiento estático es su simplicidad, además de su buen funcionamiento en redes fiables con carga estacionaria. Su desventaja radica en la falta de flexibilidad, ya que no reacciona ante fallos ni congestión en la red.

MATRIZ DE ENCAMINAMIENTO CENTRAL

Nodo destino \ Nodo origen	1	2	3	4	5	6
1	—	1	5	2	4	5
2	2	—	5	2	4	5
3	4	3	—	5	3	5
4	4	4	5	—	4	5
5	4	4	5	5	—	5
6	4	4	5	5	6	—

Tabla del nodo 1

Destino	Nodo siguiente
2	2
3	4
4	4
5	4
6	4

Tabla del nodo 2

Destino	Nodo siguiente
1	1
3	3
4	4
5	4
6	4

Tabla del nodo 3

Destino	Nodo siguiente
1	5
2	5
4	5
5	5
6	5

Tabla del nodo 4

Destino	Nodo siguiente
1	2
2	2
3	5
5	5
6	5

Tabla del nodo 5

Destino	Nodo siguiente
1	4
2	4
3	3
4	4
6	6

Tabla del nodo 6

Destino	Nodo siguiente
1	5
2	5
3	5
4	5
5	5

Figura 10.7. Encaminamiento estático (haciendo uso de la Figura 10.6).

Una mejora al encaminamiento estático que soportaría la no disponibilidad temporal de nodos y enlaces consiste en la especificación de nodos siguientes alternativos para cada dirección. Por ejemplo, los nodos alternativos en la tabla del nodo 1 podrían ser 4, 3, 2, 3, 3.

Inundaciones

Otra técnica de encaminamiento sencilla es la de inundaciones, la cual no precisa de ninguna información sobre la red y funciona como sigue. Un nodo origen envía un paquete a todos sus nodos vecinos, los cuales, a su vez, lo envían sobre todos los enlaces de salida excepto por el que llegó. Por ejemplo, si el nodo 1 de la Figura 10.6 tiene que enviar un paquete al nodo 6, envía una copia (con la dirección de destino de 6) a los nodos 2, 3 y 4. El nodo 2 enviará una copia a los nodos 3 y 4; el nodo 4 enviará a su vez una copia a los nodos 2, 3 y 5; y así sucesivamente. Dado que eventualmente el nodo 6 recibirá varias copias del paquete, éste debe contener un identificador único (por ejemplo, nodo origen y número de secuencia o número de circuito virtual y número de secuencia) para que el nodo destino pueda quedarse con una sola copia y descartar el resto.

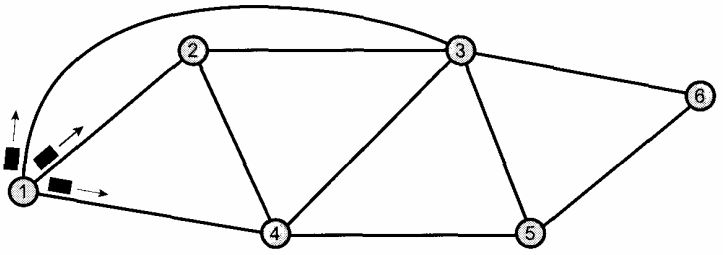
A menos que se haga algo para cesar las continuas retransmisiones de paquetes, el número de éstos en circulación para un mismo paquete origen crece sin límite. Una forma de prevenir estas retransmisiones consiste en que cada nodo recuerde la identidad de los paquetes que ha retransmitido con anterioridad, de manera que se rechazan copias duplicadas. Una técnica más sencilla consiste en incluir un campo de cuenta de saltos en cada paquete. Este contador puede ponerse inicialmente a un valor máximo como es por ejemplo el diámetro de la red (longitud de la ruta de menor número de saltos más larga a

través de la red). Cada vez que un nodo transmite un paquete decrementa la cuenta en uno, de modo que cuando el contador alcanza el valor cero se elimina el paquete de la red.

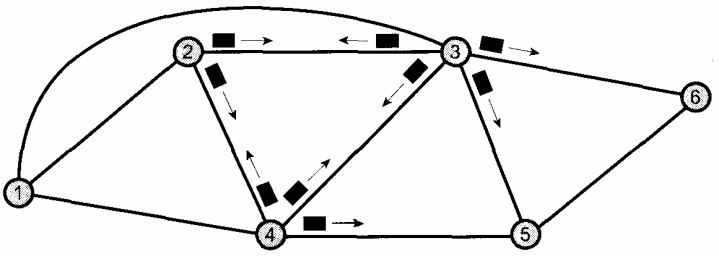
Un ejemplo de esta última técnica se muestra en la Figura 10.8. Supongamos que se envía un paquete desde el nodo 1 al nodo 6 y se le asigna una cuenta de saltos igual a 3. En el primer salto se crean tres copias del paquete; en el segundo salto de estas copias se crea un total de nueve copias. Una de estas copias alcanza el nodo 6, quien, al detectar que el destino es él, no la retransmite. Sin embargo, los otros nodos generan un total de 22 nuevas copias en el tercer y último salto. Obsérvese que si un nodo no guarda el identificador del paquete puede generar múltiples copias en este tercer paso. Todos los paquetes recibidos tras el tercer salto son eliminados, habiéndose recibido en el nodo 6 un total de cuatro copias adicionales del paquete.

La técnica de inundaciones presenta tres propiedades importantes:

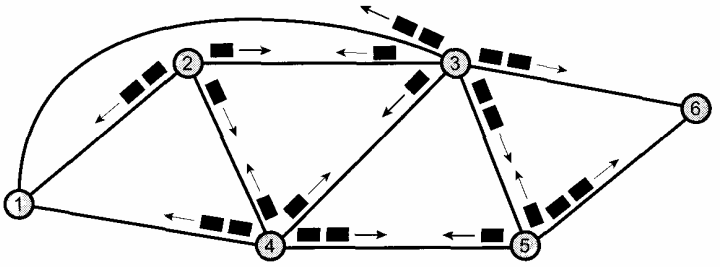
- Se prueban todos los posibles caminos entre los nodos origen y destino. De este modo, independientemente de lo que pueda sucederle a un nodo o a un enlace, se garantiza la recepción del paquete siempre que exista al menos una ruta entre el origen y el destino.
- Dado que se prueban todos los caminos, al menos una copia del paquete a recibir en el destino habrá usado una ruta de menor número de saltos.
- Se visitan todos los nodos que están directa o indirectamente conectados al nodo origen.



(a) Primer salto



(b) Segundo salto



(c) Tercer salto

Figura 10.8. *Ejemplo de inundaciones (número de saltos = 3).*

Por la primera propiedad, la técnica de inundaciones es muy robusta y puede ser usada para enviar mensajes de alta prioridad. Una ejemplo de aplicación es una red militar que sufre daños importantes. Por la segunda propiedad, la técnica de inundaciones podría emplearse inicialmente para establecer la ruta para un circuito virtual. La tercera propiedad sugiere que la técnica de inundaciones puede resultar útil para la llevar a cabo la propagación de información importante para todos los nodos; ya se verá que se utiliza en algunos esquemas para la propagación de información de encaminamiento.

La principal desventaja de la técnica de inundaciones es la gran cantidad de tráfico que genera, directamente proporcional a la conectividad de la red.

Encaminamiento aleatorio

La técnica de encaminamiento aleatorio presenta, con menor tráfico, la sencillez y robustez de la técnica de inundaciones. En esta técnica, un nodo selecciona un único camino de salida para retransmitir un paquete entrante. El enlace de salida se elige de forma aleatoria, excluyendo el enlace por el que llegó el paquete. Si todos los enlaces son igualmente probables de ser elegidos, una implementación sencilla consistiría en seleccionarlos de forma alternada.

Una mejora a esta técnica consiste en asignar una probabilidad a cada uno de los enlaces de salida y llevar a cabo la selección de acuerdo con estas probabilidades. La probabilidad se puede basar en la razón de datos, en cuyo caso se tiene

$$P_i = \frac{R_i}{\sum_j R_j}$$

donde

P_i = probabilidad de seleccionar el enlace i
R_i = razón de datos o velocidad del enlace i

La suma se realiza para todos los enlaces de salida candidatos. Este esquema proporciona una distribución del tráfico adecuada. Obsérvese que las probabilidades podrían también estar basadas en costes de enlace fijos.

Como en el caso de la técnica de inundaciones, el encaminamiento aleatorio no necesita el uso de información sobre la red. Dado que la ruta se elige de forma aleatoria, ésta no corresponderá en general con la de mínimo coste ni con la de menor número de saltos. Por tanto, la red debe transportar un tráfico superior al óptimo, aunque inferior al de la técnica de inundaciones.

Encaminamiento adaptable

Prácticamente en todas las redes de conmutación de paquetes se utiliza algún tipo de técnica de encaminamiento adaptable; es decir, las decisiones de encaminamiento cambian en la medida que lo hacen las condiciones de la red. Las principales condiciones que influyen en las decisiones de encaminamiento son:

- **Fallos:** cuando un nodo o una línea principal fallan, no pueden volver a ser usados como parte de una ruta.
- **Congestión:** cuando una parte de la red sufre una congestión importante, es deseable encaminar a los paquetes de forma que se rodease la zona congestionada en lugar de realizar el encaminamiento a través de ella.

Para hacer posible el encaminamiento adaptable es necesario que los nodos intercambien información acerca del estado de la red. El uso de la técnica de encaminamiento adaptable presenta varias desventajas en comparación con el encaminamiento estático:

- La decisión de encaminamiento es más compleja, por lo que aumenta el coste de procesamiento en los nodos de la red.
- En la mayor parte de los casos, las estrategias adaptables dependen de la información de estado obtenida en una parte de la red pero utilizada en otra. Existe un compromiso entre la calidad de la información y la cantidad de datos suplementarios o redundancia utilizada. Cuanta más, y más frecuentemente, información se intercambia, mejores serán las decisiones de encaminamiento tomadas en cada nodo. Por otro lado, esta información constituye en sí misma tráfico adicional sobre la red, lo que supone cierta degradación de sus prestaciones.
- Una estrategia adaptable puede reaccionar demasiado rápidamente, provocando oscilaciones y causando congestión, o demasiado lentamente, en cuyo caso no es válida.

A pesar de estos peligros reales, las estrategias de encaminamiento adaptable son con mucho las más utilizadas por dos razones:

- El usuario de la red percibe que las prestaciones mejoran con el uso de estas técnicas.
- Como se discutirá en el Capítulo 12, una estrategia de encaminamiento adaptable puede resultar de ayuda en el control de la congestión: dado que este tipo de técnica tiende a compensar la carga, puede retrasar la aparición de situaciones graves de congestión.

Dependiendo de la validez del diseño y de la naturaleza del tráfico, estas ventajas se pueden constatar o no debido a la complejidad en lograr un funcionamiento correcto. Como demostración de este hecho, la mayor parte de las redes de conmutación de paquetes, tales como ARPANET y sus sucesoras, TYMNET, y las desarrolladas por IBM y DEC, han sufrido al menos una revisión en sus técnicas de encaminamiento.

Una clasificación adecuada de las estrategias de encaminamiento adaptable es la realizada de acuerdo con la fuente de la información: local, nodos adyacentes, todos los nodos. Un ejemplo de técnica adaptable basada sólo en información local es aquella en la que cada nodo encamina cada paquete recibido por la línea de salida cuya cola asociada sea menor, Q, lo que haría que se compense la carga entre las distintas líneas de salida. Sin embargo, puede que algunos enlaces de salida no lleven al destino adecuado, por lo que se podría mejorar la técnica, como en el caso del encaminamiento aleatorio, teniendo en consideración la dirección deseada. En este caso, cada enlace de salida tendría un peso B_i para cada destino i. Para cada paquete recibido con destino el nodo i, el nodo elegirá aquella línea que minimice $Q + B_i$, de manera que los paquetes se envían en la dirección correcta considerando los retardos provocados por el tráfico.

Como ejemplo, en la Figura 10.9 se muestra el estado del nodo 4 de la Figura 10.6 en un instante de tiempo dado. Este nodo tiene sendos enlaces a otros cuatro nodos. Al recibirse varios paquetes se produce un exceso, de forma que se crea una cola de paquetes para cada una de las líneas de salida. ¿Hacia qué línea se debería encaminar un paquete recibido desde el nodo 1 con destino al 6? De acuerdo con las longitudes de las colas y la tabla de pesos (B_6) para cada enlace de salida, el valor mínimo de $Q + B_6$ es 4, correspondiente al enlace hacia el nodo 3. Por tanto, el nodo 4 encaminará el paquete hacia dicho nodo.

Los esquemas adaptables basados sólo en información local son raramente utilizados dado que no explotan con facilidad la información disponible. Las estrategias basadas en el uso de la información procedente de los nodos adyacentes o de todos los nodos se utilizan más debido a la mejor información acerca de los retardos en los nodos de que se dispone en estos casos. Estas técnicas adaptables pueden ser distribuidas o centralizadas. En el primer caso, cada nodo intercambia información de retardo con otros nodos, de modo que cada nodo trata de estimar el retardo a través de la red a partir de la información recibida y aplica un algoritmo de encaminamiento de mínimo coste. En el caso de una técnica centralizada, cada nodo informa sobre su estado de retardo a un nodo central, quien diseña las rutas de acuerdo con esta información recibida y devuelve la información de encaminamiento a los nodos.

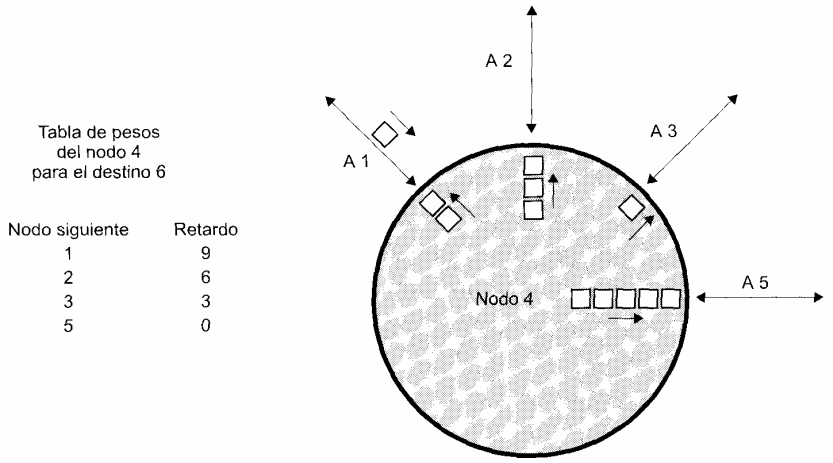


Figura 10.9. Ejemplo de encaminamiento adaptable aislado.

EJEMPLOS

En este apartado se estudiarán varios ejemplos de estrategias de encaminamiento. Todas ellas fueron desarrolladas para ARPANET, red de conmutación de paquetes predecesora de la actual Internet. Resulta instructivo examinar estas estrategias por varias razones. Primero porque estas y otras técnicas similares se usan también en otras redes de conmutación de paquetes, incluyendo las desarrolladas por DEC e IBM y otras de Internet. En segundo lugar hay que decir que los esquemas de encaminamiento basados en el trabajo de ARPANET se han usado también en la interconexión de redes en Internet y en redes privadas. Por último, porque el esquema de encaminamiento de ARPANET evolucionó de manera que aclara algunos de los aspectos clave en el diseño de los algoritmos de encaminamiento.

Primera generación

El algoritmo de encaminamiento original, diseñado en 1969, era un algoritmo adaptable distribuido que hacía uso de la estimación de los retardos como criterio de funcionamiento y de una versión del algoritmo de Bellman-Ford (Apéndice 10A). Para este algoritmo, cada nodo mantiene dos vectores:

$$D_i = \begin{bmatrix} d_{i1} \\ \vdots \\ d_{iN} \end{bmatrix} \qquad S_i = \begin{bmatrix} s_{i1} \\ \vdots \\ s_{iN} \end{bmatrix}$$

donde

D_i = vector de retardo para el nodo i

d_{ij} = estimación actual del retardo mínimo desde el nodo i al nodo j ($d_{ii} = 0$)

N = número de nodos en la red

S_i = vector del nodo sucesor para el nodo i

s_{ij} = nodo siguiente en la ruta actual de mínimo retardo de i a j

Periódicamente (cada 128 ms), cada nodo intercambia su vector de retardo con todos sus vecinos. A partir de los vectores de retardo recibidos, un nodo k actualiza sus dos vectores como sigue:

$$d_{kj} = \min_{i \in A} [d_{ij} + l_{ki}]$$

$s_{kj} = i$ siendo i el que minimiza la expresión anterior

donde

A = conjunto de nodos vecinos de k

l_{ki} = estimación actual del retardo desde el nodo k al nodo i

En la Figura 10.10 se muestra un ejemplo del algoritmo original de ARPANET usando la red de la Figura 10.11. Ésta es la misma red que la de la Figura 10.6 pero con diferentes costes asociados a los enlaces (y suponiendo el mismo coste en ambos sentidos del enlace). En la Figura 10.10a se muestra la tabla de encaminamiento del nodo 1 en un instante de tiempo que refleja los costes asociados a los enlaces de la Figura 10.11. Para cada destino se especifica un retardo y el nodo siguiente en la ruta que lo produce. En algún momento, los costes de los enlaces cambian a los valores indicados en la Figura 10.6. Supóngase que los vecinos del nodo 1 (nodos 2, 3 y 4) conocen el cambio antes que él. Cada uno de estos nodos actualizará su vector de retardo y enviará una copia a todos sus vecinos, incluyendo el nodo 1 (Figura 10.10b). El nodo 1 desecha su tabla de encaminamiento y construye una nueva basándose en los vectores de retardo recibidos y en la propia estimación que él hace del retardo para cada uno de los enlaces de salida a sus vecinos. El resultado obtenido se muestra en la Figura 10.10c.

Destino	Retardo	Nodo siguiente
1	0	—
2	2	2
3	5	3
4	1	4
5	6	3
6	8	3

D_1 S_1

(a) Tabla de encaminamiento del nodo 1 antes de actualizar

D_2	D_3	D_4
3	7	5
0	4	2
3	0	2
2	2	0
3	1	1
5	3	3

(b) Vectores de retardo enviados al nodo 1 por sus nodos vecinos

Destino	Retardo	Nodo siguiente
1	0	—
2	2	2
3	3	4
4	1	4
5	2	4
6	4	4

$l_{1,2} = 2$

$l_{1,3} = 5$

$l_{1,4} = 1$

(c) Tabla de encaminamiento del nodo 1 después de actualizar y costes de línea usados en el proceso

Figura 10.10. Algoritmo de encaminamiento original de ARPANET.

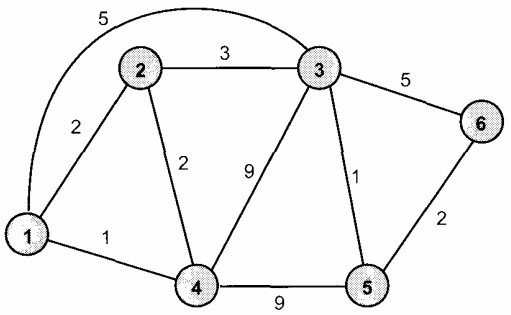


Figura 10.11. Red para el ejemplo de la Figura 10.10a.

El retardo de enlace estimado no es más que el tamaño o longitud de la cola para el enlace. Así, con la construcción de una nueva tabla de encaminamiento, el nodo tiende a favorecer aquellos enlaces con menores colas, lo que compensa la carga entre las distintas líneas de salida. Sin embargo, dado que el tamaño de las colas varía rápidamente a lo largo del tiempo, la percepción distribuida de la ruta más corta podría cambiar mientras un paquete se encuentra en tránsito. Esto podría provocar una situación en la que un paquete se encamina hacia un área de baja congestión en lugar de hacia el destino.

Segunda generación

Tras años de experiencia y algunas modificaciones sin importancia, el algoritmo de encaminamiento original se reemplazó en 1979 por otro bastante diferente [MCQU80]. Los principales inconvenientes del antiguo algoritmo eran los siguientes:

- No se consideraba la velocidad de las líneas sino sólo su tamaño de cola, por lo que a las líneas de alta capacidad no se les daba el tratamiento de favor que merecían.
- El tamaño de las colas es, en cualquier caso, una medida artificial del retardo ya que se consume un cierto tiempo de procesamiento desde que el nodo se recibe en un nodo hasta que es puesto en cola.
- El algoritmo no era demasiado seguro; de hecho, su respuesta era muy lenta ante aumentos en la congestión y en el retardo.

El nuevo algoritmo es también adaptable distribuido en el que se hace uso del retardo como criterio de funcionamiento, pero las diferencias son significativas. En lugar de usar la longitud de la cola como indicador del retardo, éste se mide directamente como sigue: a cada paquete recibido en un nodo se le coloca un sello de tiempo indicando el instante de tiempo en que llegó; se graba el instante en que se transmite; si se recibe una confirmación positiva, el retardo se calcula como el tiempo de salida menos el de llegada más el tiempo de transmisión y el de propagación. Para ello, el nodo debe conocer la velocidad del enlace y el tiempo de propagación. En cambio, si se recibe una confirmación negativa, se actualiza el tiempo de salida y el nodo vuelve a intentarlo hasta que se consigue con éxito una medida del retardo de transmisión.

El nodo calcula el retardo medio de cada enlace de salida cada 10 segundos. Si se producen cambios significativos en el valor del retardo, se envía la información a los demás nodos mediante el algoritmo de inundaciones. Cada nodo mantiene una estimación del retardo de cada enlace de la red, de modo que cuando recibe nueva información se actualiza la tabla de encaminamiento haciendo uso del algoritmo de Dijkstra (Apéndice 10A).

Tercera generación

La experiencia con esta nueva estrategia demostró que era más adecuada y estable que la anterior. El coste de la técnica de inundaciones era moderado, ya que cada nodo la llevaba a cabo cada 10 segundos; sin embargo, se observó un problema en el funcionamiento de esta nueva estrategia a medida que aumentaba el tráfico en la red, por lo que fue revisada en 1987 [KHAN89].

El problema de la segunda estrategia consistía en la suposición de que el retardo de paquetes estimado para un enlace es un buen indicador del retardo de enlace una vez que todos los nodos realizan el encaminamiento de su tráfico basándose en dicho retardo. Este mecanismo de encaminamiento resulta efectivo sólo si existe alguna correlación entre los valores estimados y los realmente experimentados una vez realizado el encaminamiento. Esta correlación tiende a ser mayor cuando el tráfico es moderado, pero cuando existe alta carga la correlación es pequeña. Por tanto, inmediatamente después de que todos los nodos hayan actualizado las tablas, éstas quedan obsoletas.

Como ejemplo considérese una red consistente en dos regiones con sólo dos enlaces, A y B, que las conectan (Figura 10.12). Cada ruta entre dos nodos situados en regiones diferentes debe atravesar uno

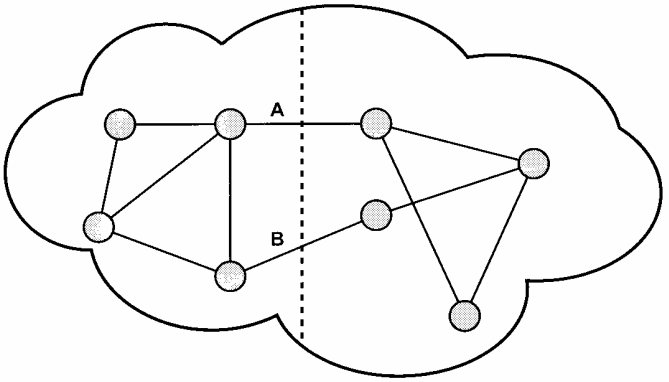


Figura 10.12. Red de conmutación de paquetes sujeta a oscilaciones.

de estos enlaces. Supóngase una situación tal que la mayor parte del tráfico lo soporta la línea A, lo que implicará que el retardo en dicha línea es importante. Enviada la información concerniente a este retardo al resto de los nodos en un instante de tiempo dado, todos ellos actualizarán inmediatamente sus tablas de encaminamiento. Es probable que este nuevo retardo para el enlace A sea lo suficientemente elevado para hacer que el enlace B sea ahora el elegido por la mayoría de las rutas, si no todas, entre ambas regiones. Dado que todos los nodos actualizan sus tablas al mismo tiempo, la mayor parte del tráfico entre las dos regiones se desplaza simultáneamente hacia la línea B. Esto provocará que sea ahora esta línea la que presente un retardo elevado, por lo que el tráfico se desplazará de nuevo hacia la línea A. Esta oscilación persistirá mientras lo haga el volumen de tráfico.

Existen varias razones por las que dicha oscilación resulta indeseable:

- Una parte importante de la capacidad disponible no se utiliza precisamente cuando se necesita: en condiciones de alta carga.
- La utilización excesiva de algunos enlaces puede provocar congestión en la red (esto se verá cuando se estudie la congestión en el Capítulo 12).
- Las oscilaciones en los valores de retardo obtenidos hacen necesaria una actualización más frecuente de las tablas de encaminamiento. Este hecho incrementa el tráfico de la red justo cuando ésta ya presenta alta cargada.

Los diseñadores de ARPANET concluyeron que la esencia del problema radicaba en el hecho de que todos los nodos estaban tratando de obtener la ruta óptima para todos los destinos, lo que provocaba conflictos. Se concluyó que, para alta carga, el objetivo del encaminamiento debería consistir en la obtención de una ruta promedio en lugar de intentar la determinación de todos los caminos mejores.

Los diseñadores decidieron que era innecesario cambiar todo el algoritmo, el cambio de la función que determinaba el coste de los enlaces bastaba para evitar las oscilaciones en el encaminamiento y reducir su coste. El cálculo comienza midiendo el retardo medio en los últimos 10 segundos. Este valor se transforma como se indica a continuación:

1. Haciendo uso de un sencillo modelo de colas con un único servidor, el retardo medido se transforma en una estimación de la utilización de la línea. Por teoría de colas, la utilización se puede expresar en función del retardo como sigue:

$$\rho = \frac{2(T_s - T)}{T_s - 2T}$$

donde

ρ = utilización del enlace
T = retardo medido
T_s = tiempo de servicio

El tiempo de servicio se hace igual al tamaño medio de los paquetes en la red (600 bits) dividido entre la velocidad de la línea.

2. El resultado se suaviza promediándolo con la utilización estimada previamente:

$$U(n + 1) = 0{,}5 \times \rho(n + 1) + 0{,}5 \times U(n)$$

donde

$U(n)$ = utilización media calculada en el instante de muestreo n
$\rho(n)$ = utilización del enlace en el instante de tiempo n

El valor promedio incrementa el periodo de las oscilaciones en el encaminamiento, lo que reduce el coste adicional de este último.

3. El coste del enlace se establece como una función de la utilización media, pensada para proporcionar una estimación razonable del coste sin provocar oscilación. En la Figura 10.13 se indica la forma de convertir la estimación de la utilización en un valor de coste, transformándose así el coste final en un valor de retardo.

En la Figura 10.13 mencionada se normaliza el retardo al valor alcanzado en una línea desocupada, que corresponde al tiempo de propagación más el tiempo de transmisión. Cada curva en la figura indica la forma en que el retardo real depende de la utilización; el incremento en el retardo se debe al retardo de cola en el nodo. Para el nuevo algoritmo, el valor del coste se mantiene al valor mínimo hasta que se alcanza un nivel de utilización dado, lo que tiene el efecto de reducir el coste del encaminamiento cuando el tráfico es pequeño. Por encima de un cierto nivel de utilización, se permite que el nivel de coste alcance un valor máximo igual a tres veces el valor mínimo. El efecto de este valor máximo es establecer que el tráfico no debe ser encaminado a través de una línea con alta carga más que en dos saltos adicionales.

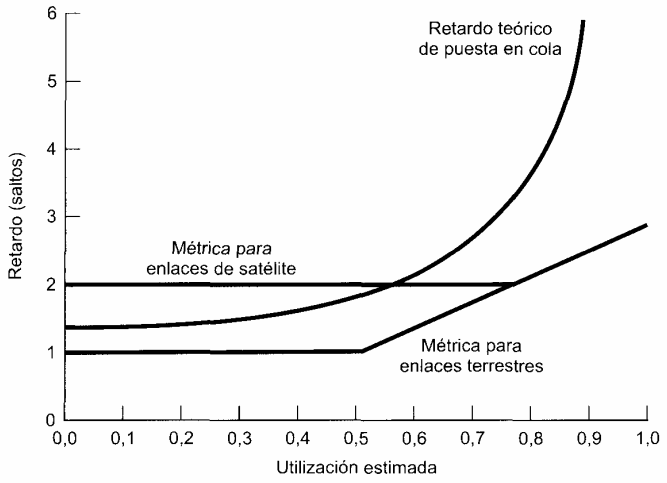


Figura 10.13. Métricas de retardo en ARPANET.

Obsérvese que el umbral mínimo es superior para enlaces satélite, lo que potencia el uso de los enlaces terrestres para condiciones de baja carga dado que éstos presentan un retardo de propagación inferior. Nótese también que la curva de retardo real es mucho más pronunciada que las curvas de transformación para altos niveles de utilización. Está pendiente en el coste del enlace provoca que el tráfico en un enlace se distribuya, lo que causa la aparición de oscilaciones en el encaminamiento.

En resumen, la función de coste estudiada está orientada más a la utilización que al retardo. La función actúa de forma similar a una métrica basada en retardo cuando la carga es baja, y a una métrica basada en la capacidad en condiciones de alta carga.

10.3. X.25

Uno de los protocolos estándares más ampliamente usado es X.25, aprobado originalmente en 1976 y sucesivamente modificado desde entonces. El estándar especifica una interfaz entre una estación y una red de conmutación de paquetes, siendo utilizado casi mundialmente para interaccionar con redes de este tipo así como en conmutación de paquetes en RDSI. El estándar especifica tres capas de protocolos:

- Capa física
- Capa de enlace
- Capa o nivel de paquete

Estas tres capas corresponden a las tres capas inferiores del modelo OSI (véase Figura 1.10). La capa física trata la interfaz física entre una estación (computador, terminal) y el enlace que la conecta con un nodo de conmutación de paquetes. En el estándar se hace referencia a la máquina de usuario como **equipo terminal de datos (DTE,** data terminal equipment), y al nodo de conmutación de paquetes al que está conectado el DTE como **equipo terminal del circuito de datos (DCE,** data circuit-terminating equipment). X.25 hace uso de la especificación de la capa física dada en el estándar conocido

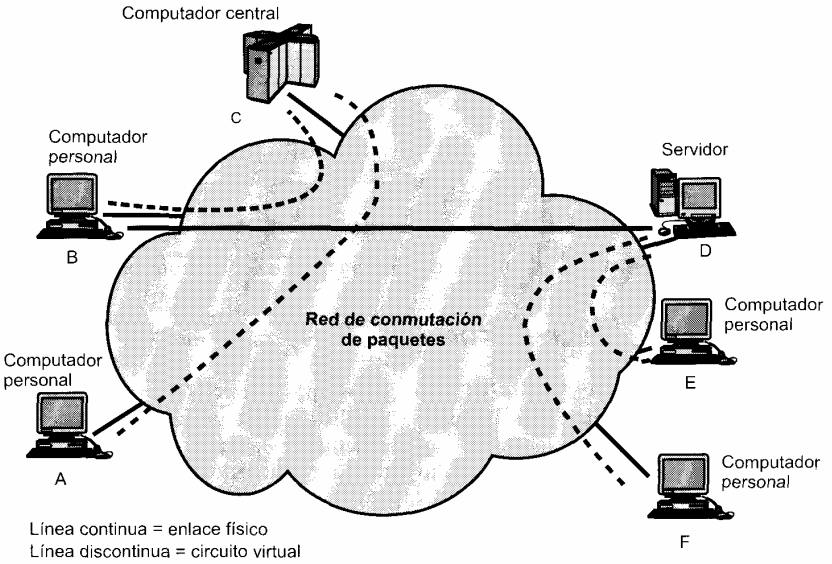


Figura 10.14. Ejemplo de utilización de circuitos virtuales.

como X.21, aunque en muchos casos se utilizan otros estándares tales como el EIA-232. La capa de enlace se encarga de la transferencia fiable de datos a través del enlace físico mediante la transmisión de los datos como una secuencia de tramas. La capa de enlace estándar es el LAPB (Protocolo Equilibrado de Acceso al Enlace, del inglés «Link Access Protocol Balanced»), el cual es un subproducto del protocolo HDLC descrito en el Capítulo 7.

El nivel de paquete proporciona un servicio de circuito virtual externo, lo que posibilita a un abonado de la red establecer conexiones lógicas, llamadas circuitos virtuales, con otros abonados. Un ejemplo de esto se muestra en la Figura 10.14 (compárese con la Figura 9.1). En este ejemplo, la estación A tiene una conexión de tipo circuito virtual con C; la estación B tiene establecidos dos circuitos virtuales, uno con C y otro con D; y cada una de las estaciones E y F mantiene un circuito virtual con D.

En la Figura 10.15 se ilustra la relación entre las capas de X.25. Los datos de usuario se pasan hacia abajo al nivel 3 de X.25, que les añade una cabecera consistente en información de control dando lugar a un **paquete.** Alternativamente, los datos de usuario se pueden segmentar en varios paquetes. La información de control incluida en el paquete tiene varios objetivos, entre los que se encuentran los siguientes:

1. Identificación de un circuito virtual dado mediante un número al que se asociarán los datos.
2. Definición de números de secuencia para su uso en el control de flujo y de errores sobre los circuitos virtuales.

El paquete X.25 completo se pasa después a la entidad LAPB, que añade información de control al principio y al final del paquete, dando lugar a una **trama** LAPB. De nuevo, esta información de control en la trama es necesaria para el funcionamiento del protocolo LAPB.

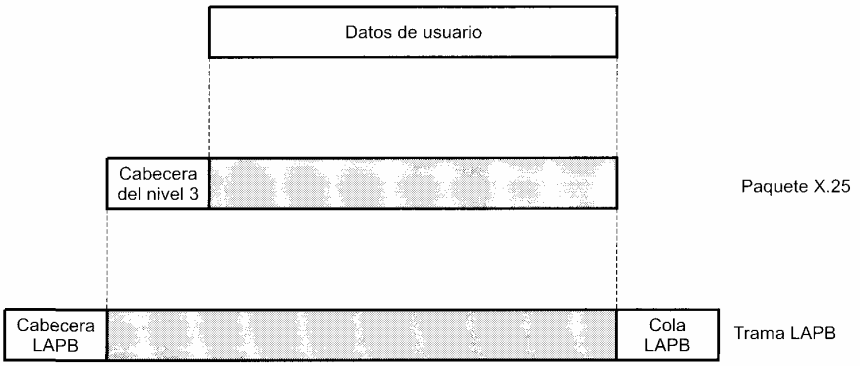


Figura 10.15. Datos de usuario e información de control del protocolo X.25.

SERVICIO DE CIRCUITO VIRTUAL

El servicio de circuito virtual de X.25 ofrece dos tipos de circuitos virtuales: llamadas virtuales y circuitos virtuales permanentes. Una **llamada virtual** es un circuito virtual que se establece dinámicamente mediante una petición de llamada y una liberación de llamada como se describe más adelante. Un **circuito virtual permanente** es un circuito virtual fijo asignado en la red. La transferencia de los datos se produce como con las llamadas virtuales, pero en este caso no se necesita realizar ni el establecimiento ni el cierre de la llamada.

En la Figura 10.16 se muestra una secuencia de eventos típica en una llamada virtual. En la parte izquierda de la figura se indican los paquetes intercambiados entre la máquina de usuario A y el nodo de

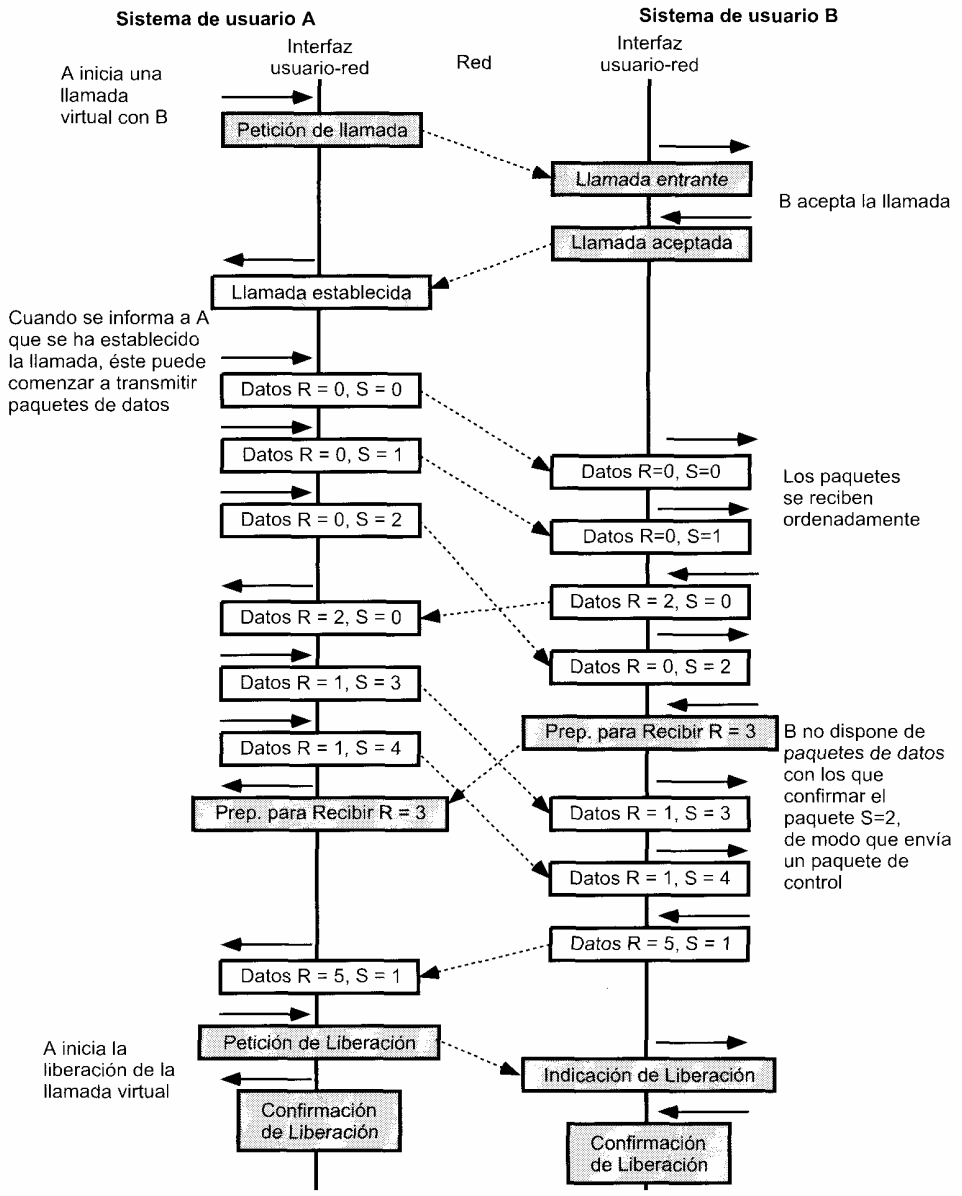


Figura 10.16. Secuencia de eventos: protocolo X.25.

conmutación de paquetes al que está conectada, mientras que la parte derecha muestra los paquetes intercambiados entre la máquina de usuario B y su nodo. El encaminamiento de los paquetes dentro de la red no es visible al usuario.

La secuencia de eventos es la que sigue:

1. A solicita un circuito virtual a B mediante el envío de un paquete Petición de Llamada («Call Request») al DCE de A. El paquete incluye las direcciones de origen y de destino así como el

número a usar para este nuevo circuito virtual. Las futuras transmisiones de entrada y salida se identificarán mediante este número de circuito virtual.

2. La red encamina esta petición de llamada al DCE de B.
3. El DCE de B recibe el paquete Petición de Llamada y envía un paquete Llamada Entrante («Incoming Call») a B. Este paquete tiene el mismo formato que el de Petición de Llamada, pero con un número de circuito virtual diferente. Este número lo elige el DCE de B de entre el conjunto de número locales libres.
4. B indica la aceptación de la llamada mediante el envío de un paquete Llamada Aceptada («Call Accepted»), que especifica el mismo número de circuito virtual que el del paquete Llamada Entrante.
5. El DCE de A recibe el paquete Llamada Aceptada y envía a A un paquete Llamada Establecida («Call Connected»). Este paquete tiene el mismo formato que el de Llamada Aceptada, pero el número de circuito virtual es el mismo que el del paquete Petición de Llamada original.
6. A y B se intercambian paquetes de datos y de control haciendo uso de sus respectivos números de circuito virtual.
7. A (o B) envía un paquete Petición de Liberación («Clear Request») para liberar el circuito virtual y recibe un paquete Confirmación de Liberación («Clear Confirmation»).
8. B (o A) recibe un paquete Indicación de Liberación («Clear Indication») y transmite uno de Confirmación de Liberación («Clear Confirmation»).

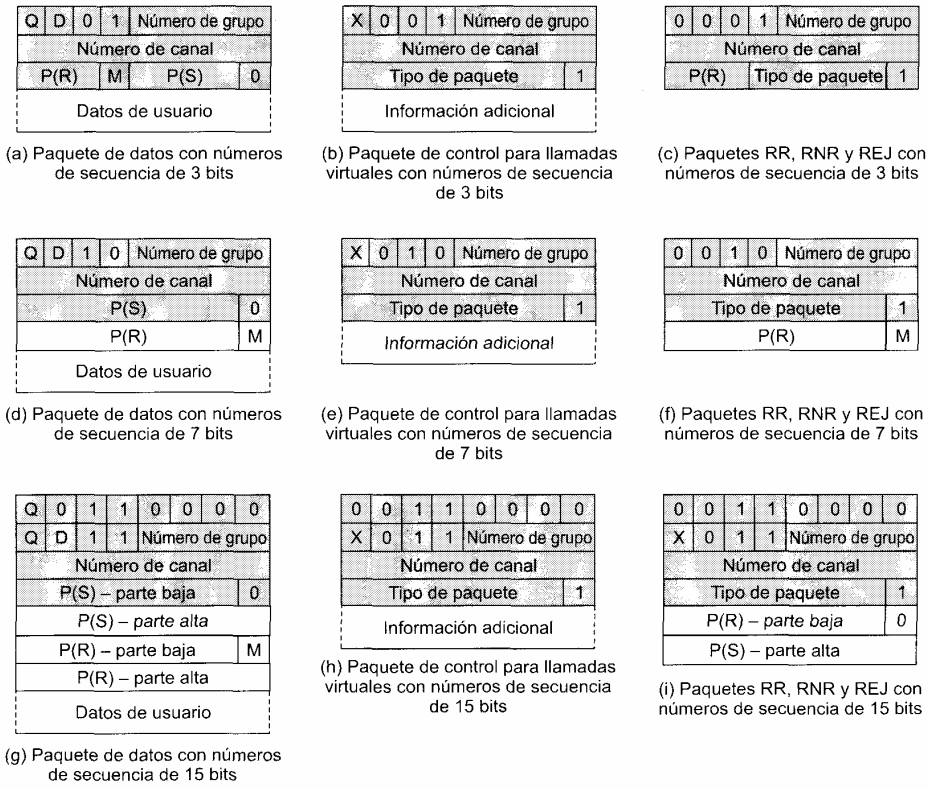
Veamos a continuación algunos detalles del estándar.

FORMATO DE PAQUETE

En la Figura 10.17 se muestran los formatos básicos de paquete en X.25. Los datos de usuario se segmentan en bloques con un cierto tamaño máximo, añadiéndosele a cada segmento una cabecera de 24, 32 o 56 bits para formar un paquete de datos. En el caso de que se utilice un número de secuencia de 15 bits para indicar el circuito virtual, la cabecera comienza con un octeto identificador de protocolo de valor 00110000. La cabecera incluye 12 bits para especificar un número de circuito virtual (4 bits para el número de grupo y 8 bits para el número de canal). Los campos P(S) y P(R) se usan para el control de flujo y de errores a través del circuito virtual tal como se explica más adelante. El bit Q no se encuentra definido en el estándar y lo utiliza el usuario para distinguir entre dos tipos de datos.

Además de la transmisión de datos de usuario, X.25 debe transmitir información de control relativa al establecimiento, mantenimiento y liberación de circuitos virtuales. Esta información se transmite en **paquetes de control,** cada uno de los cuales incluye el número de circuito virtual, el tipo de paquete, que identifica la función de control específica, e información de control adicional relacionada con esta función. Por ejemplo, un paquete Petición de Llamada incluye los siguientes campos adicionales:

- **Longitud de la dirección del DTE llamante (4 bits):** es la longitud del campo de dirección correspondiente, en unidades de 4 bits.
- **Longitud de la dirección del DTE llamado (4 bits):** es la longitud del campo de dirección correspondiente, en unidades de 4 bits.
- **Direcciones DTE (variable):** direcciones de los DTE llamante y llamado.
- **Campo de facilidades:** es una secuencia de facilidades. Cada facilidad especificada consta de un código de 8 bits y ninguno o varios códigos de parámetros. Un ejemplo de facilidad es la carga en sentido contrario.



(a) Paquete de datos con números de secuencia de 3 bits

(b) Paquete de control para llamadas virtuales con números de secuencia de 3 bits

(c) Paquetes RR, RNR y REJ con números de secuencia de 3 bits

(d) Paquete de datos con números de secuencia de 7 bits

(e) Paquete de control para llamadas virtuales con números de secuencia de 7 bits

(f) Paquetes RR, RNR y REJ con números de secuencia de 7 bits

(g) Paquete de datos con números de secuencia de 15 bits

(h) Paquete de control para llamadas virtuales con números de secuencia de 15 bits

(i) Paquetes RR, RNR y REJ con números de secuencia de 15 bits

Figura 10.17. Formatos de paquete en X.25.

En la Tabla 10.3 se listan los paquetes X.25, la mayor parte de los cuales ha sido ya presentada. Pasamos a describir brevemente el resto.

Tabla 10.3. Tipos de paquetes y parámetros.

Tipo de paquete		Servicio		Parámetros
Del DTE al DCE	**Del DCE al DTE**	**VC**	**PVC**	
Establecimiento y liberación de llamada				
Petición de llamada	Llamada entrante	X		Dirección del DTE llamante, dirección del DTE llamado, facilidades, datos de usuario de llamada
Llamada aceptada	Llamada establecida	X		Dirección del DTE llamante, dirección del DTE llamado, facilidades, datos de usuario de llamada
Petición de liberación	Indicación de liberación	X		Causa de la liberación, código de diagnóstico, dirección del DTE llamante, dirección del DTE llamado, *facilidades, datos de usuario de liberación*
Confirmación de liberación	Confirmación de liberación	X		Dirección del DTE llamante, dirección del DTE llamado, facilidades

Tabla 10.3. *(Continuación).*

Tipo de paquete		Servicio		Parámetros
Del DTE al DCE	**Del DCE al DTE**	**VC**	**PVC**	
Datos e interrupciones				
Datos	Datos	X	X	—
Interrupción	Interrupción	X	X	Datos de usuario de interrupción
Confirmación de interrupción	Confirmación de interrupción	X	X	—
Control de flujo y reinicio				
RR	RR	X	X	P(R)
RNR	RNR	X	X	P(R)
REJ		X	X	P(R)
Petición de reinicio	Indicación de reinicio	X	X	Causa del reinicio, código de diagnóstico
Confirmación de reinicio	Confirmación de reinicio	X	X	—
Rearranque				
Petición de rearranque	Indicación de rearranque	X	X	Causa del rearranque, código de diagnóstico
Confirmación de rearranque	Confirmación de rearranque	X	X	—
Diagnóstico				
	Diagnóstico	X	X	Código de diagnóstico, explicación del diagnóstico

Un DTE puede enviar un paquete Interrupción («Interrupt») que obvia el control de flujo de los paquetes de datos. Este tipo de paquete se envía a través de la red hacia el DTE destino con una prioridad superior que los paquetes de datos en tránsito. Un ejemplo del uso de esta facultad es la transmisión de carácter terminal de ruptura («break»).

Los paquetes Diagnóstico («Diagnostic») permiten indicar ciertas condiciones de error que no garantizan el reinicio. Los paquetes Registro («Registration») se utilizan para solicitar y confirmar facilidades X.25.

MULTIPLEXACIÓN

Quizás el servicio más importante ofrecido por X.25 sea la multiplexación. Un DTE puede establecer hasta 4.095 circuitos virtuales simultáneamente con otros DTE sobre el mismo enlace físico DTE-DCE. El DTE puede asignar internamente estos circuitos como le plazca. Cada uno de los circuitos virtuales corresponde, por ejemplo, a una aplicación, a un proceso o a un terminal. La línea DTE-DCE permite multiplexación *full-duplex*; es decir, un paquete asociado a un circuito virtual dado se puede transmitir en ambos sentidos en cualquier instante de tiempo.

Para saber qué paquetes pertenecen a cada circuito virtual, cada paquete contiene un número de circuito virtual de 12 bits. La asignación de números de circuito virtual sigue la convención que se muestra en la Figura 10.18. El número cero se reserva siempre para paquetes de diagnóstico comunes a todos los circuitos virtuales. Se usan rangos contiguos de números para cuatro categorías de circuitos virtuales. A los circuitos virtuales permanentes se les asigna números que comienzan por 1. La siguiente categoría la constituyen las llamadas virtuales entrantes, lo que significa que sólo a las llamadas procedentes de la red se les puede asignar estos números; el circuito virtual, en cambio, es en los dos sentidos (*full-duplex*). Cuando se recibe una solicitud de llamada, el DCE selecciona un número libre de esta categoría.

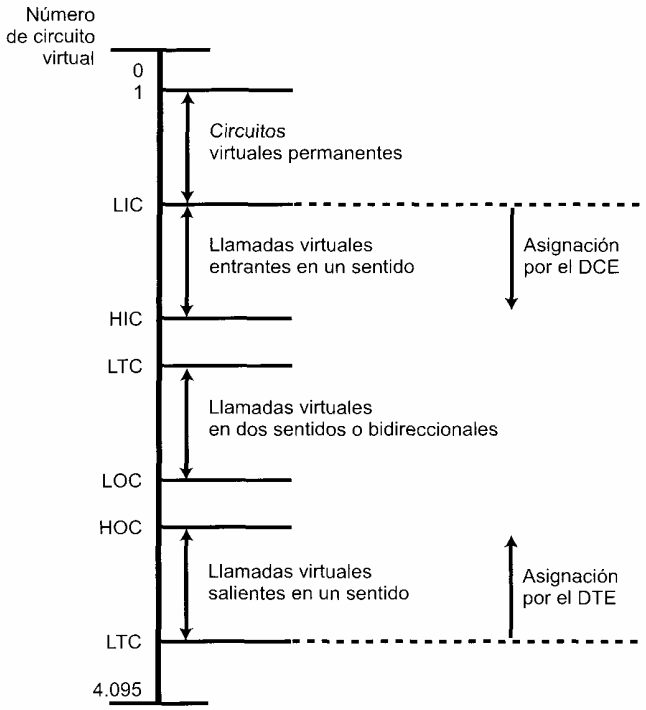


Figura 10.18. Asignación de números de circuito virtual.

Las llamadas salientes en un solo sentido (unidireccionales) se inician por parte del DTE, de modo que es él quien elige en este caso uno de los números libres reservados para estas llamadas. Esta separación de categorías está pensada para evitar la selección simultánea por parte del DTE y del DCE del mismo número para dos circuitos virtuales diferentes.

La categoría de llamadas virtuales en ambos sentidos o bidireccionales prevé un desbordamiento para la reserva compartida por el DTE y el DCE, lo que permite diferencias en los picos del flujo de tráfico.

CONTROL DE FLUJO Y DE ERRORES

El control de flujo y de errores en el nivel de paquete de X.25 es básicamente idéntico en formato y funcionamiento al control de flujo realizado por el protocolo HDLC descrito en el Capítulo 7. Se hace uso de un protocolo de ventana deslizante en el que cada paquete incluye un número de secuencia correspondiente al paquete enviado, P(S), y un número de secuencia relativo al paquete recibido, P(R). Aunque por defecto se utilizan números de secuencia de 3 bits, un DTE puede solicitar, de forma opcional a través del mecanismo de facilidades de usuario, el empleo de números de secuencia de 7 o de 15 bits.

El campo P(S) se asigna por parte del DTE a los paquetes salientes de acuerdo con el circuito virtual al que se asocian; es decir, el campo P(S) de cada nuevo paquete de salida sobre un circuito virtual es uno más que el del anterior paquete de ese circuito, módulo 8 (o módulo 128 o módulo 32.768). El campo P(R) contiene el número del siguiente paquete esperado por el otro extremo de un circuito virtual

dado, siendo usado para la confirmación en la técnica de incorporación de confirmaciones («piggybacking»). Si uno de los extremos no dispone de datos que enviar, puede llevar a cabo la confirmación de los paquetes recibidos mediante los paquetes de control Preparado para Recibir (RR, Receive Ready) y No Preparado para Recibir (RNR, Receive Not Ready), cuyo significado es el mismo que en el protocolo HDLC. El tamaño implícito de ventana es 2, pudiendo llegar a ser igual a 7 o a 32.767 para números de secuencia de 7 bits y de 15 bits, respectivamente.

El mecanismo de confirmación (en forma del campo P(R) en los datos o a través de los paquetes RR y RNR), y en consecuencia el control de flujo, puede tener significado local o extremo a extremo de acuerdo con el valor del bit D. Si D = 0 (situación usual), la confirmación tiene lugar entre el DTE y la red, lo cual se usa por el DCE local y/o la red para confirmar la recepción de paquetes y realizar el control de flujo desde el DTE hacia la red. Si D = 1, las confirmaciones proceden del DTE remoto.

El esquema de control de errores consiste en la técnica ARQ adelante-atrás-N («go-back-N»). Las confirmaciones negativas se llevan a cabo en forma de paquetes de control Rechazo (REJ, Reject), de modo que si un nodo recibe un paquete de este tipo retransmitirá el paquete especificado y todos los siguientes.

SECUENCIAS DE PAQUETES

X.25 posibilita la identificación de secuencias contiguas de paquetes de datos, lo que se conoce como **secuencia completa de paquetes.** Esta característica presenta varios usos. Uno importante es su empleo en la interconexión de redes (descrita en la Parte V del libro) para permitir el envío de bloques de datos de tamaño mayor al permitido por la red sin que pierdan su integridad.

Para especificar este mecanismo, X.25 define dos tipos de paquete: paquetes A y paquetes B. Un **paquete de tipo A** es aquel en el que el bit M toma el valor 1, el bit D el valor 0 y el paquete está completo (su longitud es la máxima permitida). Un **paquete de tipo B** es cualquier paquete que no sea de tipo A. Así, una secuencia completa de paquetes consiste en cero o más paquetes A seguidos de un paquete de tipo B. La red puede combinar esta secuencia para construir paquetes más grandes; asimismo, la red puede dividir un paquete de tipo B en paquetes de menor tamaño para producir una secuencia completa de paquetes.

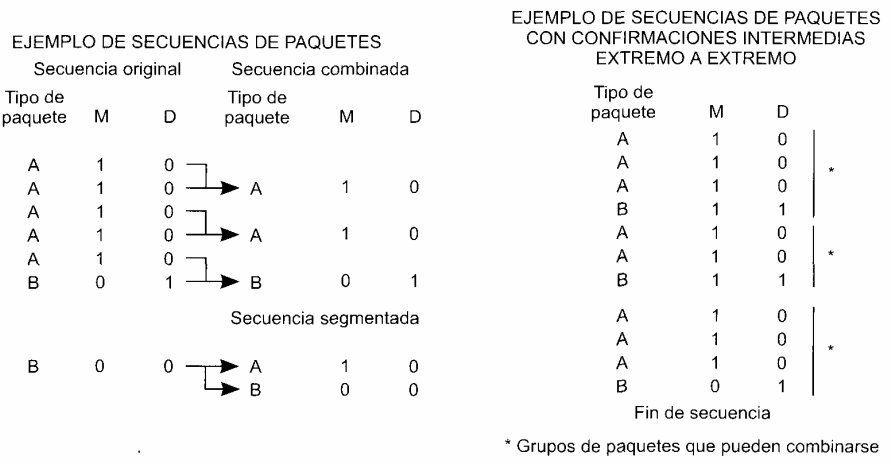


Figura 10.19. Secuencias de paquetes X.25.

La forma en que se gestiona el paquete B depende del valor de los bits M y D. Si D = 1, el DTE receptor envía una confirmación extremo a extremo hacia el DTE emisor, lo que indicaría una confirmación de la secuencia completa de paquetes. Si M = 1, existen secuencias de paquetes completas adicionales. Esto posibilita la creación de subsecuencias como parte de una secuencia más larga, de modo que se puede producir la confirmación extremo a extremo antes de que finalice la secuencia más larga.

En la Figura 10.19 se muestran algunos ejemplos acerca de estos conceptos. Es responsabilidad de los DCE reorganizar los cambios en la numeración de la secuencia causados por la segmentación y llevar a cabo la agrupación o ensamblado.

REINICIO Y REARRANQUE

X.25 proporciona dos facilidades para la recuperación de errores. La facilidad de reinicio se usa para reiniciar un circuito virtual, lo que significa que los números de secuencia se hagan igual a cero en ambos extremos y que se pierdan los paquetes de datos o de interrupción en tránsito. Es función de un protocolo de nivel superior la recuperación de los paquetes perdidos. Un reinicio puede estar provocado por diversas condiciones de error tales como la pérdida de paquetes, errores en el número de secuencia, congestión o pérdida de un circuito virtual interno a la red. En este último caso, ambos DCE deben restablecer el circuito virtual interno para atender al circuito virtual externo aún existente entre los dos DTE. Tanto un DTE como un DCE pueden originar un reinicio a través del uso de un paquete Petición de Reinicio («Reset Request») o uno Indicación de Reinicio («Reset Indication»), a los cuales responderá el receptor con un paquete Confirmación de Reinicio («Reset Confirmation»). Independientemente de quien origine el reinicio, es responsabilidad del DCE involucrado informar al otro extremo.

Una situación de error más seria requiere un rearranque. El envío de un paquete Petición de Rearranque («Restart Request») es equivalente a la emisión de un paquete Petición de Liberación sobre todas las llamadas virtuales y uno de Petición de Reinicio sobre todos los circuitos virtuales. Como antes, tanto el DCE como el DTE pueden iniciar la acción. Un ejemplo de una condición de rearranque consiste en la pérdida temporal del acceso a la red.

10.4. LECTURAS RECOMENDADAS

La bibliografía en torno a la conmutación de paquetes es muy extensa. Entre los libros que tratan adecuadamente este tema se encuentran [SPOH97], [BERT92] y [SPRA91]. También existe una gran cantidad de trabajos en torno al estudio de las prestaciones, pudiéndose encontrar buenas descripciones de ello en [STUC85], [SCHW77] y [KLEI76].

BERT92 Bertsekas, D., y Gallager, R. *Data Networks*. Englewood Cliffs, NJ: Prentice Hall, 1992.

KLEI76 Kleinrock, L. *Queuing Systems, Volume II: Computer Applications*. New York: Wiley, 1976.

SCHW77 Schwartz, M. *Computer-Communication Network Design and Analysis*. Englewood Cliffs, NJ: Prentice Hall, 1977.

SPOH97 Spohn, D. *Data Network Design*. New York: McGraw-Hill, 1994.

SPRA91 Spragins, J., Hammond, J., y Pawlikowski, K. *Telecommunications Protocols and Design*. Reading, MA: Addison-Wesley, 1991.

STUC85 Stuck, B., y Arthurs, E. *A. Computer Communications Network Performance Analysis Primer*. Englewood Cliffs, NJ: Prentice Hall, 1985.

10.5. PROBLEMAS

10.1. Explique el punto débil del siguiente razonamiento: la conmutación de paquetes requiere que a cada paquete se le añadan bits de control y de dirección, lo que provoca un coste adicional en

esta técnica. En conmutación de circuitos se establece un circuito transparente, no siendo necesario el uso de bits suplementarios.

a) No existe por tanto coste adicional en la técnica de conmutación de circuitos, por lo que

b) la utilización de la línea es más eficiente que en conmutación de paquetes.

10.2. Se definen los siguientes parámetros para una red de conmutación:

N = número de saltos entre dos sistemas finales dados.
L = longitud del mensaje en bits.
B = velocidad de transmisión (en bps) de todos los enlaces.
P = tamaño fijo del paquete, en bits.
H = bits de redundancia o suplementarios (cabecera) por paquete.
S = tiempo de establecimiento de llamada (conmutación de circuitos o circuitos virtuales) en segundos.
D = retardo de propagación por salto, en segundos.

a) Calcule el retardo extremo a extremo en conmutación de circuitos y en conmutación de paquetes mediante circuitos virtuales y mediante datagramas para $N = 4$, $L = 3.200$, $B = 9.600$, $P = 1.024$, $H = 16$, $S = 0{,}2$ y $D = 0{,}001$. Suponga que no se hace uso de confirmaciones e ignore el retardo de procesamiento en los nodos.

b) Obtenga las expresiones generales para las tres técnicas del apartado anterior, tomadas de dos en dos (tres expresiones en total), indicando las condiciones bajo las que el retardo es igual para todas ellas.

10.3. ¿Qué valor de P, como función de N, L y H, proporciona un retardo extremo a extremo mínimo en una red datagrama? Suponga que L es mucho mayor que P y $D = 0$.

10.4. Considere una red de conmutación de paquetes con N nodos conectados formando las siguientes topologías:

a) Estrella: un nodo central sin ninguna estación conectada y con todos los otros nodos conectados a él.

b) Bucle: cada nodo está conectado a otros dos nodos formando un bucle cerrado.

c) Conexión completa: cada nodo está directamente conectado a todos los otros nodos.

Determine en cada caso el número medio de saltos entre estaciones.

10.5. Considere una red de conmutación de paquetes con topología en árbol binario. El nodo raíz se conecta a otros dos nodos y todos los nodos intermedios se encuentran conectados con un nodo en la dirección hacia el nodo raíz y con dos en la dirección contraria. En la parte inferior existen nodos con un solo enlace hacia el nodo raíz. Si hay $2^N - 1$ nodos, obtenga una expresión para el número medio de saltos por paquete para un valor de N elevado suponiendo que los trayectos entre todos los pares de nodos son aproximadamente iguales. *Sugerencia*: las siguientes igualdades le serán de utilidad:

$$\sum_{i=1}^{\infty} x^i = \frac{x}{1-x}$$

$$\sum_{i=1}^{\infty} ix^i = \frac{x}{(1-x)^2}$$

10.6. Para determinar la ruta de mínimo coste desde un nodo s a un nodo t, el algoritmo de Dijkstra se puede expresar mediante el siguiente programa:

```
for n := 1 to N do
    begin
       L[n] := ∞; final[n] := false;
                        {todos los nodos se etiquetan temporalmente con ∞}

       pred[n] := 1
    end;
L[s]:= 0; final[s] := true;
                        {el nodo s se etiqueta permanentemente con 0}
recent := s;            {el nodo más reciente para etiquetarse
                        permanentemente es s}
path := true;           {inicio}
while final[t] = false do
begin
    for n := 1 to N do    {encontrar nueva etiqueta}
       if (w[recent, n] < ∞) AND (NOT final[n]) then
                        {para cada sucesor inmediato de recent que no se
                        encuentra permanentemente etiquetado, hacer}
      begin {actualizar las etiquetas temporales}
         newlabel := L[recent] + w[recent,n];
         if newlabel<L[n] then
               begin L[n] := newlabel; pred[n] := recent end
                  {se etiqueta de nuevo n si existe un camino más
                  corto a través del nodo recent y se hace recent el
                  predecesor de n en el camino más corto desde s}
      end;
    temp := ∞;
     for x := 1 to N do {encontrar el nodo con la etiqueta temporal menor}
         if (NOT final[x]) AND (L[x] <temp) then
      begin y := x; temp := L[x] end;
     if temp < ∞ then {existe una ruta}
          begin final[y] := true; recent := y end
                          {y, el siguiente nodo más cercano a s, se
                          etiqueta permanentemente}
        else begin path := false; final[t] := true end
end
```

En este programa se le asigna temporalmente una etiqueta inicial a cada nodo. Cuando se obtiene una ruta final a un nodo, se le asigna una etiqueta permanente igual al coste del camino desde *s*. Escriba un programa similar para el algoritmo de Bellman-Ford. *Sugerencia*: el algoritmo de Bellman-Ford se conoce a veces como método de corrección de etiquetas, frente al método de fijado de etiquetas seguido en el algoritmo de Dijkstra.

10.7. En la descripción del algoritmo de Dijkstra dada en el Apéndice 10A se dice que en cada iteración se añade un nuevo nodo a T y que la ruta de mínimo coste para ese nuevo nodo sólo atraviesa nodos ya incluidos en T. Demuestre que esto es cierto. *Sugerencia*: comience por el principio. Muestre que el primer nodo añadido a T debe tener un enlace directo al nodo origen, el segundo nodo en T debe tener un enlace directo con el nodo origen o con el primer nodo incluido en T, y así sucesivamente. Recuerde que los costes de todas las líneas se suponen no negativos.

10.8. En la descripción del algoritmo de Bellman-Ford se dice que en la iteración para la que $h = K$, si hay alguna ruta definida de longitud $K + 1$, los primeros K saltos de este camino forman una ruta definida en la iteración anterior. Demuestre que es cierto.

10.9. Los valores del camino de mínimo coste en el paso 3 del algoritmo de Dijkstra sólo se actualizan para nodos no incluidos aún en T. ¿No es posible encontrar una ruta de mínimo coste para un nodo en T? Si es así, demuéstrelo con un ejemplo. En caso contrario justifique razonadamente el motivo.

10.10. Haciendo uso del algoritmo de Dijkstra, genere un camino de mínimo coste para los nodos del 2 al 6 con el resto de nodos de la Figura 10.6. Muestre los resultados como en la Tabla 10.4a.

10.11. Repita el Problema 10.10 haciendo uso del algoritmo de Bellman-Ford.

10.12. Aplique el algoritmo de encaminamiento de Dijkstra para las redes de la Figura 10.20. Obtenga una tabla similar a la Tabla 10.4a y una figura análoga a la Figura 10.21.

10.13. Repita el Problema 10.12 haciendo uso del algoritmo de Bellman-Ford.

10.14. ¿Obtienen los algoritmos de Dijkstra y Bellman-Ford los mismos resultados siempre? ¿Por qué sí o por qué no?

10.15. Tanto el algoritmo de Dijkstra como el de Bellman-Ford obtienen las rutas de mínimo coste desde un nodo al resto. Por su parte, el algoritmo de Floyd-Warshall obtiene los caminos de mínimo coste entre todos las pares de nodos posibles. Se define:

N = conjunto de nodos en la red
$w(i, j)$ = coste del enlace del nodo i al nodo j; $w(i, i) = 0$ y $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados
$L_n(i, j)$ = coste del camino de mínimo coste desde el nodo i al nodo j con la condición de que sólo los nodos 1, 2, ... n se pueden usar como nodos intermedios en las rutas

El algoritmo sigue los siguientes pasos:

1. Inicio:

$$L_0(i, j) = w(i, j), \qquad \forall i, j, i \neq j$$

2. Para $n = 0, 1, \ldots N - 1$,

$$L_{n+1}(i, j) = \min [L_n(i, j), L_n(i, n + 1) + L_n(n + 1, j)], \qquad \forall i \neq j$$

Explique el algoritmo con palabras. Demuestre por inducción que éste funciona correctamente.

10.16. El nodo 1 de la Figura 10.8 envía un paquete al nodo 6 usando inundaciones. Contabilizando la transmisión de un paquete sobre una línea como una carga de uno, indique cuál será el tráfico total generado si:

a) Cada nodo descarta los paquetes entrantes duplicados.

b) Se usa un campo de cuenta de saltos con un valor inicial igual a 5.

10.17. Ya se vio que el algoritmo de inundaciones se puede utilizar para determinar la ruta con menor número de saltos. ¿Se puede usar también para la obtención del camino con menor retardo?

10.18. El algoritmo de encaminamiento aleatorio sólo permite la existencia de una copia de un paquete en un instante de tiempo dado. A pesar de ello, resulta deseable la utilización de un campo de cuenta de saltos. ¿Por qué?

10.19. Otro esquema de encaminamiento adaptable es el conocido como aprendizaje hacia atrás («backward learning»). Todo paquete encaminado a través de la red contiene no sólo la dirección de destino, sino también la dirección de origen más un contador de saltos que se incrementa en cada salto. Cada nodo construye una tabla de encaminamiento que especifica el nodo siguiente y el número de saltos para cada destino. ¿Cómo se usa la información contenida en el paquete para construir la tabla? ¿Cuáles son las ventajas y desventajas de esta técnica?

10.20. Construya una tabla de encaminamiento centralizado para las redes de la Figura 10.20.

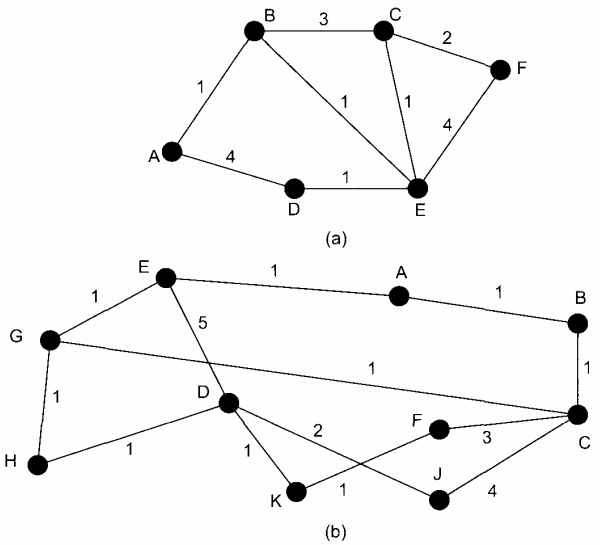


Figura 10.20. Redes de conmutación de paquetes con costes asociados.

10.21. Considérese un sistema que emplea la técnica de inundaciones con un contador de saltos que se supone inicialmente igual al «diámetro» de la red. Cuando el contador alcanza el valor cero el paquete se descarta excepto en el destino. ¿Se asegura siempre así que el paquete alcanzará el destino si existe al menos un camino operativo? Justifique la respuesta.

10.22. Suponiendo que no se producen fallos en el funcionamiento de las estaciones ni de los nodos de una red, ¿es posible que un paquete se reciba en un destino incorrecto?

10.23. En las capas 2 y 3 de X.25 se usan procedimientos de control de flujo. ¿Son necesarios ambos o, por el contrario, son redundantes? Explíquelo.

10.24. En X.25 no existe mecanismo alguno de corrección de errores (secuencia de comprobación de trama). ¿No es éste necesario para asegurar que todos los paquetes se reciben adecuadamente?

10.25. Cuando un DTE en X.25 y el DCE al que está conectado deciden establecer una llamada al mismo tiempo, se produce una colisión y se descarta la llamada entrante. Cuando ambos equipos tratan de liberar el mismo circuito virtual simultáneamente, la colisión en la liberación se resuelve sin rechazar ninguna de las solicitudes, siendo liberado el circuito virtual en cuestión. ¿Cómo cree que se resuelve la colisión de dos peticiones de reinicio, como la colisión de dos peticiones de establecimiento de llamada o como la de dos peticiones de liberación? ¿Por qué?

10.26. Dadas dos estaciones conectadas haciendo uso de X.25, ¿por qué es diferente el número de circuito virtual usado por cada una de ellas? Después de todo es el mismo circuito virtual *full-duplex*.

APÉNDICE 10A. ALGORITMOS DE MÍNIMO COSTE

Prácticamente todas las redes de conmutación de circuitos y todas las redes internet basan su decisión de encaminamiento en algún criterio de mínimo coste. Si el criterio consiste en minimizar el número de saltos, cada enlace tendrá asociado un valor igual a 1. Usualmente, el valor asociado al enlace es inver-

samente proporcional a su capacidad, proporcional a su carga actual o alguna combinación de ellos. En cualquier caso, el coste de las líneas se usa como entrada a un algoritmo de encaminamiento de mínimo coste, que establece que:

> Dada una red de nodos conectados entre sí por enlaces bidireccionales, donde cada enlace tiene un coste asociado en cada sentido, se define el coste de una ruta entre dos nodos como la suma de los costes de los enlaces atravesados. Así, para cada par de nodos se obtiene el camino de mínimo coste.

Obsérvese que el coste de un enlace puede ser diferente para cada uno de los dos sentidos. Esto sería cierto, por ejemplo, si el coste de un enlace fuese igual a la longitud de la cola de paquetes esperando ser transmitidos sobre el enlace por uno de los dos nodos.

La mayor parte de los algoritmos de encaminamiento de mínimo coste utilizados en las redes de conmutación de paquetes y en todas las internet son variantes de uno de los dos algoritmos más comunes: el de Dijkstra y el de Bellman-Ford. Este apéndice presenta una breve descripción de ambos algoritmos.

ALGORITMO DE DIJKSTRA

El algoritmo de Dijkstra [DIJK59] se puede enunciar como sigue: encontrar las rutas más cortas entre un nodo origen dado y todos los demás nodos desarrollando los caminos en orden creciente de longitud. El algoritmo actúa en dos pasos. En el paso k-ésimo se determinan los caminos más cortos a los k nodos más cercanos (de menor coste) al nodo origen; estos nodos se almacenan en el conjunto T. En el paso $(k + 1)$ se añade a la lista T aquel nodo que presente el camino más corto desde el nodo origen y que no se encuentre ya incluido en la lista. A medida que se incorporan nuevos nodos a T, se define su camino desde el origen. El algoritmo se puede describir formalmente como sigue. Definamos:

N = conjunto de nodos de la red
s = nodo origen
T = lista o conjunto de nodos añadidos o incorporados por el algoritmo.
$w(i, j)$ = coste del enlace desde el nodo i al nodo j; $w(i, i) = 0$, $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados, $w(i, j) \geq 0$ si los dos nodos están directamente conectados
$L(n)$ = coste en curso obtenido por el algoritmo para el camino de mínimo coste del nodo s al nodo n; al finalizar el algoritmo, este coste corresponde al del camino de mínimo coste de s a n en el grafo

El algoritmo consta de tres pasos, repitiéndose los pasos 2 y 3 hasta que $T = N$; es decir, hasta que las rutas finales han sido asignadas a todos los nodos en la red:

1. **[Inicio]**

   $T = \{s\}$ el conjunto de nodos incorporado sólo consta del nodo origen s
   $L(n) = w(i, j)$, con $n \neq s$ el coste inicial de las rutas a los nodos vecinos es el asociado a los enlaces

2. **[Obtención del siguiente nodo]** Se busca el nodo vecino que no esté en T con el camino de menor coste desde s y se incorpora a T; también se incorporará el enlace desde ese nodo hasta un nodo de T que forma parte del camino. Esto se puede expresar como

   $$\text{Encontrar } x \in T \text{ tal que } L(x) = \min_{j \notin T} L(j)$$

   Añadir x a T, incorporando también el enlace desde x que contribuye a $L(x)$ como la componente de menor coste (es decir, el último salto en la ruta).

3. **[Actualización de los caminos de mínimo coste]**

   $$L(n) = \min [L(n), L(x) + w(x, n)] \quad \forall n \notin T$$

Si el último término es el mínimo, el camino desde s hasta n es ahora el camino desde s hasta x concatenado con el enlace desde x hasta n.

El algoritmo concluye cuando todos los nodos han sido añadidos a T. Al final, el valor $L(x)$ asociado a cada nodo x es el coste (longitud) de la ruta de mínimo coste de s a x. Además, T define el camino de mínimo coste desde s hasta cualquier otro nodo.

Cada iteración de los pasos 2 y 3 incorpora un nuevo nodo a T y define el camino de mínimo coste desde s hasta ese nodo, atravesando dicha ruta sólo nodos incluidos en T. Para comprender mejor esto considérese el siguiente razonamiento. Tras k iteraciones existen k nodos en T, habiéndose obtenido además el camino de mínimo coste desde s hasta cada uno de esos nodos. Consideremos ahora todos los caminos posibles desde s hasta los nodos no incluidos en T. Entre estos caminos existe uno de mínimo coste que pasa exclusivamente a través de nodos en T (véase Problema 10.7), terminando con un enlace directo entre algún nodo en T y un nodo no incluido en esta lista. Este nodo se añade a T y se define el camino asociado como la ruta de mínimo coste para ese nodo.

En la Tabla 10.4a y en la Figura 10.21 se muestra el resultado de aplicar el algoritmo al grafo de la Figura 10.6 con $s = 1$. Los enlaces sombreados definen el árbol de expansión correspondiente al grafo, mientras que los valores que aparecen rodeados por un círculo corresponden a la estimación actual de $L(x)$ para cada nodo x. Los nodos sombreados representan la incorporación de éstos a T. Obsérvese que en cada paso se obtiene el camino a cada nodo así como el coste asociado al mismo. Tras la última iteración se dispone del camino de mínimo coste a cada nodo y del coste asociado. El mismo procedimiento se puede utilizar considerando como nodo origen el 2, y así sucesivamente.

ALGORITMO DE BELLMAN-FORD

El algoritmo de Bellman-Ford [FORD62] se puede enunciar así: encontrar los caminos más cortos desde un nodo origen dado con la condición de que éstos contengan a lo sumo un enlace; a continuación encontrar los caminos más cortos con la condición de que contengan dos enlaces como máximo, y así sucesivamente. Este algoritmo actúa también en pasos, pudiéndose describir formalmente como sigue. Definamos:

Tabla 10.4. Ejemplo de algoritmos de encaminamiento de mínimo coste (haciendo uso de la Figura 10.6).

(a) Algoritmo de Dijkstra ($s = 1$)

Iteración	T	L(2)	Ruta	L(3)	Ruta	L(4)	Ruta	L(5)	Ruta	L(6)	Ruta
1	{1}	2	1-2	5	1-3	1	1-4	∞	—	∞	—
2	{1, 4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	∞	—
3	{1, 2, 4}	2	1-2	4	1-4-3	1	1-4	2	1-4-5	∞	—
4	{1, 2, 4, 5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
5	{1, 2, 3, 4, 5}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
6	{1, 2, 3, 4, 5, 6}	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

(b) Algoritmo de Bellman-Ford ($s = 1$)

h	$L_h(2)$	Ruta	$L_h(3)$	Ruta	$L_h(4)$	Ruta	$L_h(5)$	Ruta	$L_h(6)$	Ruta
0	∞	—	∞	—	∞	—	∞	—	∞	—
1	2	1-2	5	1-3	1	1-4	∞	—	∞	—
2	2	1-2	4	1-4-3	1	1-4	2	1-4-5	10	1-3-6
3	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6
4	2	1-2	3	1-4-5-3	1	1-4	2	1-4-5	4	1-4-5-6

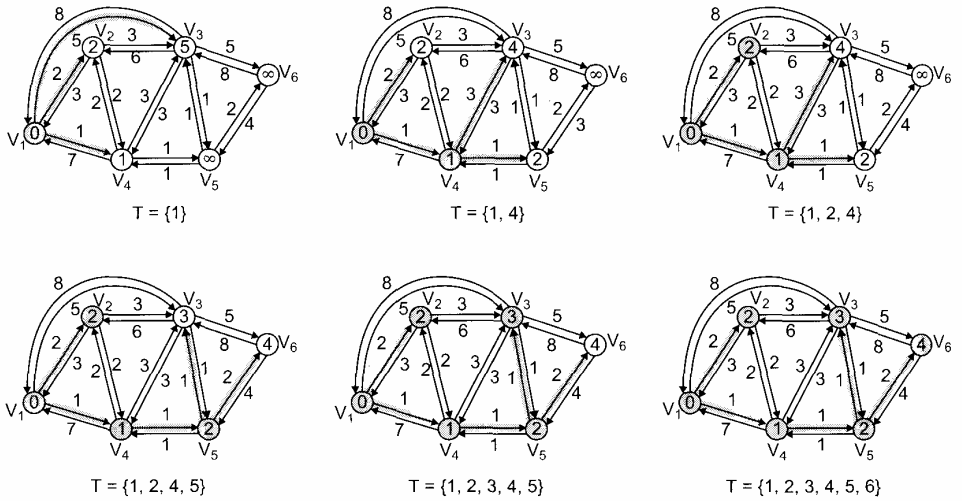


Figura 10.21. Algoritmo de Dijkstra aplicado al grafo de la Figura 10.6.

s = nodo origen

$w(i, j)$ = coste del enlace desde el nodo i al nodo j; $w(i, i) = 0$, $w(i, j) = \infty$ si los dos nodos no se encuentran directamente conectados, $w(i, j) \geq 0$ si los dos nodos están directamente conectados

h = número máximo de enlaces en un camino en el paso actual del algoritmo

$L_h(n)$ = coste del camino de mínimo coste desde el nodo s hasta el nodo n con la condición de no más de h enlaces

1. **[Inicio]**

   $L_0(n) = \infty$, $\forall n \neq s$
   $L_h(s) = 0$, $\forall h$

2. **[Actualización]**

   Para cada sucesivo $h \geq 0$:

   Para cada $n \neq s$, calcular

$$L_{h+1}(n) = \min_j [L_h(j) + w(j, n)]$$

   Conectar n con el nodo predecesor j de mínimo coste y eliminar todas las conexiones de n con un nodo predecesor diferente obtenido en una iteración anterior. El camino entre s y n finaliza con el enlace de j a n.

Para la iteración del paso 2 con $h = K$, y para cada nodo de destino n, el algoritmo compara las rutas potenciales de longitud $K + 1$ desde s hasta n con el camino existente al final de la iteración anterior. Si el camino más corto previo tiene un coste inferior, se guarda; en caso contrario, se define un nuevo camino de longitud $K + 1$ entre s y n, que consiste en una ruta de longitud K entre s y algún nodo j más un salto directo desde el nodo j hasta el nodo n. En este caso, el camino de s a j usado es la ruta de K saltos para j definida en la iteración anterior (véase Problema 10.8).

En la Tabla 10.4b y en la Figura 10.22 se muestra el resultado de aplicar este algoritmo a la Figura 10.6 usando $s = 1$. En cada paso se determinan las rutas de mínimo coste con un número máximo de

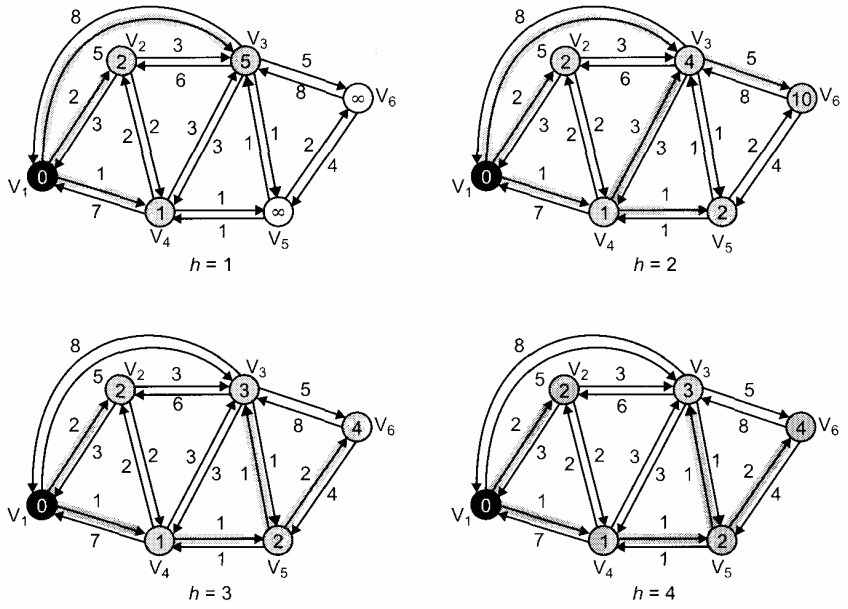


Figura 10.22. Algoritmo de Bellman-Ford aplicado al grafo de la Figura 10.6.

enlaces igual a h. Tras la última iteración se conoce el camino de mínimo coste a cada nodo y el coste asociado. El mismo procedimiento se puede usar tomando como nodo origen el nodo 2, y así sucesivamente. Obsérvese que los resultados coinciden con los obtenidos por el algoritmo de Dijkstra.

COMPARACIÓN

Una comparación interesante entre estos dos algoritmos hace referencia a la información necesaria a utilizar. Consideremos en primer lugar el algoritmo de Bellman-Ford. En el paso 2 del proceso, el cálculo para el nodo n requiere conocer el coste de los enlaces a todos los nodos vecinos de n (es decir, $w(j, n)$) además del coste total del camino a cada uno de estos nodos desde un nodo origen particular s (es decir, $L_h(j)$). Cada nodo puede mantener un conjunto de costes y rutas asociadas para cada uno de los otros nodos en la red e intercambiar periódicamente esta información con sus vecinos directos. Por tanto, cada nodo puede hacer uso de la expresión dada en el paso 2 del algoritmo de Bellman-Ford, basándose sólo en la información dada por sus vecinos y en el conocimiento del coste de las líneas asociadas, para actualizar los caminos y sus costes. Considérese por otra parte el algoritmo de Dijkstra. El paso 3 parece necesitar que cada nodo debe disponer de la información completa acerca de la topología de la red; es decir, cada nodo debe conocer todos los enlaces y los costes asociados a ellos. Así, en este algoritmo, la información se debe intercambiar con todos los demás nodos.

En general, en la evaluación de las ventajas relativas de ambos algoritmos se debe considerar el tiempo de procesamiento de los algoritmos y la cantidad de información a obtener del resto de nodos de la red o de Internet, dependiendo dicha evaluación de la implementación específica.

Por último, se ha de reseñar que ambos algoritmos convergen, hacia la misma solución, bajo condiciones estáticas de la topología y del coste de los enlaces. Si el coste de los enlaces cambia a lo largo del tiempo, el algoritmo tratará de reflejar estos cambios; sin embargo, si el coste de los enlaces depende del tráfico, quien a su vez depende de las rutas elegidas, existe una realimentación que puede provocar una situación de inestabilidad.

CAPÍTULO 11

Transferencia en modo asíncrono y retransmisión de tramas

- ATM es una interfaz funcional de transferencia de paquetes que tienen un tamaño fijo y se denominan celdas. El uso de un tamaño y formato fijos hace que esta técnica resulte eficiente para la transmisión a través de redes de alta velocidad.
- Para el transporte de celdas ATM debe usarse una estructura de transmisión. Una posibilidad consiste en la utilización de una cadena continua de celdas sin la existencia de una estructura de multiplexación de tramas en la interfaz; en este caso, la sincronización se lleva a cabo celda a celda. Una segunda opción es multiplexar las celdas mediante la técnica de división en el tiempo síncrona, en cuyo caso la secuencia de bits en la interfaz forma una trama externa basada en la jerarquía digital síncrona (SDH, Synchronous Digital Hierarchy).
- ATM proporciona servicios tanto de tiempo real como de no tiempo real, pudiendo soportar una amplia variedad de tráfico entre los que cabe citar secuencias TDM síncronas tales como T-1 usando el servicio de velocidad constante (CBR, Constant Bit Rate), voz y vídeo codificados usando el servicio de velocidad variable en tiempo real (rt-VBR, Real-time Variable Bit Rate), tráfico con requisitos específicos de calidad de servicio usando el servicio de no tiempo real de velocidad variable (nrt-VBR, non-real-time VBR) y tráfico IP haciendo uso de los servicios de velocidad disponible (ABR, Available Bit Rate) y de velocidad sin especificar (UBR, Unspecified Bit Rate).
- El uso de ATM implica la necesidad de una capa de adaptación para aceptar protocolos de transferencia de información que no se encuentren basados en ATM. La capa de adaptación ATM (AAL, ATM adaptation layer) agrupa la información del usuario AAL en paquetes de 48 octetos y la encapsula en una celda ATM, lo que puede conllevar la agrupación de bits de una cadena o la segmentación de una trama en trozos más pequeños.

El modo de transferencia asíncrono (ATM, Asynchronous Transfer Mode), también conocido como retransmisión de celdas, aprovecha las características de fiabilidad y fidelidad de los servicios digitales modernos para proporcionar una conmutación de paquetes más rápida que X.25. ATM se desarrolló como parte del trabajo en RDSI de banda ancha, pero ha encontrado aplicación en entornos distintos de RDSI en los que se necesitan velocidades de transmisión muy elevadas.
En primer lugar se presenta una descripción detallada del esquema ATM. A continuación se examinará el concepto de capa de adaptación ATM (AAL). Finalmente se ofrecerá un breve estudio de una tecnología anterior a ATM pero aún hoy muy utilizada: retransmisión de tramas («frame relay»).

11.1. ARQUITECTURA DE PROTOCOLOS

El modo de transferencia asíncrono (ATM) es similar en muchos aspectos a la conmutación de paquetes usando X.25 y a la técnica de retransmisión de tramas. Como ellas, ATM lleva a cabo la transferencia de los datos en trozos discretos. Además, al igual que X.25 y retransmisión de tramas, ATM permite la multiplexación de varias conexiones lógicas a través de una única interfaz física. En el caso de ATM, el flujo de información en cada conexión lógica se organiza en paquetes de tamaño fijo denominados **celdas**.

ATM es un protocolo funcional con mínima capacidad de control de errores y de flujo, lo que reduce el coste de procesamiento de las celdas ATM y reduce el número de bits suplementarios necesarios en cada celda, posibilitándose así su funcionamiento a altas velocidades. El uso de ATM a altas velocidades se ve apoyado adicionalmente por el empleo de celdas de tamaño fijo, ya que de este modo se simplifica el procesamiento necesario en cada nodo ATM.

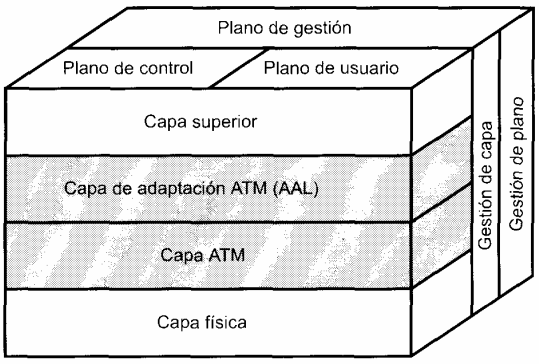


Figura 11.1. Arquitectura de protocolos ATM.

Las normalizaciones de ITU-T para ATM se basan en la arquitectura de protocolos mostrada en el Figura 11.1, donde se ilustra la arquitectura básica para una interfaz entre un usuario y la red. La capa física especifica un medio de transmisión y un esquema de codificación de señal. Las velocidades de transmisión especificadas en la capa física van desde 25,6 Mbps hasta 622,08 Mbps, siendo posibles velocidades superiores e inferiores.

Dos capas de la arquitectura están relacionadas con las funciones ATM. Existe una capa ATM común a todos los servicios de transferencia de paquetes, y una capa de adaptación ATM (AAL) dependiente del servicio. La capa ATM define la transmisión de datos en celdas de tamaño fijo, al tiempo que establece el uso de conexiones lógicas. El empleo de ATM crea la necesidad de una capa de adaptación para dar soporte a protocolos de transferencia de información que no se basan en ATM. AAL convierte la información procedente de capas superiores en celdas ATM para enviarlas a través de la red, al tiempo que extrae la información contenida en las celdas ATM y la transmite hacia las capas superiores.

El modelo de referencia de protocolos involucra tres planos independientes:

- **Plano de usuario:** permite la transferencia de información de usuario así como de controles asociados (por ejemplo, control de flujo y de errores).
- **Plano de control:** realiza funciones de control de llamada y de control de conexión.
- **Plano de gestión:** comprende la gestión de plano, que realiza funciones de gestión relacionadas con un sistema como un todo y proporciona la coordinación entre todos los planos, y la gestión de capa, que realiza funciones de gestión relativas a los recursos y a los parámetros residentes en las entidades de protocolo.

11.2. CONEXIONES LÓGICAS ATM

Las conexiones lógicas en ATM se denominan conexiones de canal virtual (VCC, virtual channel connection). Una VCC es similar a un circuito virtual en X.25 y constituye la unidad básica de conmutación en una red ATM. Una VCC se establece a través de la red entre dos usuarios finales, intercambiándose sobre la conexión celdas de tamaño fijo en un flujo *full-duplex* de velocidad variable. Las VCC se utilizan también para intercambios usuario-red (señalización de control) y red-red (gestión de red y encaminamiento).

En ATM se ha introducido una segunda subcapa de procesamiento para abordar el concepto de camino virtual (Figura 11.2). Una conexión de camino virtual (VPC, virtual path connection) es un haz de VCC con los mismos extremos, de manera que todas las celdas transmitidas a través de todas las VCC de una misma VPC se conmutan conjuntamente.

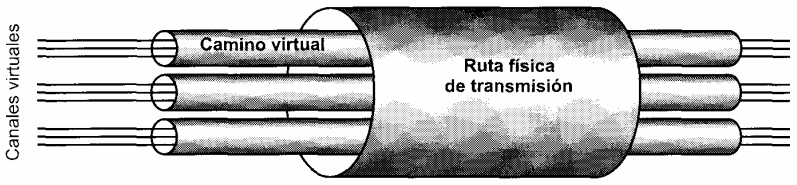


Figura 11.2. Relaciones entre conexiones ATM.

El concepto de camino virtual se desarrolló en respuesta a una tendencia en redes de alta velocidad en la que el coste del control está alcanzando una proporción cada vez mayor del coste total de la red. La técnica de camino virtual ayuda a contener el coste asociado al control mediante la agrupación en una sola unidad de aquellas conexiones que comparten rutas comunes a través de la red. Las acciones de la gestión de red se pueden aplicar a un reducido número de grupos en lugar de a un número de conexiones individuales elevado.

El uso de los caminos virtuales presenta varias ventajas:

- **Arquitectura de red simplificada:** las funciones de transporte de la red se pueden separar en dos grupos: aquellas relacionadas con una conexión lógica individual (canal virtual) y las relativas a un grupo de conexiones lógicas (camino virtual).
- **Incremento en eficiencia y fiabilidad:** la red maneja entidades totales menores.
- **Reducción en el procesamiento y tiempo de establecimiento de conexión pequeño:** gran parte del trabajo se realiza cuando se establece el camino virtual, de modo que la reserva de capacidad en la VPC antes de la llegada de nuevas llamadas permite establecer nuevos canales virtuales mediante la ejecución de funciones de control sencillas en los extremos del camino virtual. No se necesita procesamiento de llamadas en los nodos de tránsito, por lo que la incorporación de nuevos canales virtuales a un camino virtual ya existente conlleva un procesamiento mínimo.
- **Servicios de red mejorados:** el camino virtual se usa internamente a la red, aunque también es visible para el usuario final. Así, el usuario puede definir grupos de usuarios fijos o redes fijas de haces de canales virtuales.

En la Figura 11.3 se sugiere una forma general para el establecimiento de llamada haciendo uso de canales y caminos virtuales. El proceso de establecimiento de un camino virtual se encuentra desvinculado del proceso de establecimiento de un canal virtual individual:

- Entre los mecanismos de control de un camino virtual se encuentra la obtención de las rutas, la reserva de capacidad y el almacenamiento de información de estado de la conexión.
- El establecimiento de un canal virtual precisa la existencia previa de un camino virtual hacia el nodo de destino deseado con suficiente capacidad disponible para soportar dicho canal virtual y con la calidad de servicio adecuada. El establecimiento se lleva a cabo mediante el almacenamiento de la información de estado necesaria (asociación canal virtual/camino virtual).

La terminología de caminos y canales virtuales usada en la normalización es un poco confusa, y se resume en la Tabla 11.1. Mientras que la mayoría de los protocolos de la capa de red tratados en este libro se refieren exclusivamente a la interfaz entre el usuario y la red, los conceptos de camino y canal virtual se definen en las recomendaciones ITU-T con relación a la interfaz usuario-red y al funcionamiento interno de la red.

USO DE CANALES VIRTUALES

Los extremos de una VCC pueden ser usuarios finales, entidades de red o un usuario final y una entidad de red. En todos los casos se preserva la integridad de la secuencia de celdas dentro de una VCC; es

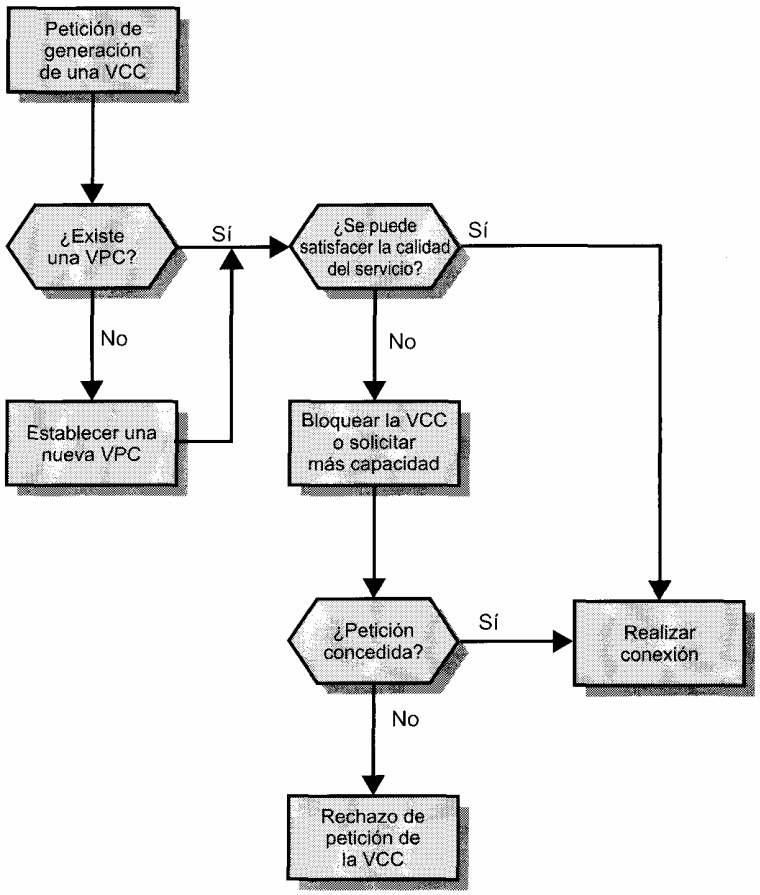


Figura 11.3. Establecimiento de llamadas mediante rutas virtuales.

decir, las celdas se entregan en el mismo orden en que se enviaron. Veamos ejemplos de los tres usos de una VCC:

- **Entre usuarios finales:** se puede utilizar para el transporte extremo a extremo de datos de usuario y, como se verá más adelante, para la transmisión de señalización de control entre usuarios finales. Una VPC entre usuarios finales les concede a éstos una capacidad total; la organización de la VPC en VCC se utiliza por los dos usuarios finales siempre que el conjunto de las VCC no supere la capacidad de la VPC.
- **Entre un usuario final y una entidad de red:** se usa para la señalización de control desde el usuario hacia la red como se verá posteriormente. Una VPC del usuario a la red se puede emplear para el tráfico total desde un usuario final hacia un conmutador o un servidor de red.
- **Entre dos entidades de red:** utilizado para la gestión del tráfico de red y con funciones de encaminamiento. Una VPC red-a-red puede ser usada para definir una ruta común para el intercambio de información de gestión de red.

CARACTERÍSTICAS CAMINO VIRTUAL/CANAL VIRTUAL

En la recomendación I.150 de ITU-T se especifican las siguientes características para las conexiones de canal virtual:

Tabla 11.1. Terminología de camino virtual/canal virtual.

Canal virtual (VC)	Término genérico usado para describir el transporte unidireccional de celdas ATM asociadas a un valor identificador único común.
Enlace de canal virtual	Medio de transporte unidireccional de celdas ATM entre un punto al que se asigna un valor de VCI y el punto en que éste se traduce o termina.
Identificador de canal virtual (VCI)	Marca numérica única que identifica un enlace VC particular de una VPC dada.
Conexión de canal virtual (VCC)	Concatenación de enlaces VC que se extiende entre dos puntos donde los usuarios de servicio ATM acceden a la capa ATM. Las VCC se utilizan con fines de transferencia de información usuario-usuario, usuario-red o red-red. Se preserva la integridad de la secuencia de celdas para aquéllas pertenecientes a la misma VCC.
Camino virtual	Término genérico usado para describir el transporte unidireccional de celdas ATM pertenecientes a canales virtuales asociados a un valor de identificación único común.
Enlace de camino virtual	Grupo de enlaces VC, identificado por un valor común de VPI, entre un punto al que se asigna un valor de VPI y el punto en que este valor se traduce o termina.
Identificador de camino virtual (VPI)	Identifica un enlace VP particular.
Conexión de camino virtual (VPC)	Concatenación de enlaces VP que se extiende entre el punto en que se asignan los valores de VCI y el punto en que estos valores se traducen o eliminan (es decir, amplía la longitud de un haz de enlaces VC que comparten el mismo VPI). Las VPC se emplean con objeto de transferir información usuario-usuario, usuario-red o red-red.

- **Calidad de servicio:** un usuario de una VCC es provisto con una calidad de servicio especificada por parámetros tales como la tasa de pérdida de celdas (relación entre las celdas perdidas y las transmitidas) y la variación del retardo de celdas.
- **Conexiones de canales virtuales conmutadas y semipermanentes:** una VCC conmutada es una conexión bajo demanda que necesita señalización de control de llamada para su establecimiento y terminación. Una VCC semipermanente se caracteriza por ser de larga duración y llevarse a cabo su establecimiento a través de una acción de configuración o de gestión de red.
- **Integridad de la secuencia de celdas:** se preserva la naturaleza secuencial de la secuencia de celdas transmitida en una VCC.
- **Negociación de parámetros de tráfico y supervisión del uso:** entre un usuario y la red se pueden negociar parámetros de tráfico para cada VCC. La entrada de celdas a la VCC es supervisada por la red para asegurar que se cumplen los parámetros negociados.

Entre los tipos de parámetros de tráfico que se pueden negociar se encuentran la velocidad media, la velocidad de pico, el tipo de ráfagas y la duración de pico. La red puede necesitar la utilización de varias estrategias para abordar la congestión y gestionar tanto las VCC existentes como las solicitadas. Al nivel más básico, la red puede limitarse simplemente a denegar nuevas peticiones de VCC para prevenir la congestión. Adicionalmente, las celdas se pueden descartar si no se respetan los parámetros negociados o si la congestión llega a ser importante, pudiendo llegar a liberarse las conexiones existentes si la situación es extrema.

El documento I.150 especifica también características de las VPC. Las cuatro primeras son idénticas a las de las VCC; es decir, calidad de servicio, VPC conmutadas y semipermanentes, integridad de la secuencia de celdas y negociación de parámetros de tráfico y supervisión del uso son también características propias de una VPC. Existen varias razones para esta duplicidad. En primer lugar, se provee así de cierta flexibilidad sobre cómo el servicio de red gestiona los requisitos que debe cumplir. En segundo lugar, la red debe ocuparse de las necesidades de una VPC, y dentro de una VPC puede negociar el establecimiento de canales virtuales con unas características concretas. Por último, una vez que se ha establecido una VPC, los usuarios finales pueden negociar la creación de nuevas VCC. Las características de la VPC determinan las elecciones que los usuarios finales pueden hacer.

Adicionalmente, existe una quinta característica para las VPC:

- **Restricción de identificador de canal virtual en una VPC:** puede que no sea posible proporcionar al usuario de una VPC uno o más identificadores, o números, de canal virtual, pero sí se pueden reservar para el uso de la red. Algunos ejemplos incluyen el uso de VCC para la gestión de la red.

SEÑALIZACIÓN DE CONTROL

En ATM es necesario un mecanismo para el establecimiento y liberación de VPC y VCC. El intercambio de información involucrado en este proceso se denomina señalización de control y tiene lugar a través de conexiones distintas de las que están siendo gestionadas.

El documento I.150 especifica cuatro métodos para llevar a cabo el establecimiento/liberación de VCC. En todas las redes se usa una o más combinaciones de estos métodos:

1. Las **VCC semipermanentes** se pueden usar para el intercambio usuario-usuario, en cuyo caso no se necesita señalización de control.
2. Si no existe canal de señalización de control de llamada preestablecido, se debe establecer uno. Con este fin debe tener lugar un intercambio de señales de control entre el usuario y la red a través de algún canal. Por tanto, es necesario un canal permanente, probablemente de baja velocidad, que pueda ser utilizado para establecer las VCC usadas para el control de llamadas. Un canal de este tipo se denomina **canal de meta-señalización** dado que se emplea para establecer canales de señalización.
3. El canal de meta-señalización se puede usar para establecer una VCC entre el usuario y la red para la señalización de control de llamadas. Este **canal virtual de señalización del usuario a la red** se puede utilizar para establecer VCC para la transmisión de datos de usuario.
4. El canal de meta-señalización se puede usar también para establecer un **canal virtual de señalización usuario-usuario**, que debe configurarse en una VPC preestablecida. Este canal se puede utilizar para posibilitar a los dos usuarios finales, sin que la red intervenga, el establecimiento y liberación de VCC usuario-usuario para el transporte de datos de usuario.

En I.150 se definen tres métodos para las VPC:

1. Una VPC se puede establecer de forma **semipermanente** con negociación previa. En este caso no se necesita señalización de control.
2. El establecimiento/liberación de las VPC puede ser **controlado por el usuario,** en cuyo caso el usuario utiliza una VCC de señalización para solicitar la VPC a la red.
3. El establecimiento/liberación de las VPC puede ser **controlado por la red.** En este caso, la red establece una VPC para su propio uso, pudiendo ser el camino de tipo red-red, del usuario a la red o usuario-usuario.

11.3. CELDAS ATM

El modo de transferencia asíncrono hace uso de celdas de tamaño fijo, que constan de 5 octetos de cabecera y de un campo de información de 48 octetos. El empleo de celdas pequeñas de tamaño fijo presenta varias ventajas. En primer lugar, el uso de celdas pequeñas puede reducir el retardo de cola para celdas de alta prioridad, ya que la espera es menor si se reciben ligeramente después de que una celda de baja prioridad hay conseguido el acceso a un recurso (por ejemplo, el transmisor). En segundo lugar, parece que las celdas de tamaño fijo se pueden conmutar más eficientemente, lo que es importante para las altas velocidades de ATM [PARE88]. La implementación física de los mecanismos de conmutación es más fácil para celdas de tamaño fijo.

FORMATO DE CABECERA

En la Figura 11.4a se muestra el formato de cabecera de las celdas en la interfaz usuario-red, mientras que en la Figura 11.4b se muestra el formato de cabecera de las celdas internas a la red.

El campo de **control de flujo genérico** (GFC, Generic Flow Control) no se incluye en la cabecera de las celdas internas a la red, sino sólo en la interfaz usuario-red, por lo que únicamente se puede usar para llevar a cabo el control de flujo de celdas en la interfaz local entre el usuario y la red. Este campo podría utilizarse para ayudar al usuario en el control del flujo de tráfico para diferentes calidades de servicio. En cualquier caso, el mecanismo GFC se usa con el fin de aliviar la aparición esporádica de sobrecarga en la red.

El documento I.150 especifica como requisito del mecanismo GFC que todos los terminales sean capaces de acceder a sus respectivas capacidades aseguradas. Esto incluye a todos los terminales de ve-

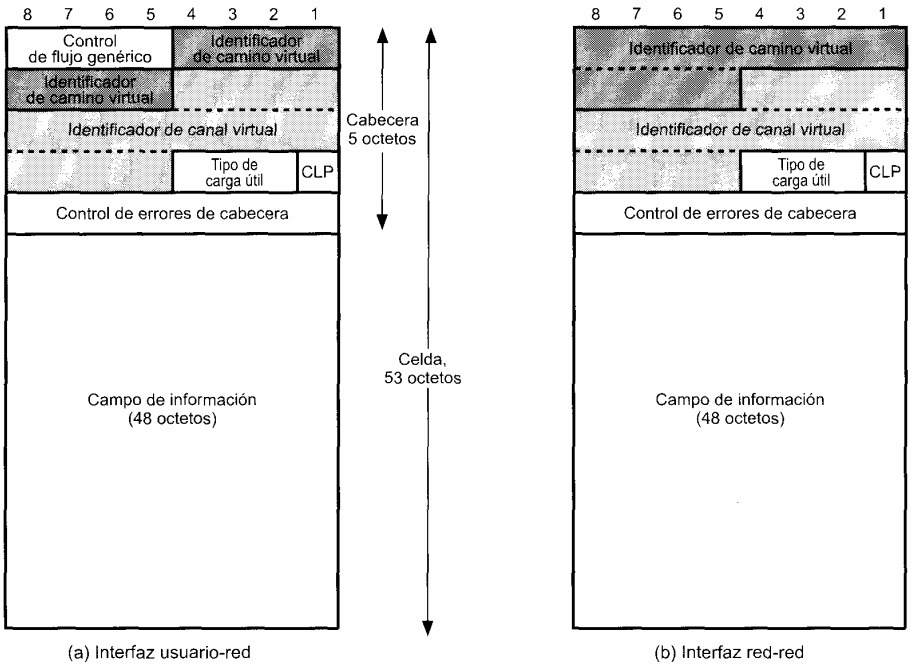


Figura 11.4. Formato de celda ATM.

Tabla 11.2. Codificación del campo de tipo de carga útil (PT).

Codificación PT	Interpretación
0 0 0	Celda de datos de usuario, no se ha producido congestión, tipo de SDU = 0
0 0 1	Celda de datos de usuario, no se ha producido congestión, tipo de SDU = 1
0 1 0	Celda de datos de usuario, se ha producido congestión, tipo de SDU = 0
0 1 1	Celda de datos de usuario, se ha producido congestión, tipo de SDU = 1
1 0 0	Ccelda asociada al segmento OAM
1 0 1	Ccelda asociada al OAM extremo a extremo
1 1 0	Celda de gestión de recursos
1 1 1	Reservada para funciones futuras

SDU = Unidad de Datos de Servicio.
OAM = Funcionamiento, Administración y Mantenimiento.

locidad constante (CBR, constant-bit-rate) así como a los de velocidad variable (VBR, variable-bit-rate) que disponen de un elemento de capacidad garantizada (CBR y VBR se explicarán en la Sección 11.5). El mecanismo GFC actual se describe en el siguiente apartado.

El **identificador de camino virtual** (VPI) es un campo de encaminamiento para la red, de 8 bits para la interfaz usuario-red y de 12 bits para la interfaz red-red. Este último caso permite un número superior de VPC internas a la red, tanto para dar servicio a subscriptores como las necesarias para la gestión de red. El **identificador de canal virtual** (VCI) se emplea para encaminar a y desde el usuario final.

El campo **tipo de carga útil** (PT, payload type) indica el tipo de información contenida en el campo de información. En la Tabla 11.2 se muestra la interpretación de los bits PT. Un valor 0 en el primer bit indica información de usuario (es decir, información procedente de la capa inmediatamente superior). En este caso, el segundo bit indica si se ha producido o no congestión; el tercer bit, llamado tipo de unidad de datos de servicio (SDU)[1], es un campo de 1 bit que se puede usar para discriminar dos tipos de SDU ATM asociadas a una conexión dada. El término SDU se refiere a la carga útil de 48 octetos de la celda. Un valor de 1 en el primer bit del campo PT indica que la celda transporta información de gestión de red o de mantenimiento. Esto permite la inserción de celdas de gestión de red en una VCC de usuario sin afectar a los datos de usuario, de modo que el campo PT proporciona información de control en banda.

El bit **prioridad de pérdida de celdas** (CLP) se emplea para ayudar a la red ante la aparición de congestión. Un valor 0 indica que la celda es de prioridad relativamente alta, no debiendo ser descartada a menos que no queda otra opción; un valor 1 indica por el contrario que la celda puede descartarse en la red. El usuario puede utilizar este campo para insertar celdas extra (una vez negociada la velocidad), con CLP igual a 1, y transmitirlas al destino si la red no está congestionada. La red puede poner este campo a 1 en aquellas celdas que violen los parámetros de tráfico acordados entre el usuario y la red. En este caso, el conmutador que lo activa se percata de que la celda excede los parámetros de tráfico establecidos pero que ésta puede ser procesada. Posteriormente, si se encuentra congestión en la red, esta celda se marcará para su rechazo antes que aquellas que se encuentran dentro de los límites de tráfico fijados.

Como se explica más adelante, el campo de **control de errores de cabecera** se usa tanto para el control de errores como con fines de sincronización.

CONTROL DE FLUJO GENÉRICO

En el documento I.150 se especifica el uso del campo GFC para llevar a cabo el control del flujo de tráfico en la interfaz usuario-red (UNI, user-network interface) con objeto de solucionar la aparición

[1] Éste es el término utilizado en los documentos del Foro ATM. Por su parte, en los documentos de la ITU-T se refiere a este bit como bit de indicación usuario ATM-usuario ATM (AAU). El significado es el mismo en ambos casos.

esporádica de sobrecarga. El mecanismo de control de flujo en sí se define en el documento I.361: el control de flujo GFC forma parte de un mecanismo de transferencia controlada de celdas (CCT, controlled cell transfer) propuesto, que está pensado para satisfacer los requisitos de redes LAN ATM conectadas a una red ATM de área extensa [LUIN97]. En particular, el mecanismo CCT está ideado para ofrecer un buen servicio para tráfico a ráfagas elevado con mensajes de longitud variable. En el resto de este apartado se estudia el mecanismo GFC tal como se especifica en la normalización.

Cuando los equipos en la UNI están configurados para aceptar el mecanismo GFC, se usan dos tipos de procedimientos: transmisión controlada y transmisión no controlada. Esencialmente, una conexión se identifica como sujeta a control de flujo o como no sujeta a control de flujo. Para las primeras puede existir un grupo de conexiones controladas (grupo A), caso por defecto, o el tráfico controlado se puede clasificar en dos grupos de conexiones controladas (grupo A y grupo B), las cuales se conocen como modelos de 1 cola y de 2 colas, respectivamente. El control de flujo se lleva a cabo por parte de la red en la dirección desde el abonado hacia ésta.

Considérese en primer lugar el funcionamiento del mecanismo GFC cuando sólo existe un grupo de conexiones controladas. El equipo controlado, llamado equipo terminal (TE, terminal equipment), inicia el valor de dos variables: TRANSMIT es un bit de señalización que se hace igual a SET (1), y GO_ NTR, contador de créditos, toma inicialmente el valor 0. Una tercera variable, GO_ VALUE, se hace igual a 1 o un valor superior en el momento de la configuración. Las reglas de transmisión para el dispositivo controlado son las siguientes:

1. Si TRANSMIT = 1, se pueden enviar celdas en cualquier instante de tiempo sobre conexiones no controladas.
   Si TRANSMIT = 0, no se pueden enviar celdas ni sobre las conexiones controladas ni sobre las no controladas.
2. Si se recibe una señal HALT del equipo de control, se hace TRANSMIT igual a 0 y permanece en este valor hasta que se reciba una señal NO_ HALT, en cuyo caso TRANSMIT pasará a valer 1.
3. Si TRANSMIT = 1 y no se dispone de celdas a transmitir sobre ninguna conexión no controlada:
   - Si GO_NTR > 0, el TE puede enviar una celda sobre una conexión controlada. El TE marca esta celda como una celda de una conexión controlada y decrementa GO_NTR.
   - Si GO_NTR = 0, el TE no puede enviar una celda sobre una conexión controlada.
4. El TE hace GO_NTR igual a GO_VALUE ante la recepción de una señal SET; una señal nula no tiene efecto sobre la variable GO_NTR.

La señal HALT se usa lógicamente para limitar la velocidad ATM efectiva, debiendo ser de naturaleza cíclica. Por ejemplo, para reducir a la mitad la velocidad de un enlace, el equipo de control genera la orden HALT de forma que sea efectiva durante el 50 % del tiempo. Esto se lleva a cabo de forma regular y predecible a lo largo de la duración de una conexión física.

En el modelo de 2 colas existen dos contadores, cada uno de ellos con un valor actual y otro de inicio: GO_NTR_A, GO_VALUE_A, GO_NTR_B y GO_VALUE_B. Esto permite al NT2 controlar dos grupos distintos de conexiones.

En la Tabla 11.3 se resumen las reglas de activación de los bits GFC.

CONTROL DE ERRORES DE CABECERA

Cada celda ATM incluye un campo de control de errores de cabecera (HEC, header error control) que se calcula en base a los restantes 32 bits de la cabecera. El polinomio usado para generar el código es $X^8 + X^2 + X + 1$. En la mayor parte de los protocolos existentes que incluyen un campo de control de errores, como HDLC, la cantidad de datos de entrada para el cálculo del código de error es generalmente mayor que el tamaño del código de error resultante, lo que permite la detección de errores. En el

Tabla 11.3. Codificación del campo de control de flujo genérico (GFC).

	No controlado	Controlador → controlado		Controlado → controlador	
		Modelo de 1 cola	Modelo de 2 colas	Modelo de 1 cola	Modelo de 2 colas
Primer bit	0	HALT(0)/ NO_HALT(1)	HALT(0)/ NO_HALT(1)	0	0
Segundo bit	0	SET(1) NULL(0)	SET(1)/ NULL(0) para el grupo A	Celda perteneciente a conexión controlada (1)/ no controlada (0)	Celda perteneciente (1)/ o no (0) al grupo A
Tercer bit	0	0	SET (1)/ NULL (0) para el grupo B	0	Celda perteneciente (1)/ o no (0) al grupo B
Cuarto bit	0	0	0	El equipo es no controlado (0)/controlado (1)	El equipo es no controlado (0)/controlado (1)

caso de ATM la entrada para el cálculo es sólo de 32 bits, comparados con los 8 bits del código. El hecho de que la entrada sea relativamente pequeña permite el uso del código no sólo para la detección de errores, sino que, en algunos casos, es posible la corrección de éstos. Esto se debe a que hay suficiente redundancia en el código para recuperar ciertos patrones de error.

En la Figura 11.5 se muestra el funcionamiento del algoritmo HEC en el receptor. Inicialmente, el algoritmo de corrección de errores del receptor corrige implícitamente errores simples. Para cada celda recibida se calcula y compara el HEC. Si no se detectan errores el receptor permanece en el modo de corrección de errores. En cambio, si se detecta un error, el receptor lo corrige si se trata de un error simple o, en caso contrario, detectará la ocurrencia de un error múltiple. En cualquier caso, el receptor pasa a modo de detección, no tratando de corregir errores. La razón de este cambio es que un ruido de tipo ráfaga u otro suceso podrían causar una secuencia de errores, situación para la que el HEC resulta insuficiente para su corrección. El receptor permanece en el modo de detección mientras se reciban celdas erróneas, pasando al modo de corrección cuando se examina una cabecera y no se encuentra error alguno. El diagrama de flujo de la Figura 11.6 muestra el efecto de la aparición de errores en la cabecera de una celda.

La función de protección de errores permite la recuperación de los errores de cabecera simples y la existencia de una baja probabilidad de envío de celdas con errores de cabecera provocados por condicio-

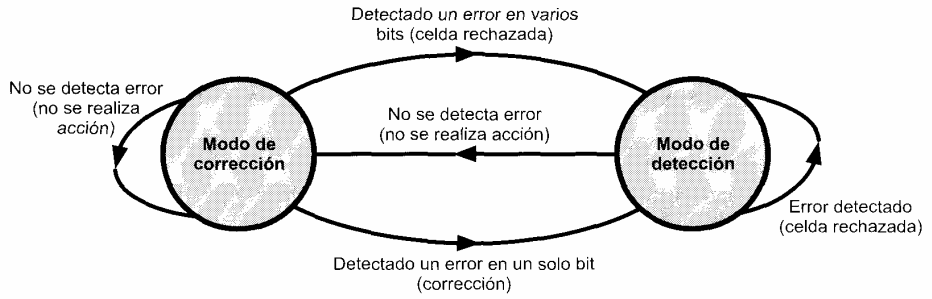


Figura 11.5. Operación HEC en el receptor.

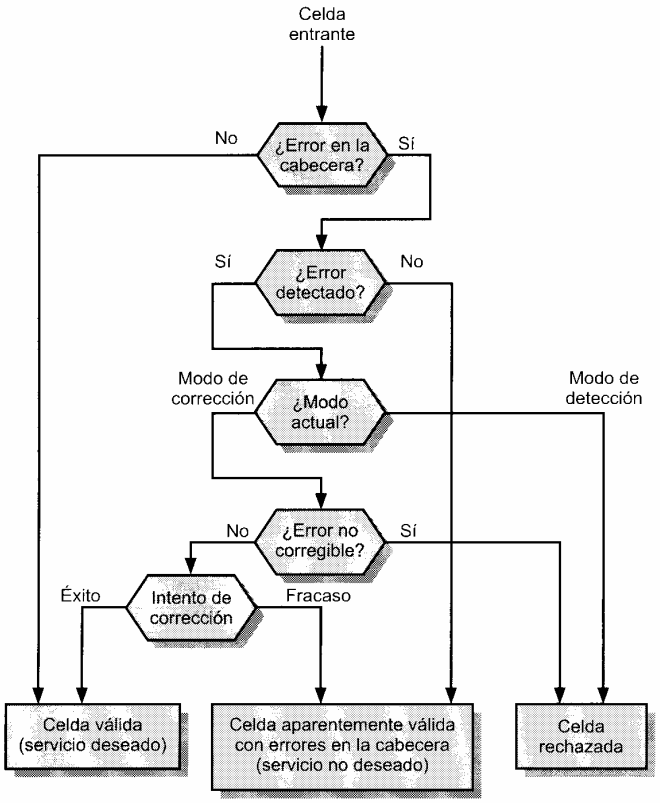


Figura 11.6. Efecto de un error en la cabecera de una celda.

nes de error a ráfagas. Las características de error en sistemas de transmisión de fibra óptica parecen ser una mezcla de errores simples y errores a ráfagas relativamente largas. En algunos sistemas de transmisión no se utiliza la capacidad de detección de errores debido a su alto coste temporal.

En la Figura 11.7, basada en una que aparece en la recomendación I.432 de ITU-T, se indica la forma en que los errores en bits aleatorios afectan a la probabilidad de rechazo de celdas y a la obtención de celdas válidas con cabeceras erróneas cuando se usa HEC.

11.4. TRANSMISIÓN DE CELDAS ATM

El documento I.432 especifica que las celdas ATM se pueden transmitir a distintas velocidades: 622,08 Mbps, 155,52 Mbps, 51,84 Mbps o 25,6 Mbps, siendo necesario especificar la estructura de transmisión a usar para el transporte de la carga útil. En el documento referido se definen dos enfoques: una capa física basada en celdas y una capa física basada en SDH[2]. A continuación se estudia cada una de ellas.

[2] La aproximación basada en SDH no está definida para 25,6 Mbps.

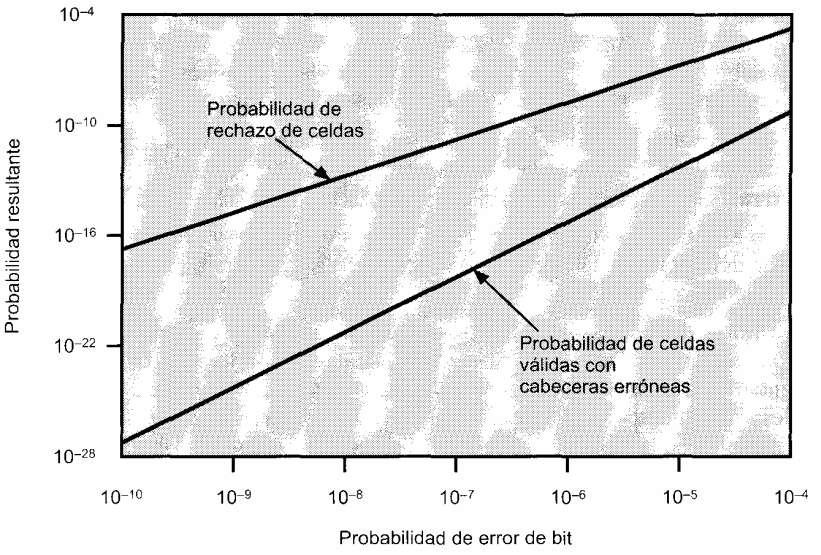


Figura 11.7. Impacto de errores de bit aleatorios en las prestaciones del HEC.

CAPA FÍSICA BASADA EN CELDAS

Para la capa física basada en celdas no se impone fragmentación o delimitación, consistiendo la estructura de la interfaz en una secuencia continua de celdas de 53 octetos. Dado que no existe imposición externa de tramas en esta aproximación, es necesaria alguna forma de llevar a cabo la sincronización. Ésta se consigue con el campo de control de errores de cabecera (HEC) incluido en la cabecera de la celda, siendo el procedimiento como sigue (Figura 11.8):

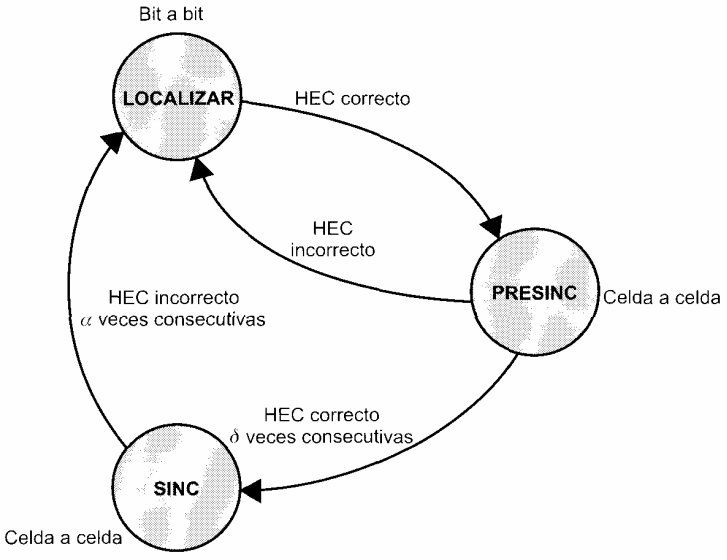


Figura 11.8. Diagrama de estados del procedimiento de delimitación de celdas.

1. En el estado LOCALIZAR se ejecuta bit a bit un algoritmo de delimitación de celdas para determinar el cumplimiento de la regla de codificación HEC (es decir, coincidencia entre el HEC recibido y el calculado). Una vez conseguida una coincidencia, se supone que se ha encontrado una cabecera, pasando el método al estado PRESINC.
2. En el estado PRESINC se supone una estructura de celda. El algoritmo de delimitación de celdas se lleva a cabo celda a celda hasta que la regla de codificación se confirme δ veces consecutivas.
3. En el estado SINC se usa el HEC para la detección y corrección de errores (véase Figura 11.5). La delimitación de la celda se supone perdida si la regla de codificación HEC resulta incorrecta α veces consecutivas.

Los valores de α y δ son parámetros de diseño. Valores de δ elevados provocan grandes retardos en la sincronización, pero mayor robustez contra falsas delimitaciones. Por su parte, valores grandes de α incrementan los retardos en la detección de desalineamientos, aunque también lo hace la robustez contra falsos desalineamientos. En las Figuras 11.9 y 11.10, basadas en el documento I.432, se muestra el impacto de errores en bits aleatorios sobre las prestaciones de la delimitación de celdas para distintos valores de α y δ. La primera figura muestra el tiempo promedio que el receptor mantendrá la sincronización ante la producción de errores, con α como parámetro. La segunda figura muestra el tiempo medio necesario para conseguir la sincronización en función de la tasa de error, con δ como parámetro.

La ventaja de usar el esquema de transmisión basado en celdas es la sencillez de la interfaz que resulta cuando tanto las funciones en modo de transferencia como las de en modo de transmisión se basan en una estructura común.

CAPA FÍSICA BASADA EN SDH

La capa física basada en SDH impone una estructura sobre la secuencia de celdas ATM. En esta sección se verá la especificación I.432 para 155,52 Mbps, usándose estructuras similares para otras velocidades.

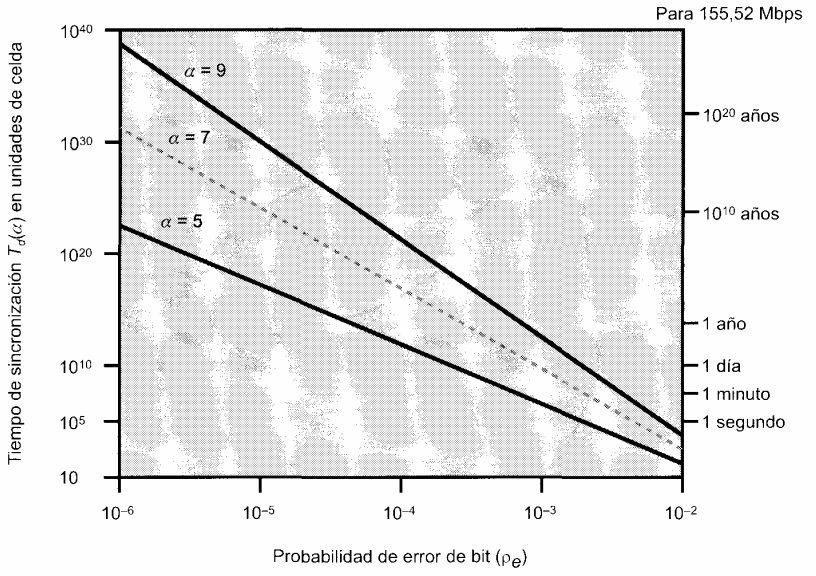


Figura 11.9. Impacto de errores de bit aleatorios en las prestaciones de la delimitación de celdas.

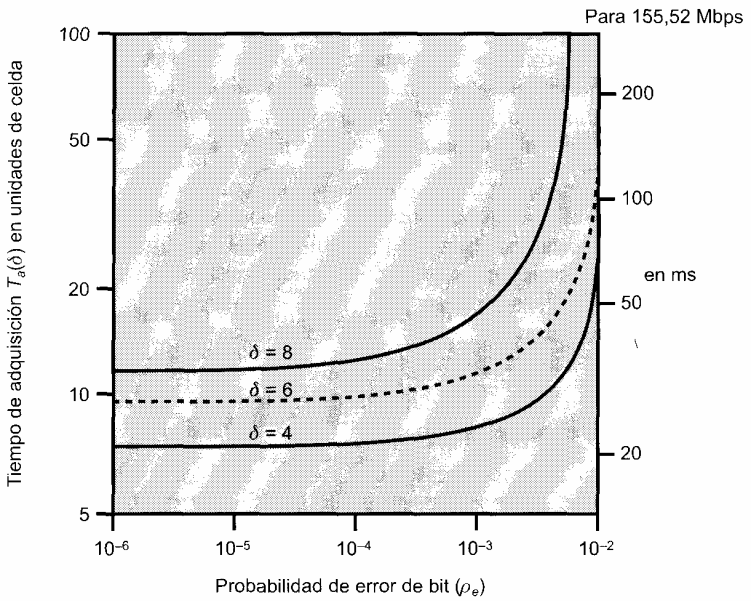


Figura 11.10. Tiempo de adquisición frente a la probabilidad de error de bit.

En la capa física basada en SDH se impone la delimitación o fragmentación haciendo uso de la trama STM-1 (STS-3). En la Figura 11.11 se muestra la porción de carga útil de una trama STM-1 (véase Figura 8.12). Esta carga útil puede estar desplazada respecto del principio de la trama como indica el puntero en la parte de redundancia de la misma. Como puede verse, la carga útil consta de 9 octetos suplementarios de camino y el resto, que contiene las celdas ATM. Dado que la capacidad de la carga útil (2.340 octetos) no es un múltiplo entero del tamaño de la celda (53 octetos), ésta puede superar un límite de carga útil.

El octeto suplementario de camino H4 se utiliza en el extremo emisor para indicar la próxima ocurrencia de una frontera de celda; es decir, el valor del campo H4 indica el número de octetos hasta la primera frontera de celda que sigue al octeto H4. El rango de posibles valores es de 0 a 52.

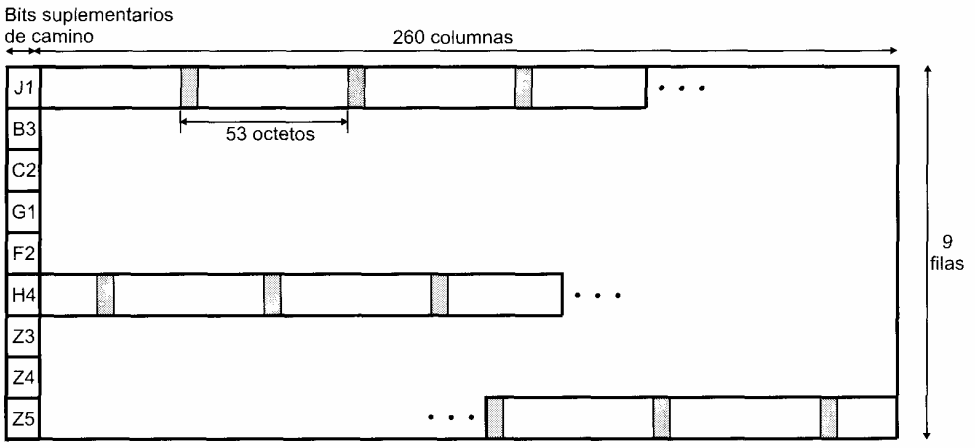


Figura 11.11. Carga útil STM-1 para transmisión de celdas ATM basada en SDH.

Entre las ventajas del enfoque basado en SDH se encuentran las siguientes:

- Se puede usar para transportar cargas útiles basadas en ATM o en STM (modo de transferencia síncrono), haciendo posible el despliegue inicial de una infraestructura de transmisión de fibra óptica de alta capacidad para un gran número de aplicaciones basadas en conmutación de circuitos y dedicadas y de fácil migración para el soporte de ATM.
- Algunas conexiones específicas pueden ser de conmutación de circuitos usando un canal SDH. Por ejemplo, el tráfico de una conexión de vídeo a velocidad constante puede llevarse a cabo segmentando éste en cargas útiles de la señal STM-1, que puede ser conmutada por circuitos. Esto puede resultar más eficiente que la conmutación ATM.
- Haciendo uso de las técnicas de multiplexación síncrona SDH se pueden combinar varias secuencias ATM para construir interfaces de velocidad superior a las ofrecidas por la capa ATM en un lugar específico. Por ejemplo, se pueden combinar cuatro secuencias ATM distintas, cada una a 155 Mbps (STM-1), para dar lugar a una interfaz de 622 Mbps (STM-4). Esta técnica puede ser más efectiva desde el punto de vista del coste que el uso de una única secuencia ATM a 622 Mbps.

11.5. CLASES DE SERVICIOS ATM

Una red ATM se diseña para poder transmitir simultáneamente diferentes tipos de tráfico, entre los que se encuentra la transmisión en tiempo real como voz, vídeo y tráfico TCP a ráfagas. Aunque cada uno de estos flujos de tráfico se gestiona como una secuencia de celdas de 53 octetos a través de un canal virtual, la forma en que se gestiona cada uno de ellos en la red depende de las características del flujo en cuestión y de los requisitos de la aplicación. Por ejemplo, el tráfico de vídeo en tiempo real se debe transmitir con variaciones mínimas de retardo.

En el Capítulo 12 se estudiará la forma en que una red ATM gestiona distintos tipos de tráfico. En esta sección se presentan las clases de servicios ATM, usadas por un sistema final para identificar el tipo de servicio requerido. En el Foro ATM se han definido las siguientes clases de servicios:

- **Servicio de tiempo real:**

  A velocidad constante (CBR, Constant Bit Rate).

  A velocidad variable en tiempo real (rt-VBR, real-time Variable Bit Rate).

- **Servicio de no tiempo real:**

  A velocidad variable en no tiempo real (nrt-VBR, non-real-time Variable Bit Rate).

  A velocidad disponible (ABR, Available Bit Rate).

  A velocidad no especificada (UBR, Unspecified Bit Rate).

SERVICIOS DE TIEMPO REAL

La distinción más importante entre aplicaciones se refiere al retardo y a la variabilidad de éste, conocida como fluctuación, que puede tolerar la aplicación. Las aplicaciones en tiempo real implican generalmente un flujo de información hacia un usuario que lo reproduce en una fuente. Por ejemplo, un usuario espera que la recepción de un flujo de información de audio o vídeo tenga lugar de forma continua y homogénea. La falta de continuidad o pérdidas excesivas provoca una disminución importante en la calidad, por lo que aquellas aplicaciones que conllevan una interacción entre usuarios son muy estrictas respecto del retardo, resultando generalmente perjudicial cualquier retardo que supere unas pocas centenas de milisegundos. En consecuencia, en una red ATM son elevadas las demandas de conmutación y envío de datos en tiempo real.

Velocidad constante (CBR)

El servicio CBR es quizás el más sencillo de definir. Se usa en aplicaciones que precisan una velocidad constante disponible durante toda la conexión y un retardo de transmisión máximo relativamente estable. CBR se usa comúnmente para información de audio y vídeo sin comprimir. Algunos ejemplos de aplicaciones CBR son los siguientes:

- Videoconferencia.
- Audio interactivo (por ejemplo, telefonía).
- Distribución de audio/vídeo (por ejemplo, televisión, enseñanza a distancia, servicios de tipo pagar-por-ver-«pay-per-view»-).
- Recuperación de audio/vídeo (por ejemplo, vídeo bajo demanda, audioteca).

Velocidad variable en tiempo real (rt-VBR)

La clase rt-VBR está pensada para aplicaciones sensibles al tiempo; es decir, aquellas que presentan fuertes restricciones en el retardo y en la variación de éste. La principal diferencia entre aplicaciones adecuadas para rt-VBR y aquellas indicadas para CBR es que en las primeras la transmisión se realiza a una velocidad que varía en el tiempo, o, lo que es lo mismo, una fuente rt-VBR se puede caracterizar por su funcionamiento a ráfagas. Por ejemplo, el enfoque estándar para compresión de vídeo produce una secuencia de tramas de imágenes de tamaño variable, por lo que, dado que el vídeo en tiempo real necesita una velocidad de transmisión de tramas uniforme, la velocidad real variará.

El servicio rt-VBR permite más flexibilidad a la red que el servicio CBR, ya que la red puede multiplexar estadísticamente varias conexiones sobre la misma capacidad dedicada y aun así proporcionar el servicio requerido para cada una de ellas.

SERVICIOS DE NO TIEMPO REAL

Los servicios que no son en tiempo real están pensados para aplicaciones que presentan características de tráfico a ráfagas y no presentan fuertes restricciones por lo que respecta al retardo y a la variación del mismo. Consecuentemente, la red presenta una mayor flexibilidad en la gestión de los flujos de tráfico y puede hacer un mayor uso de la multiplexación estadística para aumentar su eficiencia.

Velocidad variable en no tiempo real (nrt-VBR)

Para algunas aplicaciones que no son en tiempo real es posible caracterizar el flujo de tráfico esperado de forma que la red pueda proporcionar una calidad de servicio (QoS, Quality of Service) sustancialmente mejorada desde el punto de vista de las pérdidas y el retardo. Estas aplicaciones pueden hacer uso del servicio nrt-VBR, en el que el usuario final especifica una velocidad de pico de celdas, una velocidad de celdas sostenible o promedio y una medida acerca de cómo de agrupadas o en ráfagas pueden estar las celdas. Con esta información, la red puede reservar recursos para ofrecer un retardo relativamente pequeño y una pérdida de celdas mínima.

El servicio nrt-VBR se puede utilizar para transmisiones de datos que presentan requisitos críticos en cuanto a la respuesta en el tiempo. Algunos ejemplos de ello son reserva de vuelos, transacciones bancarias y supervisión de procesos.

Velocidad no especificada (UBR)

En cualquier instante de tiempo, una cierta cantidad de la capacidad de una red ATM se consume en el transporte de tráfico CBR y tráfico VBR de los dos tipos existentes. Una parte adicional de la capacidad

se encuentra disponible por una o las dos razones siguientes: (1) no todos los recursos se han destinado a tráfico CBR y VBR, y (2) la naturaleza a ráfagas del tráfico VBR implica que a veces se usa menos capacidad de la reservada. Toda esta capacidad sin usar se encuentra disponible para el servicio UBR. Este servicio es adecuado para aplicaciones que toleran retardos variables y cierta tasa de pérdida de celdas, lo que es generalmente cierto para tráfico TCP. En el servicio UBR, las celdas se transmiten según una cola FIFO (first-in-first-out) haciendo uso de la capacidad no consumida por otros servicios, siendo posible la aparición de retardos y pérdidas variables. Hemos de señalar que en el servicio UBR no se hacen reservas iniciales ni se proporciona realimentación relativa a la congestión, por lo que se conoce como **servicio de mínimo esfuerzo.** Algunos ejemplos de aplicaciones UBR son los siguientes:

- Transferencia, mensajería, distribución, recuperación de texto/datos/imágenes.
- Terminal remoto (por ejemplo, teleconmutación).

Velocidad disponible (ABR)

Como se estudiará en el Capítulo 17, las aplicaciones de transmisión a ráfagas que usan un protocolo fiable extremo a extremo como TCP pueden detectar congestión en una red a través del incremento en los retardos en el viaje de ida y vuelta y en base al rechazo de paquetes. Sin embargo, TCP no dispone de ningún mecanismo para compartir los recursos internos a la red entre varias conexiones TCP; además, TCP no minimiza la congestión tan eficientemente como es posible haciendo uso de información explícita de los nodos de la red congestionados.

Para mejorar el servicio ofrecido a las fuentes de naturaleza a ráfagas, que deberían hacer uso del servicio UBR, se ha definido el servicio ABR. Una aplicación que haga uso de ABR especifica una velocidad de pico de celdas (PCR, Peak Cell Rate) a usar y una velocidad de celdas mínima (MCR, Minimum Cell Rate) necesaria. La red reserva los recursos de forma que todas las aplicaciones ABR reciban al menos su capacidad MCR, compartiéndose la capacidad no usada de forma equitativa y controlada por todas las fuentes ABR. El mecanismo ABR hace uso explícito de realimentación hacia las fuentes para asegurar que la capacidad se ha reservado adecuadamente. La capacidad no usada por las fuentes ABR permanece disponible para tráfico UBR.

Un ejemplo de aplicación que usa ABR es la interconexión de redes LAN. En este caso, los sistemas finales conectados a la red ATM son dispositivos de encaminamiento.

En la Figura 11.12 se sugiere cómo una red lleva a cabo la reserva de recursos durante un periodo de tiempo estable (no se añaden ni se eliminan canales virtuales).

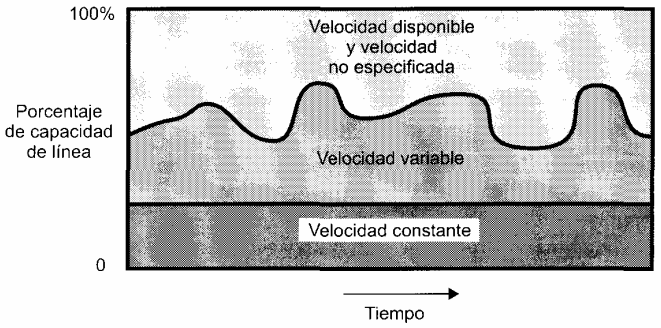


Figura 11.12. Servicios ATM a distintas velocidades.

11.6. CAPA DE ADAPTACIÓN ATM

El uso de ATM hace necesaria la existencia de una capa de adaptación para dar soporte a protocolos de transferencia de información que no estén basados en ATM. Dos ejemplos de ello son voz PCM (modulación por código de pulso) y el protocolo Internet (IP). Voz PCM es una aplicación que genera una secuencia de bits a partir de una señal de voz. Para utilizar esta aplicación sobre ATM es necesario agrupar bits PCM en celdas para su transmisión, y leerlas cuando sean recibidas en el receptor de manera que se obtenga un flujo homogéneo y constante de bits. En un entorno heterogéneo en el que existen redes IP interconectadas con redes ATM, una forma adecuada de integrar los dos tipos de redes es realizar una transformación entre paquetes IP y celdas ATM; esto implicará en general la segmentación de un paquete IP en varias celdas para su transmisión y el ensamblado de la trama a partir de las celdas en el receptor. Permitiendo el uso de IP sobre ATM es posible la utilización de toda la infraestructura IP existente sobre una red ATM.

SERVICIOS AAL

El documento I.362 de ITU-T especifica los siguientes ejemplos generales de servicios ofrecidos por AAL:

- Gestión de errores de transmisión.
- Segmentación y ensamblado para permitir la transmisión de bloques de datos mayores en el campo de información de las celdas ATM.
- Gestión de condiciones de pérdida de celdas y de celdas mal insertadas.
- Control de flujo y de temporización.

Con objeto de minimizar el número de protocolos AAL diferentes que se deben especificar para dar respuesta a distintas necesidades, ITU-T ha definido cuatro clases de servicios que cubren un amplio rango de requisitos. La clasificación se realiza teniendo en cuenta si se debe mantener una relación de temporización entre el emisor y el receptor, si la aplicación necesita una velocidad constante y si la transferencia es o no orientada a conexión. El sistema de clasificación no se encuentra en ningún documento de la ITU-T, pero el concepto ha permitido el desarrollo de protocolos AAL. Esencialmente, la capa AAL proporciona mecanismos para dar cabida a una amplia variedad de aplicaciones sobre la capa ATM y ofrece protocolos construidos sobre la base de las capacidades de gestión de tráfico de la capa ATM. En consecuencia, el diseño de los protocolos AAL debe estar relacionado con las clases de servicio estudiadas en la Sección 11.5.

En la Tabla 11.4, que está basada en una tabla de [MCDY99], se relacionan los cuatro protocolos AAL con las clases de servicios definidas por el Foro ATM. En la tabla se sugieren los tipos de aplicaciones que pueden soportar conjuntamente AAL y ATM. Entre ellas se encuentran las siguientes:

- **Emulación de circuitos:** hace referencia al soporte de estructuras de transmisión TDM síncronas, tales como T-1, sobre redes ATM.
- **Voz y vídeo VBR:** son aplicaciones en tiempo real que se transmiten en formato comprimido. Un efecto de la compresión es que la aplicación puede estar soportada por una velocidad variable, lo que requiere un envío continuo de bits hacia el destino.
- **Servicios generales de datos:** entre ellos se incluyen servicios de mensajería y transacciones que no precisan soporte en tiempo real.
- **IP sobre ATM:** transmisión de paquetes IP en celdas ATM.
- **Encapsulado multiprotocolo sobre ATM (MPOA):** soporte de protocolos distintos de IP (por ejemplo, IPX, AppleTalk, DECNET) en ATM.

Tabla 11.4. Protocolos y servicios AAL.

	CBR	rt-VBR	nrt-VBR	ABR	UBR
AAL 1	Emulación de circuitos, RDSI, voz sobre ATM				
AAL 2		Voz y vídeo VBR			
AAL 3/4			Servicios generales de datos		
AAL 5	Emulación de redes LAN	Voz bajo demanda, emulación LANE	Retransmisión de tramas, ATM, emulación LANE	Emulación LANE	IP sobre ATM

- **Emulación de redes LAN:** soporte de tráfico entre redes LAN a través de redes ATM, con emulación de la capacidad de difusión LAN (la transmisión de una estación se recibe en muchas otras estaciones). LANE se diseña para permitir una transición cómoda entre un entorno LAN y otro ATM.

PROTOCOLOS AAL

La capa AAL se organiza en dos subcapas lógicas: la de convergencia (CS, convergence sublayer) y la de segmentación y agrupación o ensamblado (SAR, segmentation and reassembly sublayer). La primera proporciona las funciones necesarias para dar soporte a aplicaciones específicas que hacen uso de AAL. Cada usuario AAL se conecta a la capa AAL a través de un punto de acceso al servicio (SAP, service access point), que no es más que la dirección de la aplicación. Esta subcapa es, por tanto, dependiente del servicio.

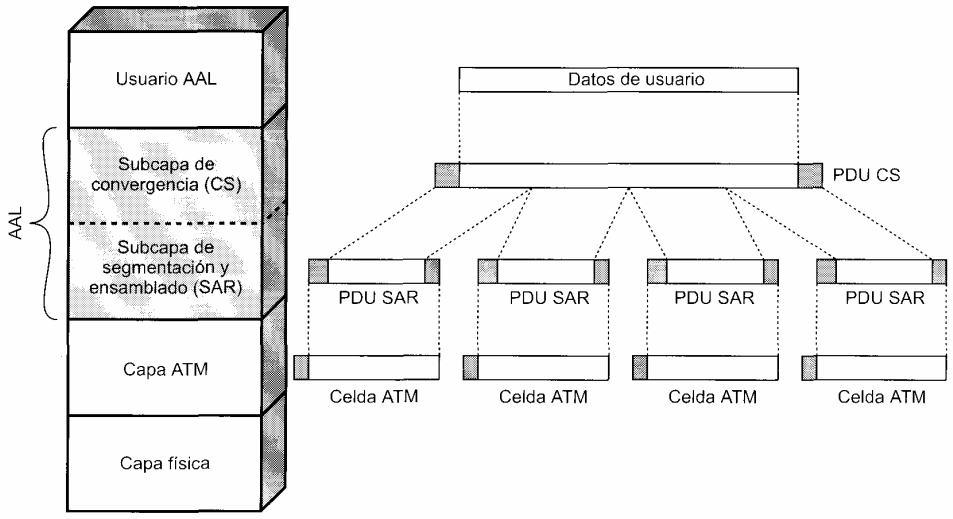


Figura 11.13. Protocolos y PDU AAL.

La subcapa de segmentación y ensamblado es responsable de empaquetar la información recibida desde la subcapa CS en celdas para su transmisión, y desempaquetar la información en el otro extremo. Como se ha visto, cada celda en la capa ATM consta de una cabecera de 5 octetos y de un campo de información de 48 octetos. Así, la subcapa SAR debe empaquetar las cabeceras y colas SAR y añadir información de la subcapa CS en bloques de 48 octetos.

En la Figura 11.13 se indica la arquitectura de protocolos general para ATM y AAL. Generalmente, un bloque de datos procedente de una capa superior se encapsula en una unidad de datos de protocolo (PDU, protocol data unit) consistente en los datos de la capa superior y posiblemente una cabecera y una cola con información de protocolo del nivel CS. Esta PDU de la subcapa CS se pasa después hacia abajo hacia la capa SAR y se segmenta en varios bloques, cada uno de los cuales se encapsula en una PDU SAR de 48 octetos que puede incluir una cabecera y una cola además del bloque de datos procedente de la subcapa CS. Por último, cada PDU SAR constituye el campo de carga útil de una sola celda ATM.

Inicialmente, ITU-T definió cuatro tipos de protocolos, llamados Tipo 1 a Tipo 4. Realmente, cada tipo de protocolo consta de dos protocolos, uno en la subcapa CS y otro en la subcapa SAR. Recientemente se han unido los tipos 3 y 4, dando lugar al protocolo Tipo 3/4, y se ha definido un nuevo tipo, Tipo 5. En todos los casos, un bloque de datos procedente de una capa superior se encapsula en una unidad de datos de protocolo (PDU) de la subcapa CS. De hecho, esta subcapa se conoce como subcapa de convergencia común (CPCS, common part convergence sublayer), dejando abierta la posibilidad de que se puedan realizar funciones adicionales especializadas en la subcapa CS. La PDU CPCS se pasa posteriormente a la subcapa SAR, donde se trocea en bloques de carga útil. Cada uno de estos bloques se puede incluir en una PDU de la subcapa SAR, que tiene una longitud total de 48 octetos. A su vez, cada PDU SAR de 48 octetos se encapsula en una sola celda ATM.

En la Figura 11.14 se muestran los formatos de las unidades de datos de protocolo (PDU) de la capa SAR excepto para el Tipo 2, que no ha sido especificado aún.

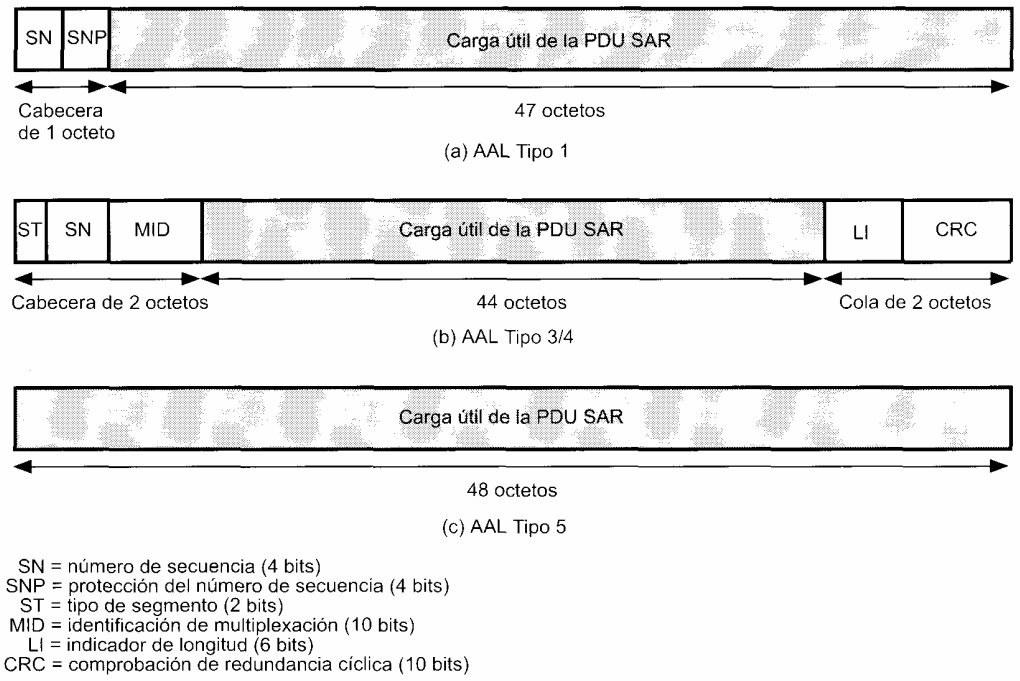


Figura 11.14. Unidades de datos de protocolo (PDU) de segmentación y ensamblado (SAR).

AAL Tipo 1

En la operación de tipo 1 se trabaja con fuentes de velocidad constante, siendo la única responsabilidad del protocolo SAR la de empaquetar los bits en celdas para su transmisión, y desempaquetarlos en el extremo receptor. Cada bloque se acompaña de un **número de secuencia** (SN) de forma que se pueda seguir la pista de las PDU erróneas. El campo SN de 4 bits consiste en un bit indicador de la subcapa de convergencia (CSI) y un contador de secuencia de 3 bits (SC). En el proceso de transmisión la subcapa CS proporciona un valor CSI a la subcapa SAR para su inclusión en el campo SN, pasando la subcapa SAR este valor hacia la subcapa CS en el proceso de recepción. El bit CSI se emplea para transmitir información de la siguiente forma. El contador de secuencia de 3 bits define una estructura de trama consistente en 8 celdas ATM consecutivas, numeradas de 0 a 7. Los valores del bit CSI en las celdas 1, 3, 5 y 7 se interpretan como un valor de tiempo de 4 bits usado para proporcionar una medida de la diferencia de frecuencia entre el reloj de referencia de la red y el del emisor. Por su parte, en las celdas pares, el bit CSI se puede usar para realizar el empaquetado de la información procedente de una capa superior: si este bit vale uno en una celda par (0, 2, 4, 6), el primer octeto del campo de carga útil de la PDU SAR es un puntero que indica el comienzo del siguiente bloque estructurado dentro de la carga útil de esta y de la siguiente celda; es decir, dos celdas (0-1, 2-3, 4-5, 6-7) se tratan como si contuviesen un puntero de un octeto y una carga útil de 93 octetos, indicando el puntero que es el primer octeto del siguiente bloque de datos dentro de la carga útil de 93 octetos. El valor de desplazamiento 93 se utiliza para indicar que el final de la carga útil de 93 octetos coincide con el final de un bloque estructurado, usándose el valor 127 cuando no se indica la frontera de la estructura.

Como se ha visto, el campo SC de 3 bits proporciona una estructura de trama de 8 celdas. También representa una forma de llevar a cabo la detección de celdas perdidas/desordenadas.

El campo de **protección del número de secuencia** (SNP) es un código de error para la detección y posible corrección de errores sobre el campo de número de secuencia. El campo SNP consta de una secuencia de comprobación de redundancia cíclica (CRC) de 3 bits, calculada sobre el campo SN de 4 bits, y de un bit de paridad, que se fija de modo que la paridad de la cabecera SAR de 8 bits sea par.

No se ha definido PDU CS alguna para el Tipo 1, estando en este caso relacionadas las funciones de la subcapa CS con la temporización y la sincronización y no siendo necesaria una cabecera CS independiente.

AAL Tipo 2

El resto de los tipos de protocolo (2, 3/4 y 5) gestionan información de velocidad variable. El Tipo 2 está destinado a aplicaciones analógicas, tales como vídeo y audio, que necesitan información temporal pero no precisan una velocidad constante. Se ha retirado una especificación inicial dada para los protocolos de tipo 2 (SAR y CS), enunciándose en la versión actual del documento I.363 una simple lista de servicios y funciones a proveer.

AAL Tipo 3/4

Las especificaciones iniciales de la capa AAL de Tipo 3 y de Tipo 4 eran muy similares en cuanto al formato de la PDU y a la funcionalidad. Consecuentemente, ITU-T decidió combinar los dos tipos en una sola especificación de protocolo para las subcapas SAR y CS, conocida como Tipo 3/4.

Los tipos de servicio proporcionados por AAL Tipo 3/4 se pueden caracterizar doblemente:

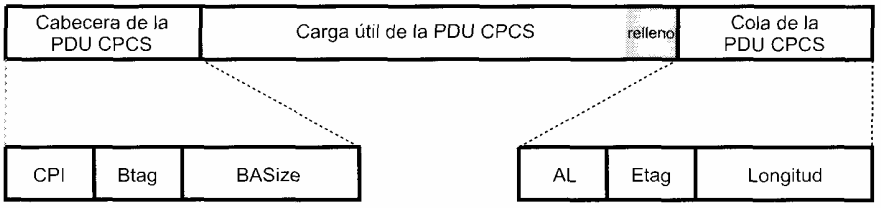
1. El servicio puede ser orientado o no a conexión. En el segundo caso, cada bloque de datos presentado a la capa SAR (unidad de datos de servicio de SAR o SDU SAR) se trata de forma independiente, mientras que en el caso del servicio orientado a conexión es posible definir varias conexiones lógicas SAR en una misma conexión ATM.
2. El servicio puede realizarse en modo de mensaje o en modo continuo. En el primer tipo de servicio se transfieren los datos por medio de tramas, teniendo así cabida en este tipo de servicio

los protocolos y aplicaciones OSI; en particular, LAPD o la técnica de retransmisión de tramas se podrían llevar a cabo en modo de mensaje: un solo bloque de datos de la capa superior a AAL se transmite en una o más celdas. Por su parte, el servicio en modo continuo implica la transferencia continua de datos de baja velocidad con requisitos de pequeño retardo; en este caso, los datos se pasan a AAL en bloques de tamaño fijo que pueden ser tan cortos como un octeto, transmitiéndose un bloque por celda.

El protocolo AAL de Tipo 3/4 lleva a cabo su servicio de transferencia de datos aceptando bloques de éstos de la capa superior y transmitiendo cada uno de ellos hacia el usuario AAL de destino. Dado que la capa ATM limita la transferencia de datos a la carga útil de 48 octetos de una celda, la capa AAL debe realizar, como mínimo, una función de segmentación y ensamblado.

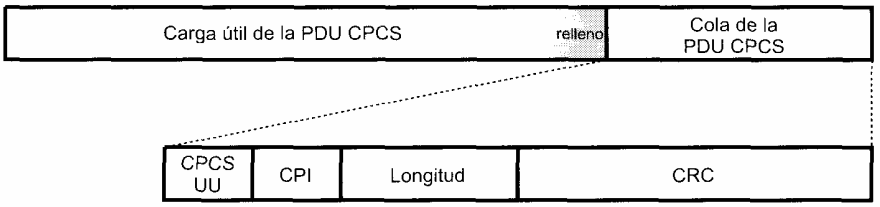
La aproximación considerada en el Tipo 3/4 es la que sigue. Un bloque de datos de una capa superior, como una PDU, se encapsula en una PDU de la subcapa CPCS, la cual se pasa a la subcapa SAR y se segmenta en bloques de carga útil de 44 octetos. Cada bloque de carga útil se encapsula en una PDU SAR, que incluye una cabecera y una cola en un total de 48 octetos de longitud. Finalmente, cada PDU SAR de 48 octetos se encapsula en una sola celda ATM.

Para comprender el funcionamiento de las dos subcapas en AAL de Tipo 3/4, veamos las respectivas PDU. La PDU de la subcapa CPCS se muestra en la Figura 11.15a, cuya cabecera consta de tres campos:



CPI = indicador de parte común (1 octeto)
Btag = marca de inicio (1 octeto)
BASize = tamaño de la reserva de memoria temporal (2 octetos)
AL = alineamiento (1 octeto)
Etag = marca de fin (1 octeto)
Longitud = longitud de la carga útil de la PDU CPCS (2 octetos)

(a) AAL Tipo 3/4



CPCS UU = indicador usuario-usuario CPCS (1 octeto)
CPI = indicador de parte común (1 octeto)
Longitud = longitud de la carga útil de la PDU CPCS (2 octetos)
CRC = comprobación de redundancia cíclica (4 octetos)

(b) AAL Tipo 5

Figura 11.15. PDU de la subcapa CPCS.

- **Indicador de parte común —CPI— (1 octeto):** indica la interpretación del resto de campos en la cabecera de la PDU CPCS. Actualmente sólo se define una interpretación: un valor de CPI igual a 0 indica que el campo BASize define las necesidades de reserva de memoria temporal en octetos y que el campo Longitud especifica la longitud de la carga útil de la PDU CPCS en octetos.
- **Marca de inicio —Btag— (1 octeto):** número asociado con una PDU CPCS particular. El mismo valor aparece en el campo Btag de la cabecera y en el campo Etag de la cola. El emisor cambia el valor para cada PDU CPCS sucesiva, posibilitando al receptor asociar correctamente la cabecera y la cola de cada PDU CPCS.
- **Tamaño de la reserva de memoria temporal —BASize— (2 octetos):** indica a la entidad par receptora el tamaño máximo de memoria temporal necesario para el ensamblado de las SDU (unidad de datos de servicio) CPCS. Para el modo de mensaje, este valor es igual a la longitud de la carga útil de la PDU CPCS, mientras que para el modo continuo el valor de BASize es mayor o igual que dicha longitud.

La carga útil procedente de la capa superior se somete a un relleno de bits de forma que la cola comience en un límite de 32 bits. La cola de la PDU CPCS contiene tres campos:

- **Alineamiento (1 octeto):** octeto de relleno con el único objeto de hacer la longitud de la PDU CPCS igual a 32 bits.
- **Marca de fin (1 octeto):** usado con el campo Btag de la cabecera.
- **Longitud (2 octetos):** longitud del campo de carga útil de la PDU CPCS.

Así, el propósito de la capa CPCS es avisar al receptor sobre la recepción en segmentos de un bloque de datos y la necesidad de llevar a cabo la reserva de memoria temporal para el proceso de ensamblado. Esto posibilita a la función de recepción CPCS verificar la correcta recepción de la PDU CPCS completa.

En la Figura 11.14b se muestra el formato de la PDU SAR de Tipo 3/4. De la capa CS superior se recibe información en bloques denominados unidades de datos de servicio (SDU) SAR, siendo transmitida cada SDU en una o más PDU SAR. A su vez, cada PDU SAR se transmite sobre una celda ATM. El campo de cabecera de las PDU SAR se usa en la transmisión para el proceso de segmentación en la transmisión y para el proceso de ensamblado en la recepción de las SDU:

- **Tipo de segmento:** existen cuatro tipos de PDU para la subcapa SAR. Un mensaje de secuencia único (SSM) contiene una SDU SAR completa, de modo que si ésta se segmenta en una o más PDU SAR, la primera PDU será el comienzo del mensaje (BOM, Beginning Of Message), la última el final del mensaje (EOM, End Of Message) y las PDU SAR intermedias son continuación del mensaje (COM, Continuation Of Message).
- **Número de secuencia:** se usa en el ensamblado de una SDU SAR para verificar que todas las PDU SAR se han recibido y concatenado adecuadamente. En la PDU BOM se especifica un valor de número de secuencia, el cual se incrementa para cada PDU COM sucesiva y para la PDU EOM de una misma SDU SAR.
- **Identificación de multiplexación (10 bits):** identificador único asociado al conjunto de PDU SAR que transportan una sola SDU SAR. De nuevo se precisa este número para asegurar un ensamblado adecuado. En aplicaciones orientadas a conexión, este campo permite la multiplexación de varias conexiones SAR sobre una sola conexión ATM.

La cola de las PDU de la subcapa SAR contiene los siguientes campos:

- **Indicación de longitud:** indica el número de octetos de la SDU SAR que ocupan la unidad de segmentación de la PDU SAR. Este número tiene un valor comprendido entre 4 y 44 octetos en múltiplos de 4, siendo siempre igual a 44 para las PDU SAR BOM y COM. Este valor es menor para un SSM si la PDU SAR tiene un tamaño inferior a 44 octetos. Este indicador es también menor que 44 para una PDU EOM si la longitud de la PDU SAR no es un múltiplo entero de 44

octetos de longitud, precisándose el uso de una EOM a la que se ha realizado un relleno parcial. En este caso, al resto de la carga útil de la PDU SAR se le somete a un relleno de bits.

- **CRC:** es una secuencia CRC de 10 bits sobre la PDU SAR completa.

Una característica distintiva de AAL 3/4 es que puede multiplexar diferentes secuencias de datos sobre la misma conexión ATM virtual (VCI/VPI). En el servicio orientado a conexión, a cada conexión lógica entre usuarios AAL se le asigna un valor MID único, de modo que se puede multiplexar y mezclar sobre una sola conexión ATM el tráfico de celdas procedente de hasta 2^{10} conexiones AAL diferentes. En el caso del servicio no orientado a conexión, el campo MID se puede usar para comunicar un identificador único asociado a cada usuario del servicio y, de nuevo, se puede multiplexar tráfico proveniente de varios usuarios AAL.

AAL Tipo 5

La más reciente incorporación a la especificación AAL es el protocolo de tipo 5. Éste se introdujo para proporcionar un servicio de transporte funcional para protocolos de capa superior orientados a conexión. Si se supone que la capa superior lleva a cabo la gestión de la conexión y que la capa ATM produce errores mínimos, no son necesarios la mayor parte de los campos de las PDU SAR y CPCS de Tipo 3/4. Por ejemplo, el campo MID no es necesario para el servicio orientado a conexión: el VCI/VPI se encuentra disponible para la multiplexación celda a celda y la capa superior admite multiplexación mensaje a mensaje.

El Tipo 5 se introdujo para:

- Reducir el coste suplementario de procesamiento del protocolo.
- Reducir el coste de la transmisión.
- Asegurar la adaptabilidad a los protocolos de transporte existentes.

En las Figuras 11.14c y 11.15b se muestran los formatos de las PDU de las subcapas SAR y CPCS para el Tipo 5. En comparación con el Tipo 3/4, el Tipo 5 introduce los siguientes costes suplementarios:

Tipo 3/4	Tipo 5
8 octetos por SDU AAL	8 octetos por SDU AAL
4 octetos por celda ATM	0 octetos por celda ATM

Para comprender el funcionamiento del Tipo 5, comencemos por la capa CPCS. La PDU de esta capa (Figura 11.15b) incluye una cola con los siguientes campos:

- **Indicación usuario-usuario CPCS (1 octeto):** usado para la transferencia transparente de información entre usuarios.
- **Indicador de parte común (1 octeto):** indica la interpretación del resto de campos de la cola de la PDU CPCS. Actualmente sólo se encuentra definida una interpretación.
- **Longitud (2 octetos):** longitud del campo de carga útil de la PDU CPCS.
- **Comprobación de redundancia cíclica (4 octetos):** campo empleado para detectar errores de bits en la PDU CPCS.

Obsérvese que se ha eliminado el campo BASize. Si el receptor considera necesario la reserva de memoria temporal para llevar a cabo el ensamblado, esta información se debe pasar a una capa superior. De hecho, muchos protocolos de capa superior fijan o negocian un tamaño máximo de PDU, el receptor puede usar esta información para realizar la reserva de memoria. Una secuencia CRC de 32 bits protege

la PDU CPCS entera, mientras que en el caso del AAL de Tipo 3/4 se usa un CRC de 10 bits en cada PDU SAR. El CRC de 32 bits usado en el protocolo AAL Tipo 5 proporciona una fuerte protección contra errores de bits al tiempo que, como se muestra en [WANG92], una detección robusta de celdas desordenadas, fallo que podría darse ante ciertas condiciones de mal funcionamiento de la red.

La carga útil de la capa superior se somete a un relleno de modo que el tamaño total de la PDU CPCS sea múltiplo de 48 octetos. Así, parte de la PDU CPCS se transportará en el campo de carga útil de la PDU SAR, de sólo 48 octetos de longitud. La ausencia de coste suplementario del protocolo tiene varias implicaciones:

- Dado que no existe número de secuencia, el receptor debe suponer que todas las PDU de la capa SAR llegan en el orden adecuado para su ensamblado, utilizándose el campo CRC de la PDU CPCS para verificar este hecho.
- La ausencia del campo MID implica que no es posible la mezcla de celdas correspondientes a diferentes PDU de la subcapa CPCS. Por tanto, cada PDU SAR sucesiva contiene una parte de la PDU CPCS actual o el primer bloque de la PDU CPCS siguiente. Para distinguir entre estos dos casos se usa el bit indicador de tipo de la SDU ATM en el campo de tipo de carga útil de la cabecera de la celda ATM (Figura 11.4).
- Una PDU CPCS consiste en una o más PDU SAR consecutivas con el bit tipo de SDU igual a 0 seguidas inmediatamente por una PDU SAR con el bit mencionado puesto a 1.
- La no existencia del campo LI significa que no hay forma de que la entidad SAR distinga entre octetos correspondientes a una PDU CPCS y bits de relleno en el caso de la última PDU SAR. Así pues, no hay manera de que la entidad SAR encuentre la cola de la PDU CPCS en la última PDU SAR. Para evitar este hecho, se precisa que la carga útil de la PDU CPCS se rellene de forma que el último bit de la cola CPCS coincida con el último bit de la PDU SAR final.

En la Figura 11.16 se muestra un ejemplo de transmisión AAL 5. La PDU CPCS, incluyendo los datos de relleno y la cola, se divide en bloques de 48 octetos, cada uno de los cuales se transmite en una sola celda ATM.

11.7. RETRANSMISIÓN DE TRAMAS

La técnica de retransmisión de tramas («frame relay»), como ATM, se diseñó para proporcionar un esquema de transmisión más eficiente que el de X.25. Tanto las normalizaciones como los productos comerciales relacionados con la retransmisión de tramas aparecieron antes que los correspondientes a ATM, por lo que existe una amplia base de productos de retransmisión de tramas instalados. Es por ello que, a pesar del desplazamiento sufrido por esta técnica como consecuencia del interés actual por las redes de alta velocidad ATM, en esta sección se presenta una revisión de la retransmisión de tramas.

FUNDAMENTOS

La aproximación tradicional de conmutación de paquetes hace uso de X.25, lo que no sólo determina la interfaz usuario-red sino que también afecta al diseño interno de la red. Algunas de las características básicas de X.25 son:

- Los paquetes de control de llamada, usados para el establecimiento y liberación de circuitos virtuales, se transmiten por el mismo canal y circuito virtual que los paquetes de datos, empleándose, en consecuencia, una señalización en banda.
- La multiplexación de circuitos virtuales tiene lugar en la capa 3.
- Tanto la capa 2 como la 3 incluyen mecanismos de control de flujo y de errores.

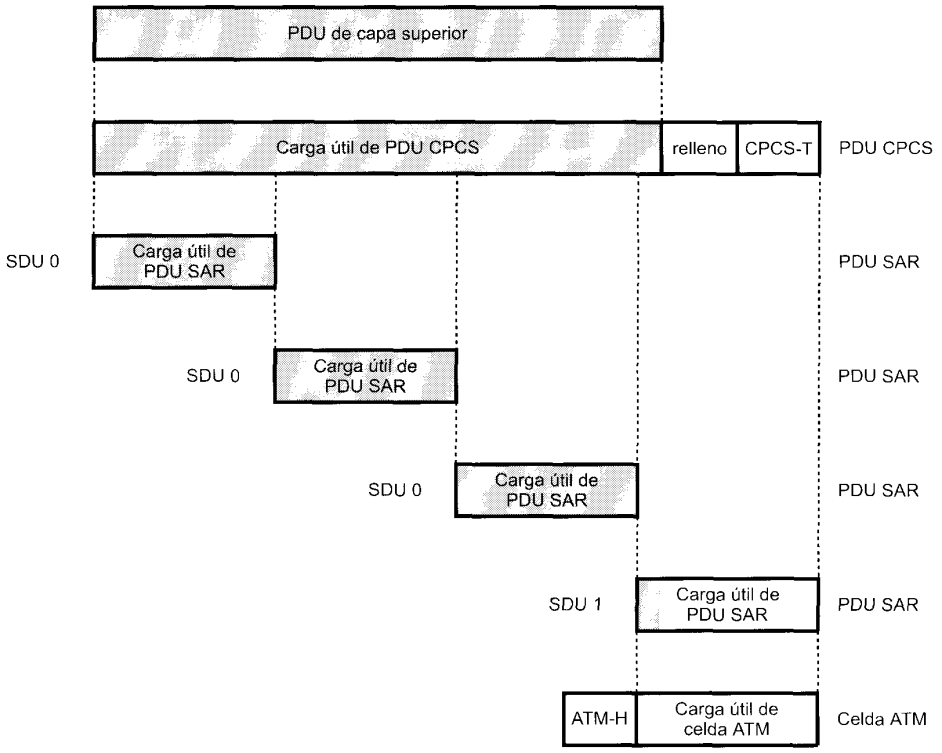


Figura 11.16. Ejemplo de transmisión de AAL 5.

Esta aproximación es muy costosa, ya que en cada salto a través de la red el protocolo de control de enlace intercambia tramas de datos y de confirmación. Además, cada nodo intermedio debe mantener tablas de estado para cada circuito virtual con objeto de abordar aspectos de gestión de llamadas y de control de flujo/errores del protocolo X.25. Este coste queda justificado en caso de que la probabilidad de error en los enlaces de la red sea significativa, por lo que esta técnica puede no ser la más apropiada para los servicios de comunicación digitales modernos dado que las redes actuales hacen uso de tecnologías de transmisión fiables sobre enlaces de transmisión de alta calidad, fibra óptica en muchos de los casos. Adicionalmente a este hecho, con la utilización de fibra óptica y transmisión digital se pueden conseguir velocidades de transmisión de datos elevadas. En este contexto, el coste de X.25 no sólo es innecesario sino que además degrada la utilización efectiva de las altas velocidades de transmisión disponibles.

La retransmisión de tramas se ha diseñado para eliminar gran parte del coste que supone X.25 para el sistema final de usuario y para la red de conmutación de paquetes. Las principales diferencias entre la técnica de retransmisión de tramas y un servicio convencional de conmutación de paquetes X.25 son:

- La señalización de control de llamadas se transmite a través de una conexión lógica distinta de la de los datos de usuario. De este modo, los nodos intermedios no necesitan mantener tablas de estado ni procesar mensajes relacionados con el control de llamadas individuales.

- La multiplexación y conmutación de conexiones lógicas tienen lugar en la capa 2 en lugar de en la capa 3, eliminándose así una capa completa de procesamiento.
- No existe control de flujo ni de errores a nivel de líneas individuales. Si se lleva a cabo este control, será extremo a extremo y responsabilidad de capas superiores.

Así pues, en retransmisión de tramas sólo se envía una trama de datos de usuario desde el origen hasta el destino, devolviéndose al primero una trama de confirmación generada por una capa superior. En este caso no existe intercambio de tramas de datos y confirmaciones en cada uno de los enlaces del camino entre el origen y el destino.

Veamos las ventajas y desventajas de esta técnica. En comparación con X.25, la principal desventaja teórica en retransmisión de tramas es que se pierde la posibilidad de llevar a cabo un control de flujo y de errores en cada enlace (aunque la retransmisión de tramas no ofrece control de flujo y de errores extremo a extremo, éste se puede implementar fácilmente en una capa superior). En X.25 existen varios circuitos virtuales a través de un mismo enlace físico, permitiendo el protocolo LAPB una transmisión fiable a nivel de enlace desde el origen hacia la red de conmutación de paquetes, y desde ésta hacia el destino. El protocolo de control de enlace proporciona además fiabilidad en cada enlace de la red. Con el uso de la técnica de retransmisión de tramas desaparece dicho control a nivel de enlace, aunque este hecho no supone un gran inconveniente gracias al incremento en la fiabilidad en la transmisión y en los servicios de conmutación.

La ventaja de la retransmisión de tramas es la potencia del proceso de comunicaciones, reduciéndose la funcionalidad del protocolo necesaria en la interfaz usuario-red así como el procesamiento interno de red. En consecuencia, cabe esperar un menor retardo y un mayor rendimiento. Así, algunos estudios indican que la mejora en el rendimiento mediante el uso de la técnica de retransmisión de tramas frente a X.25 puede ser de un orden de magnitud o más [HARB92]. La recomendación I.233 de ITU- T especifica que la retransmisión de tramas consigue velocidades de acceso de hasta 2 Mbps.

ARQUITECTURA DE PROTOCOLOS EN RETRANSMISIÓN DE TRAMAS

En la Figura 11.17 se muestra la arquitectura de protocolos para proveer servicios de transporte en modo trama. Se consideran dos planos diferentes de operación: plano de control (C), relacionado con el establecimiento y liberación de conexiones lógicas, y plano de usuario (U), responsable de la transferencia de los datos de usuario entre abonados. Así, los protocolos del plano C se implementan entre el usuario y la red, mientras que los del plano U proveen de funcionalidad extremo a extremo.

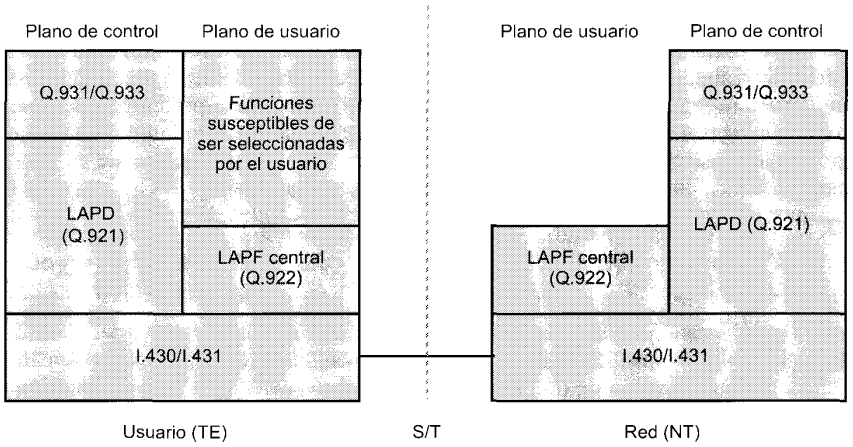


Figura 11.17. Arquitectura de protocolos en la interfaz usuario-red.

Plano de control

El plano de control para servicios en modo trama es similar al de señalización por canal común para servicios de conmutación de circuitos por cuanto que se utiliza un canal lógico diferente para la información de control. En la capa de enlace se utiliza el protocolo LAPD (Q.921) para proporcionar un servicio de control de enlace de datos fiable, con control de errores y de flujo, entre el usuario (TE) y la red (NT) sobre el canal D. Este servicio de enlace de datos se usa para el intercambio de mensajes de señalización de control Q.933.

Plano de usuario

LAPF (Procedimiento de Acceso al Enlace para Servicios en Modo Trama) es el protocolo del plano de usuario para la transferencia real de información entre usuarios finales. Este protocolo está definido en Q.922, que es una versión mejorada de LAPD (Q.921). En retransmisión de tramas sólo se usan las funciones centrales de LAPF:

- Delimitación de tramas, alineamiento y transparencia.
- Multiplexación/demultiplexación de tramas utilizando el campo de dirección.
- Inspección de la trama, para asegurarnos que ésta consta de un número entero de octetos, antes de llevar a cabo la inserción de bits cero o tras una extracción de bits cero.
- Inspección de la trama para asegurarnos que no es demasiado larga ni demasiado corta.
- Detección de errores de transmisión.
- Funciones de control de congestión.

La última función es nueva en LAPF, mientras que el resto son también funciones de LAPD. Las funciones centrales de LAPF en el plano de usuario constituyen una subcapa de la capa de enlace de datos. Esto proporciona el servicio de transferencia de tramas de enlace de datos entre abonados sin control de flujo ni de errores. Además de este hecho, el usuario puede seleccionar funciones extremo a extremo adicionales de la capa de enlace o de la de red, las cuales no forman parte del servicio de retransmisión de tramas. De acuerdo con las funciones básicas, una red ofrece retransmisión de tramas como un servicio orientado a conexión de la capa de enlace con las siguientes propiedades:

- Se preserva el orden de la transferencia de tramas entre el origen y el destino.
- Existe una probabilidad pequeña de pérdida de tramas.

TRANSFERENCIA DE DATOS DE USUARIO

El funcionamiento de la técnica de retransmisión de tramas por lo que respecta a la transferencia de datos de usuario se explica mejor considerando el formato de trama, mostrado en la Figura 11.18a. Éste es el formato definido para el protocolo LAPF de funcionamiento mínimo (conocido como protocolo central LAPF), el cual es similar al de LAPD y LAPB con una salvedad: no existe campo de control, lo que tiene las siguientes implicaciones:

- Existe un único tipo de trama usada para el transporte de datos de usuario y no existen tramas de control.
- No es posible el uso de señalización en banda; una conexión lógica sólo puede transmitir datos de usuario.
- No es posible llevar a cabo control de flujo ni de errores dado que no existen números de secuencia.

Los campos indicador y secuencia de comprobación de trama (FCS) actúan como en LAPD y LAPB. El campo de información contiene datos de capas superiores, de modo que si el usuario decide implementar funciones adicionales de control de enlace de datos extremo a extremo se puede incluir una trama de datos en este campo. En particular, una opción usual es el empleo del protocolo LAPF comple-

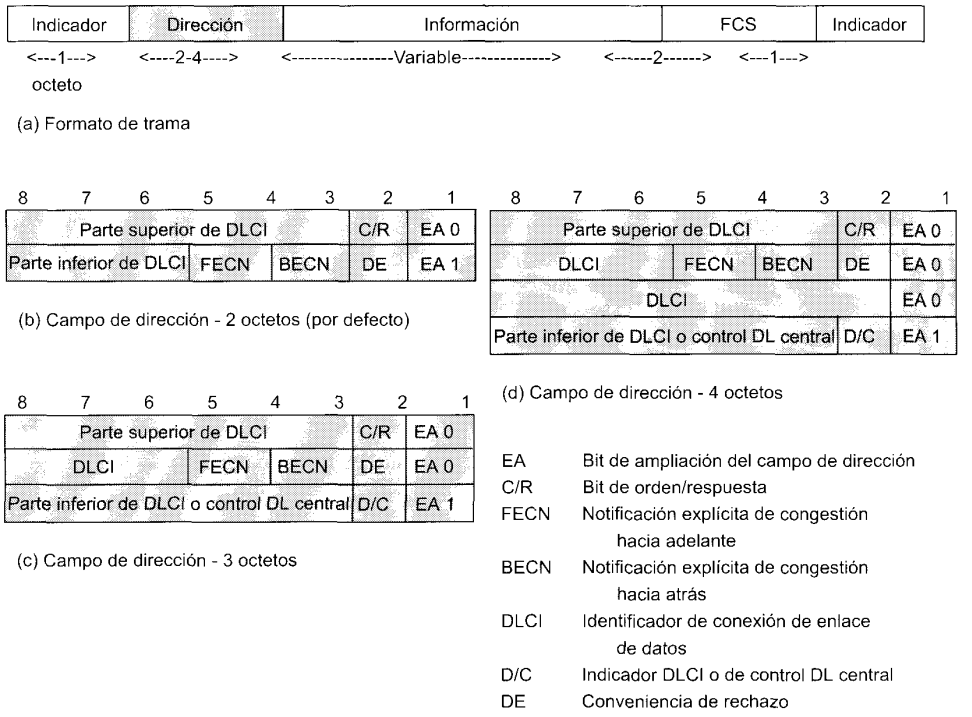


Figura 11.18. Formatos del protocolo central LAPF.

to (conocido como protocolo de control LAPF) para llevar a cabo funciones por encima de las funciones centrales de LAPF. Obsérvese que el protocolo así implementado es estrictamente entre los abonados finales y es transparente a la red de retransmisión de tramas.

El campo de dirección tiene una longitud por defecto de 2 octetos, y se puede ampliar hasta 3 o 4 octetos. Este campo contiene un identificador de conexión de enlace de datos (DLCI) de 10, 17 o 24 bits. El DLCI realiza la misma función que el número de circuito virtual en X.25: permite la multiplexación de varias conexiones lógicas de retransmisión de tramas a través de un único canal. Como en X.25, el identificador de conexión tiene sólo significado local: cada extremo de la conexión lógica asigna su propio DLCI de acuerdo con los números libres, debiendo realizar la red la conversión correspondiente entre ellos. Alternativamente, el uso del mismo DLCI por parte de ambos extremos requeriría algún tipo de gestión global de los valores de DLCI.

La longitud del campo de dirección, y por tanto del DLCI, se determina mediante los bits de ampliación del campo de dirección (EA). El bit C/R es específico de la aplicación y no se usa en el protocolo de retransmisión de tramas estándar. Los bits restantes del campo de dirección están relacionados con el control de congestión y se discutirán en el Capítulo 12.

11.8. LECTURAS Y SITIOS WEB RECOMENDADOS

[GORA95], [MCDY99], [HAND94] y [PRYC96] presentan un estudio en profundidad de ATM. La aproximación de camino virtual/canal virtual en ATM se examina en [SATO90], [SATO91] y [BURG91], mientras que en [ARMI93] y [SUZU94] se discute AAL y se comparan los Tipos 3/4 y 5.

[BLAC98] ofrece una buena revisión de la técnica de retransmisión de tramas, con especial énfasis en los aspectos técnicos y de protocolo. Otro tratamiento técnico adecuado se presenta en [SPOH97]. [DORL96] proporciona también una extensa descripción, incluyendo un buen tratamiento técnico así como consideraciones acerca de productos e implementación, de la retransmisión de tramas.

ARMI93 Armitage, G., y Adams, K. «Packet Reassembly During Cell Loss.» *IEEE Network*, September 1993.

BLAC98 Black, U. *Frame Relay Networks: Specifications and Implementations.* New York: McGraw-Hill, 1998.

BURG91 Burg, J., y Dorman, D. «Broadband ISDN Resource Management: The Role of Virtual Paths.» *IEEE Communications Magazine*, September 1991.

DORL96 Dorling, B.; Pieters, P.; y Valenzuela, E. *IBM Frame Relay Guide.* IBM Publication SG24-4463-01, 1996. Available at www.redbooks.ibm.com.

GORA95 Goralski, W. *Introduction to ATM Networking.* New York: McGraw-Hill, 1995.

HAND94 Handel, R.; Huber, N.; y Schroder, S. *ATM Networks: Concepts, Protocols, Applications.* Reading, MA: Addison-Wesley, 1994.

MCDY99 McDysan, D., y Spohn, D. *ATM: Theory and Applications.* New York: McGraw-Hill, 1999.

PRYC96 Prycker, M. *Asynchronous Transfer Mode: Solutions for Broadband ISDN.* New York: Ellis Horwood, 1996.

SATO90 Sato, K.; Ohta, S.; y Tokizawa, I. «Broad-band ATM Network Architecture Based on Virtual Paths.» *IEEE Transactions on Communications*, August 1990.

SATO91 Sato, K.; Ueda, H.; y Yoshikai, M. «The Role of Virtual Path Crossconnection.» *IEEE LTS*, August 1991.

SPOH97 Spohn, D. *Data Network Design.* New York: McGraw-Hill, 1997.

SUZU94 Suzuki, T. «ATM Adaptation Layer Protocol.» *IEEE Communications Magazine*, April 1994.

SITIOS WEB RECOMENDADOS

- **Web del Foro ATM:** contiene especificaciones técnicas, documentos oficiales y copias actualizadas de la publicación 53 *Bytes* del Foro.
- **Refugio de la retransmisión de celdas:** contiene archivos de listas de correo de la retransmisión de celdas y enlaces a numerosos documentos y sitios Web relacionados con ATM.
- **Foro de Retransmisión de Tramas:** asociación compuesta por vendedores, proveedores, usuarios y consultores cuyo objetivo común es la implementación de la técnica de retransmisión de tramas de acuerdo con los estándares nacionales e internacionales. Este sitio Web incluye una lista de documentos técnicos y de implementación en venta.
- **Recursos de retransmisión de tramas:** conjunto de punteros a información sobre la retransmisión de tramas en la Web.

11.9. PROBLEMAS

11.1. Liste los 16 posibles valores del campo GFC y la interpretación de cada uno de ellos (algunos valores no son válidos).

11.2. Una decisión de diseño importante en ATM es el uso de celdas de tamaño fijo o variable. Consideremos esta decisión desde el punto de vista de la eficiencia. La eficiencia de la transmisión se puede definir como:

$$N = \frac{\text{Número de octetos de información}}{\text{Número de octetos de información + número de octetos suplementarios}}$$

a) En el caso de paquetes de longitud fija, la información suplementaria consiste en los octetos de cabecera. Definamos:

L = tamaño del campo de datos de la celda en octetos
H = tamaño de la cabecera de la celda en octetos
X = número de octetos de información a transmitir como un único mensaje

Derive una expresión para N. *Sugerencia:* la expresión requiere el uso del operador $[\bullet]$, donde $[Y]$ = menor entero mayor o igual que Y.

b) Si las celdas son de longitud variable, los octetos suplementarios se determinan como la cabecera más los indicadores para delimitar las celdas o un campo de longitud adicional en la cabecera. Sea Hv los octetos suplementarios adicionales necesarios para posibilitar el uso de celdas de longitud variable. Obtenga una expresión para N en términos de X, H y Hv.

c) Sea $L = 48$, $H = 5$ y $Hv = 2$. Dibuje N en función del tamaño del mensaje para celdas de tamaño fijo y variable. Comente los resultados.

11.3. Otra decisión de diseño importante en ATM es el tamaño del campo de datos para celdas de longitud fija. Consideremos esta decisión desde el punto de vista de la eficiencia y del retardo.

a) Suponga que tiene lugar una transmisión larga, de forma que todas las celdas están completamente llenas. Obtenga una expresión para la eficiencia N en función de H y L.

b) El retardo de empaquetamiento es el retardo introducido en la transmisión de una secuencia ante la necesidad de almacenar temporalmente los bits hasta que se haya completado un paquete para su transmisión. Obtenga una expresión para este retardo en función de L y de la velocidad R de la fuente.

c) Velocidades de transmisión usuales para codificación de voz son 32 kbps y 64 kbps. Represente el retardo de empaquetamiento en función de L para estas dos velocidades; use un eje de ordenadas con valor máximo de 2 ms. Dibuje en la misma gráfica la eficiencia de la transmisión en función de L; use un eje de abscisas con un valor máximo del 100%. Comente los resultados.

11.4. Suponga que se usa AAL 3/4 y que el receptor se encuentra en un estado desocupado (no se reciben celdas). A continuación se transmite un bloque de datos de usuario como una secuencia de PDU SAR.

a) Suponiendo que la PDU SAR BOM se pierde, ¿qué sucede en el receptor?

b) ¿Qué ocurrirá en el extremo receptor si se pierde una de las PDU SAR COM?

c) Supongamos que se pierden 16 PDU SAR COM consecutivas. ¿Qué sucede en el receptor?

d) ¿Qué ocurrirá en el extremo receptor si se perdiese de forma consecutiva un número múltiplo de 16 PDU SAR COM?

11.5. Haciendo uso de nuevo de AAL 3/4, suponga que el receptor se encuentra en un estado desocupado y que se transmiten dos bloques de datos usuario como dos secuencias diferentes de PDU SAR.

a) Suponga que se pierde la PDU SAR EOM de la primera secuencia. ¿Qué ocurrirá en el extremo receptor?

b) Supóngase ahora que se pierden la PDU SAR EOM de la primera secuencia y la PDU SAR BOM de la segunda. ¿Qué sucederá en el receptor?

11.6. Supongamos que se utiliza AAL 5 y que el extremo receptor se encuentra en un estado desocupado (no se reciben celdas). Transmitido un bloque de datos de usuario como una secuencia de PDU SAR:

a) ¿Qué ocurriría en el extremo receptor si se produjese un error simple en una de las PDU SAR?

b) Suponga ahora que se pierde una de las celdas con el bit de tipo de SDU igual a 0. ¿Qué sucederá en el receptor?

c) ¿Qué ocurrirá en el extremo receptor si se supone que se pierde una de las celdas con el bit de tipo de SDU igual a 1?

11.7. El documento Q.933 recomienda un procedimiento para llevar a cabo la negociación de la ventana de control de flujo mediante ventana deslizante, la cual puede tomar valores entre 1 y 127. Este proceso de negociación hace uso de la variable k, calculada mediante una expresión a partir de los siguientes parámetros:

L_{td} = tamaño de la trama de datos en octetos
R_u = rendimiento en bits/s
T_{td} = retardo de transmisión extremo a extremo en segundos
k = tamaño de la ventana (número máximo de tramas I salientes)

El procedimiento es como sigue:

> El tamaño de ventana se debe negociar como sigue. El usuario origen calcula k haciendo uso de la expresión mencionada sustituyendo el retardo máximo de transmisión extremo a extremo y el tamaño máximo de trama de salida por T_{td} y L_d, respectivamente. El mensaje SETUP incluirá los parámetros del protocolo de la capa de enlace, los parámetros básicos de la capa de enlace y la información acerca del retardo de transmisión extremo a extremo. El usuario destino debe calcular su propio parámetro k haciendo uso de la expresión anterior sustituyendo el retardo de transmisión extremo a extremo acumulado y su propio tamaño máximo de trama de salida por T_{td} y L_d, respectivamente. El mensaje CONNECT incluirá los parámetros básicos de la capa de enlace y la información acerca del retardo de transmisión extremo a extremo, de modo que el usuario origen puede modificar su parámetro k de acuerdo con esta información. El usuario origen debe calcular k haciendo uso de la expresión anterior sustituyendo el retardo de transmisión extremo a extremo acumulado y el tamaño máximo de trama de entrada por T_{td} y L_d, respectivamente.

SETUP y CONNECT son mensajes intercambiados sobre un canal de control durante el establecimiento de una conexión de retransmisión de tramas. Sugiera una expresión para calcular k a partir de las otras variables y justifíquela.

CAPÍTULO 12

Congestión en redes de datos

- El problema de la congestión se produce cuando el número de paquetes que se transmite a través de una red comienza a aproximarse al límite de su capacidad de gestión de paquetes. El objetivo del control de congestión es mantener el número de paquetes en la red por debajo del nivel para el que decaen dramáticamente las prestaciones.
- La ausencia de mecanismos de control de flujo en los protocolos ATM y de retransmisión de tramas dificulta el control de congestión. Se han desarrollado diversas técnicas para hacer frente a la congestión y garantizar distintas calidades de servicio para diferentes tipos de tráfico.
- En las redes ATM se lleva a cabo un acuerdo de tráfico con cada usuario que especifica las características del tráfico esperado y del tipo de servicio a proveer por la red. La red implementa técnicas de control de congestión para proteger a ésta de la congestión al tiempo que se cumplen los acuerdos de tráficos establecidos.
- Una red ATM supervisa el flujo de celdas procedente de cada fuente y puede rechazar o marcar para su rechazo potencial aquellas celdas que excedan los acuerdos de tráficos establecidos. Además, la red puede adaptar el tráfico procedente de los usuarios y suavizar los flujos de tráfico de salida mediante el almacenamiento temporal de las celdas.

El control de congestión es un aspecto de diseño de consideración necesaria en las redes de datos, tales como las de conmutación de paquetes, las de retransmisión de tramas y las redes ATM, y en la interconexión de redes (Internet). El control de la congestión, como en sí el fenómeno de la congestión, es un problema complejo. En términos muy generales, la congestión ocurre cuando el número de paquetes[1] que se transmite sobre una red comienza a aproximarse al límite de la capacidad de gestión de paquetes de la misma. El objetivo del control de congestión es mantener el número de paquetes en la red por debajo del nivel para el que decaen dramáticamente las prestaciones.

Para comprender los elementos involucrados en el control de la congestión hemos de fijarnos en algunos resultados de la teoría de colas. Una red de datos o una internet es esencialmente una red de colas, de modo que en cada nodo (un conmutador en una red de datos, un dispositivo de encaminamiento en una internet) existe una cola de paquetes asociada a cada canal de salida. Si la velocidad a la que se reciben y ponen en cola los paquetes supera la velocidad a la que éstos se pueden transmitir, el tamaño de la cola crece sin límite y el retardo sufrido por los paquetes tiende a infinito. Incluso si la velocidad de llegada de los paquetes es menor que la de transmisión de éstos, el tamaño de la cola crecerá drásticamente conforme la primera se aproxime a la segunda. Como regla empírica, cuando el porcentaje de utilización de la línea en la que se ponen en cola los paquetes supera el 80 %, el tamaño de la cola crece de forma alarmante. Este crecimiento del tamaño de la cola implica el aumento del retardo sufrido por un paquete en cada nodo. Así pues, dado que el tamaño de una cola cualquiera es finito, cuando éste crece se produce el desbordamiento de la cola.

12.1. EFECTOS DE LA CONGESTIÓN

Considérese la situación de las colas en un nodo de conmutación de paquetes o en un dispositivo de encaminamiento tal como se muestra en la Figura 12.1. Todos los nodos tienen un número de puertos de

[1] En este capítulo se usa el término *paquete* en un sentido muy amplio para hacer referencia a paquetes en una red de conmutación de paquetes, a tramas en una red de retransmisión de tramas, a celdas en una red ATM y a datagramas IP en una internet.

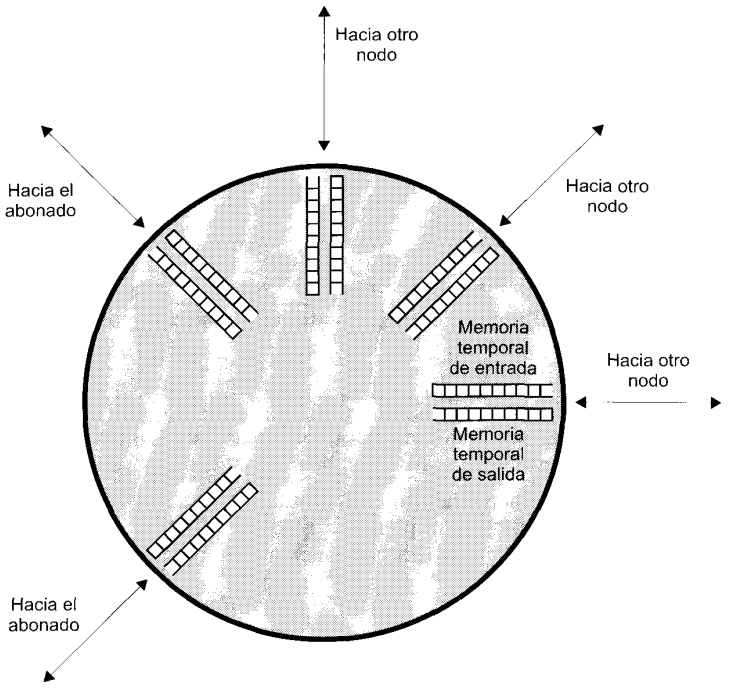


Figura 12.1. Colas de entrada y de salida de un nodo.

entrada/salida[2] conectados: uno o más hacia otros nodos y cero o más hacia sistemas finales. Los paquetes se reciben y transmiten por cada puerto. Consideremos la existencia de dos memorias temporales para cada puerto, una para aceptar los paquetes de llegada y otra para gestionar los paquetes a transmitir. En la práctica podrían existir dos memorias temporales de tamaño fijo asociadas a cada uno de los puertos, o bien una única memoria para todas las actividades de almacenamiento. El último caso es equivalente a pensar que cada puerto dispone de dos memorias temporales de tamaño variable con la restricción de que la suma de todas ellas es constante.

En cualquier caso, a medida que se reciben los paquetes, se almacenan en la memoria temporal de entrada del puerto correspondiente. El nodo examina cada paquete de entrada para tomar una decisión de encaminamiento y lo coloca en la memoria temporal de salida pertinente. Los paquetes en cola se transmiten tan rápido como es posible, lo que corresponde a multiplexación por división en el tiempo estadística. Si los paquetes se reciben en el nodo demasiado deprisa para ser procesados (toma de decisión de encaminamiento), o más rápido que el borrado de los paquetes en la memoria temporal de salida, no existirá eventualmente memoria temporal disponible para los paquetes recibidos.

Cuando se alcanza este punto de saturación, se pueden adoptar dos estrategias. La primera consiste simplemente en descartar cualquier paquete de entrada para el que no exista memoria disponible. La alternativa es que el nodo que sufra este problema implemente algún tipo de control de flujo sobre sus vecinos de forma que el tráfico sea manejable. El problema es que, como se ilustra en la Figura 12.2, cada uno de los nodos vecinos gestiona también varias colas. Así, si el nodo 6 frena el flujo de paquetes

[2] En el caso de un nodo de conmutación en una red de conmutación de paquetes, de retransmisión de tramas o ATM, cada puerto de entrada/salida conecta con una línea de transmisión a otro nodo o sistema final. En el caso de un dispositivo de encaminamiento en una red internet, cada puerto de entrada/salida conecta con un enlace directo a otro nodo o con una subred.

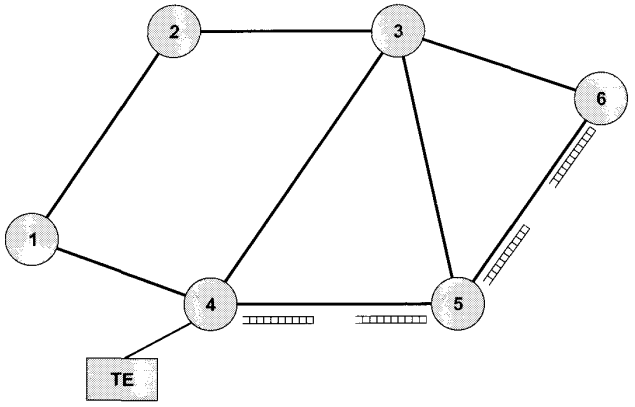


Figura 12.2. Interacción de las colas en una red de datos.

del nodo 5, se llenará la memoria temporal de salida del nodo 5 asociada al puerto hacia 6. De esta manera, la congestión sufrida en un punto de la red se propagará rápidamente a otra zona o incluso a toda la red. El control de flujo es una herramienta muy potente, debiendo utilizarse para gestionar el tráfico de toda la red.

FUNCIONAMIENTO IDEAL

En la Figura 12.3 se muestra el comportamiento ideal de la utilización de una red. La gráfica superior representa el rendimiento de la red (número de paquetes enviados a sistemas finales destino) en función de la carga ofrecida (número de paquetes transmitidos por sistemas finales origen), ambos parámetros normalizados al rendimiento máximo teórico de la red. Por ejemplo, si una red consta de un único nodo con dos líneas *full-duplex* a 1 Mbps, la capacidad teórica de la red será 2 Mbps, correspondiendo a un flujo de 1 Mbps en cada sentido. En el caso ideal, el rendimiento de la red crece hasta aceptar una cantidad de carga igual a la capacidad total de la red, permaneciendo el rendimiento normalizado a valor 1,0 para cargas de entrada superiores. Obsérvese sin embargo lo que sucede con el retardo extremo a extremo medio experimentado por un paquete incluso bajo esta suposición de funcionamiento ideal. Cuando la carga es baja, existe un retardo pequeño constante consistente en el retardo de propagación a través de la red desde el origen hasta el destino más un retardo de procesamiento en cada nodo. A medida que la carga de la red aumenta, al valor de retardo fijo anterior se suman los retardos de las colas en cada nodo. Finalmente, cuando la carga excede la capacidad de la red el retardo aumenta sin límite.

Existe una sencilla explicación intuitiva sobre por qué el retardo tiende a infinito. Supongamos que cada nodo de la red dispone de memorias temporales de tamaño infinito y que la carga de entrada supera la capacidad de la red. Bajo condiciones ideales, la red continuará presentando un rendimiento normalizado de 1,0, por lo que la velocidad de salida de paquetes de la red será 1,0. Dado que la velocidad de entrada de paquetes a la red es mayor que 1,0, el tamaño de las colas internas crece. En el estado estacionario, en el que la entrada es superior a la salida, estos tamaños de cola crecen sin límite y, en consecuencia, los retardos de cola también crecerán de forma ilimitada.

Es importante comprender el significado de la Figura 12.3 antes de pasar a estudiar las condiciones de funcionamiento real. La figura representa el objetivo ideal, inasequible, de todos los esquemas de control de tráfico y de congestión. En ningún esquema se pueden exceder las prestaciones dibujadas en la Figura 12.3.

Veremos que el término *potencia* se emplea a veces en la bibliografía existente acerca de las prestaciones de las redes. Este parámetro se define como la relación entre el rendimiento y el retardo, repre-

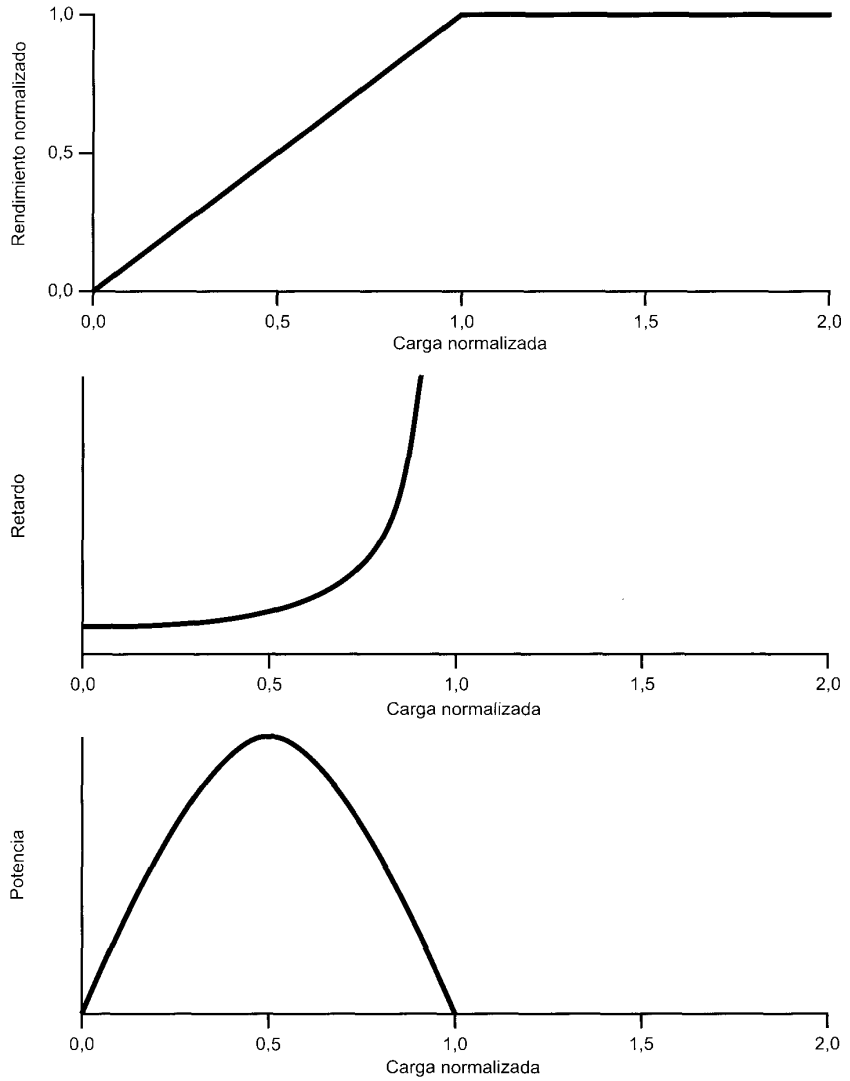


Figura 12.3. *Utilización ideal de una red.*

sentándose en la gráfica inferior de la Figura 12.3 para el caso ideal. Ya se ha visto que, generalmente, los esquemas de control de configuración y de congestión de red que mejoran el rendimiento presentan también un mayor retardo [JAIN91], y que la potencia es una métrica concisa que puede ser usada para comparar diferentes esquemas.

FUNCIONAMIENTO REAL

En el caso ideal ilustrado en la Figura 12.3 se ha supuesto que las memorias temporales son infinitas y que no existe coste asociado a la transmisión de los paquetes ni al control de congestión. En la práctica,

las memorias son finitas, lo que provoca rebosamientos, y el control de congestión consume capacidad de la red debido al intercambio de señales de control.

Considérese lo que sucede en una red con memorias temporales finitas si no se lleva a cabo el control de congestión ni se controla la entrada procedente de los sistemas finales. Aunque es claro que los detalles diferirán según la configuración de la red y las estadísticas de tráfico, obsérvese el descorazonador resultado mostrado en términos generales en la Figura 12.4.

Para alta carga, el rendimiento, y por tanto la utilización de la red, aumenta conforme lo hace la carga. A medida que ésta continúa creciendo, llega un momento (punto A en la gráfica) a partir del cual

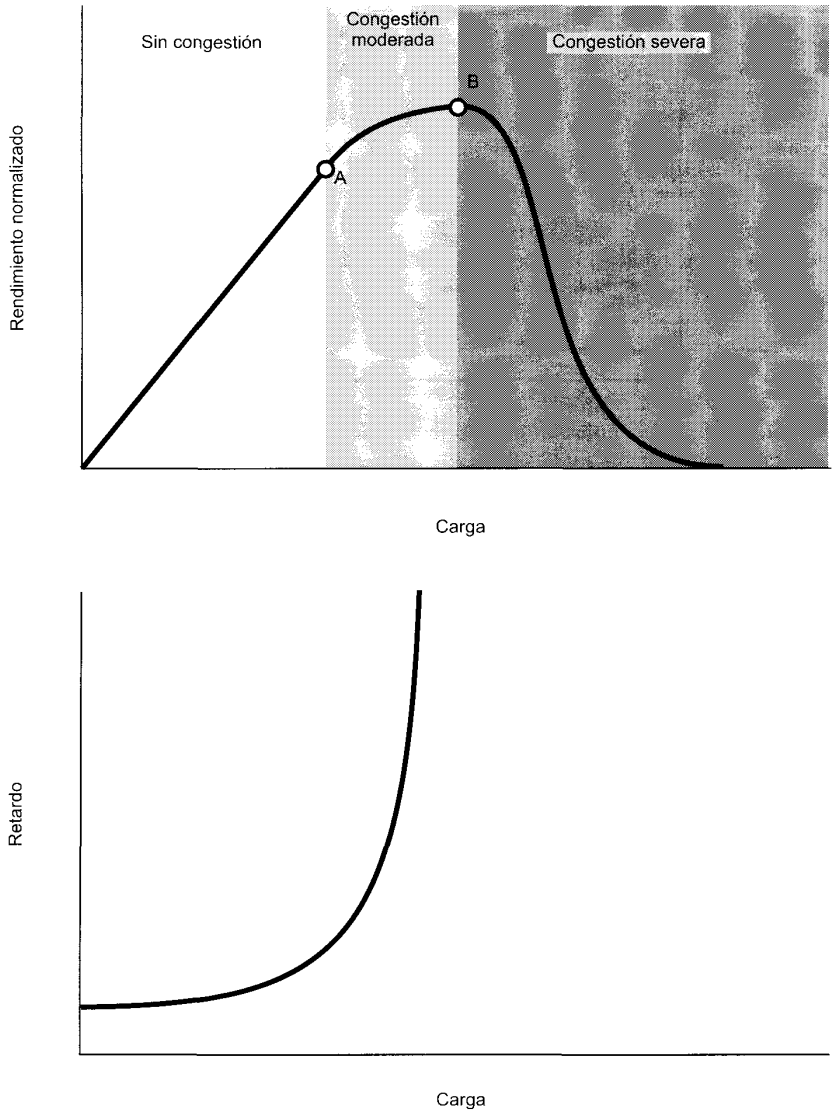


Figura 12.4. Efectos de la congestión.

el rendimiento de la red crece a una velocidad menor a la que lo hace la carga. Este hecho se debe a que la red entra en un estado de congestión moderada, en la que la red sigue dando curso al tráfico aunque con un incremento en el retardo. El alejamiento del rendimiento de su comportamiento ideal está motivado por varios factores. Por una parte, es improbable la distribución uniforme de la carga a través de la red, de modo que algunos nodos sufrirán una congestión moderada mientras que otros experimentarán una congestión severa y precisarán descartar algún tráfico. Adicionalmente, la red tratará de equilibrar la carga conforme ésta aumenta mediante el encaminamiento de paquetes a través de zonas menos congestionadas. Por lo que se refiere a la función de encaminamiento de la red, los nodos deben intercambiar entre sí un mayor número de paquetes para avisarse acerca de las zonas congestionadas; este coste reduce la capacidad disponible para los paquetes de datos.

A medida que la carga de la red continúa aumentando, el tamaño de las colas de los distintos nodos sigue creciendo. Eventualmente, llega un momento (punto B en la gráfica) a partir del cual el rendimiento real decae al aumentar la carga de entrada. La razón para ello es que las memorias temporales existentes en cada nodo son de tamaño finito. Cuando las memorias en un nodo dado se llenan, éste debe descartar paquetes. Por tanto, los sistemas origen deben retransmitir los paquetes rechazados además de otros nuevos. Esto sólo consigue empeorar la situación: conforme se retransmiten más y más paquetes, la carga del sistema aumenta y se saturarán más memorias temporales. Mientras el sistema trata desesperadamente de eliminar el exceso de paquetes, los usuarios continúan enviando paquetes, nuevos y anteriores, al sistema. Incluso puede que tengan que retransmitirse aquellos paquetes enviados con éxito debido a que una capa superior (por ejemplo, la de transporte) tarda mucho tiempo en confirmarlos: el emisor supone que el paquete no se recibió en el receptor y lo retransmite. En estas circunstancias la capacidad efectiva del sistema es prácticamente cero.

12.2. CONTROL DE CONGESTIÓN

En este libro se presentan distintas técnicas de control de congestión usadas en redes de conmutación de paquetes, de retransmisión de tramas y ATM y en interconexiones de redes basadas en IP. Para situar en un contexto este estudio, la Figura 12.5 muestra un esquema general de las principales técnicas de control de congestión.

CONTRAPRESIÓN

Ya se ha hecho referencia a la contrapresión como técnica de control de congestión. Esta técnica produce un efecto similar a la contrapresión en fluidos que caen por un tubo. Cuando el extremo del tubo está

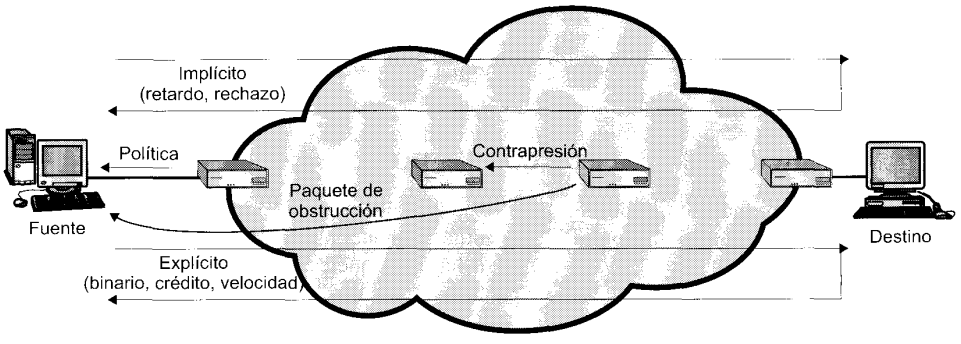


Figura 12.5. Mecanismos de control de congestión.

cerrado (u obstruido) el fluido realiza una presión hacia atrás en el tubo hasta el punto origen, donde el flujo es nulo (o menor).

La contrapresión se puede realizar a nivel de enlaces o de conexiones lógicas (por ejemplo, circuitos virtuales). Volviendo de nuevo a la Figura 12.2, si el nodo 6 sufre congestión (se llenan las memorias temporales asociadas), éste puede frenar parcial o totalmente el flujo de paquetes desde el nodo 5 (o del nodo 3, o de los dos). Si persiste esta restricción, el nodo 5 necesitará frenar también parcial o totalmente el tráfico sobre sus líneas de entrada. Esta restricción sobre el flujo se propagará hacia atrás (en sentido contrario al flujo del tráfico de datos) hacia los sistemas emisores, cuya transmisión de nuevos paquetes hacia la red quedará limitada.

La contrapresión se puede aplicar de forma selectiva a las conexiones lógicas, de manera que el flujo desde un nodo al siguiente sólo se reduzca o se pare para algunas conexiones, generalmente para aquéllas con mayor tráfico. En este caso, la restricción se propagará hacia atrás hacia los emisores a lo largo de las conexiones en cuestión.

La contrapresión resulta de una utilidad limitada, pudiéndose utilizar en redes orientadas a conexión que permiten control de flujo a nivel de enlace (de un nodo al siguiente). Las redes de conmutación de paquetes X.25 presentan generalmente esta característica, pero no así las redes de retransmisión de tramas ni las redes ATM. Aunque, como se presentará en la Parte V del libro, recientemente se han desarrollado algunos esquemas basados en flujo, las redes internet IP han sido tradicionalmente construidas de forma que no implementan ningún mecanismo para la regulación del flujo de datos entre dos dispositivos de encaminamiento a lo largo de una ruta a través de la red.

PAQUETES DE OBSTRUCCIÓN

Un paquete de obstrucción es un paquete de control generado por un nodo congestionado y transmitido hacia atrás, hacia un nodo origen a fin de reducir el flujo de tráfico. Un ejemplo de paquete de obstrucción es el paquete Ralentización del Emisor («Source Quench») usado en ICMP («Internet Control Message Protocol»). Tanto un dispositivo de encaminamiento como un sistema final destino pueden llevar a cabo el envío de este mensaje hacia un sistema final fuente solicitando la reducción de la velocidad a la que éste emite tráfico hacia la internet de destino. Cuando se recibe un mensaje de ralentización del origen, el sistema emisor frena la velocidad a la que envía tráfico hacia el destino correspondiente hasta que no reciba más mensajes de ralentización del emisor. Este mensaje se puede usar por parte de un dispositivo de encaminamiento o de un sistema final que debe descartar datagramas IP debido al llenado de una memoria temporal, en cuyo caso el dispositivo de encaminamiento o sistema final generará un mensaje de ralentización del emisor para cada uno de los datagramas que rechaza. Adicionalmente, un sistema se puede anticipar a la ocurrencia de congestión mediante la generación de mensajes de ralentización del emisor cuando la ocupación de sus memorias temporales se aproxime a su capacidad. En este caso, se puede llevar a cabo sin problema la transmisión del datagrama a que hace referencia el mensaje de ralentización del origen. Por tanto, la recepción de este mensaje no implica el envío o no del datagrama correspondiente.

El uso de paquetes de obstrucción es una técnica relativamente burda de controlar la congestión, presentándose más adelante algunos métodos más sofisticados de señalización explícita de congestión.

SEÑALIZACIÓN IMPLÍCITA DE CONGESTIÓN

Cuando se produce congestión en la red pueden suceder dos cosas: (1) el retardo de transmisión de un paquete dado desde un emisor hasta un destino aumenta hasta ser apreciablemente mayor que el término de retardo de propagación fijo, y (2) se rechazan paquetes. Si un emisor es capaz de detectar el incremento en los retardos y el rechazo de paquetes, tiene una evidencia implícita de la congestión de la red. Si todos los emisores pueden detectar la ocurrencia de congestión y, en respuesta a ella, reducir el flujo, dicha congestión se podrá aliviar. Así pues, el control de congestión en base a la señalización implícita es responsabilidad de los sistemas finales y no precisa acción alguna por parte de los nodos de la red.

La señalización implícita es una técnica de control de congestión efectiva para configuraciones no orientadas a conexión, o datagrama, tales como redes de conmutación de paquetes mediante datagramas y redes internet IP. En estos casos, aunque no existen conexiones lógicas a través de la internet sobre las que se puedan regular el tráfico, se pueden establecer conexiones lógicas entre dos sistemas finales a nivel TCP. TCP incluye mecanismos para confirmar la recepción de segmentos TCP y regular el flujo de datos entre el origen y el destino de una conexión TCP. En el Capítulo 17 se estudiarán las técnicas de control de congestión en TCP basadas en la capacidad de detectar el incremento en el retardo y en la pérdida de segmentos.

La señalización implícita se puede usar también en redes orientadas a conexión. Por ejemplo, en redes de retransmisión de tramas, el protocolo de control LAPF, que es extremo a extremo, incluye facilidades similares a las de TCP para el control de flujo y de errores. El control de LAPF es capaz de detectar tramas perdidas y adaptar el flujo de datos en consecuencia.

SEÑALIZACIÓN EXPLÍCITA DE CONGESTIÓN

Resulta deseable hacer tanto uso como sea posible de la capacidad disponible de una red, pero aún más lo es reaccionar de forma controlada y adecuada ante la congestión. Este es el objetivo de las técnicas de prevención explícita de congestión. En términos generales, para evitar explícitamente la congestión, la red alerta a los sistemas finales acerca del incremento de la congestión en la red, y éstos toman las medidas oportunas para reducir la carga de entrada a la red.

Generalmente, las técnicas explícitas de control de congestión operan sobre redes orientadas a conexión y controlan el flujo de paquetes de conexiones individuales. Las aproximaciones de señalización explícita de congestión pueden trabajar en uno de los dos siguientes sentidos:

- **Hacia atrás:** se notifica al origen que los procedimientos de prevención de congestión deberían ser iniciados allá donde son aplicables para el tráfico en el sentido opuesto al que se recibe la notificación. Se indica así que los paquetes transmitidos por el usuario sobre esta conexión lógica pueden encontrar recursos congestionados. La información hacia atrás se transmite alterando bits en la cabecera de un paquete de datos encabezado por la dirección del emisor a controlar o transmitiendo hacia el origen paquetes de control diferentes de los de datos.
- **Hacia adelante:** se notifica al usuario que los procedimientos de prevención de congestión deberían ser puestos en marcha allá donde son aplicables para el tráfico en el mismo sentido en que se recibe la notificación. Se indica que un paquete dado, sobre una conexión lógica dada, ha encontrado recursos congestionados. De nuevo, esta información se puede transmitir como bits alterados en paquetes de datos o mediante paquetes de control separados. En algunos esquemas, cuando se recibe la señal de notificación hacia adelante en un sistema final, éste devuelve un eco de ella sobre la conexión lógica hacia el emisor. Por su parte, en otros esquemas, se espera que el sistema final realice un control de flujo sobre el sistema final origen en una capa superior (por ejemplo, TCP).

Las técnicas de señalización explícita de congestión se pueden dividir en tres categorías generales:

- **Binarias:** se activa un bit en un paquete de datos transmitido por un nodo congestionado, de modo que un emisor puede reducir su flujo de tráfico cuando recibe una indicación binaria de congestión sobre una conexión lógica.
- **Basadas en crédito:** estos esquemas proporcionan de forma explícita un crédito a un emisor sobre una conexión lógica. Este crédito indica cuántos octetos o cuántos paquetes puede transmitir el emisor, de manera que cuando el crédito se agota el emisor debe esperar la concesión de crédito adicional antes de llevar a cabo el envío de más datos. Los esquemas basados en crédito son usuales para el control de flujo extremo a extremo, en el que un sistema destino hace uso de crédito para evitar que el emisor provoque el desbordamiento de las memorias temporales de recepción, así como para llevar a cabo el control de congestión.

- **Basadas en velocidad:** estos esquemas proporcionan un límite explícito de velocidad para el emisor sobre una conexión lógica, de forma que el origen sólo puede transmitir datos por debajo de este límite. Para controlar la congestión, cualquier nodo a lo largo del camino de la conexión puede reducir el límite de la velocidad mediante el envío de un mensaje de control hacia el emisor. En la Sección 12.6 se describe un esquema basado en velocidad para redes ATM.

12.3. GESTIÓN DE TRÁFICO

Existen numerosas cuestiones relacionadas con el control de congestión que podrían incluirse bajo el título general de gestión de tráfico. En su forma más simple, el control de congestión está relacionado con el uso eficiente de una red con alta carga. Cuando se presenta una situación así se pueden aplicar los distintos mecanismos estudiados en la sección anterior, sin importar el emisor o el destino particulares afectados. Cuando un nodo se satura y debe rechazar paquetes se puede aplicar alguna regla sencilla tal como la consistente en el rechazo de los paquetes más recientemente recibidos. Sin embargo, se pueden utilizar otras consideraciones para mejorar la aplicación de las técnicas de control de congestión y de la política de rechazo.

IDONEIDAD

A medida que aumenta la congestión, los flujos de paquetes entre los emisores y los destinos sufrirán aumentos en el retardo y, para alta congestión, pérdidas de paquetes. Sería deseable asegurar que, como mínimo, los distintos flujos sufran congestión en la misma medida. El simple hecho de rechazar paquetes de acuerdo con la regla último-recibido-primero-descartado puede no resultar justo. Un ejemplo de una técnica que podría ser adecuada consiste en el mantenimiento por parte de los nodos de una cola separada para cada conexión lógica o para cada pareja origen-destino. Si todas las memorias temporales asociadas a las colas tienen el mismo tamaño, las colas con mayor tráfico sufrirán rechazos más a menudo, permitiendo que las conexiones con bajo tráfico compartan la capacidad.

CALIDAD DE SERVICIO

Se podría dar un trato diferente a los distintos flujos de tráfico. Por ejemplo, como se indica en [JAIN92], algunas aplicaciones tales como voz y vídeo, son sensibles al retardo pero insensibles a la pérdida de datos; otras, como la transferencia de ficheros y el correo electrónico, son insensibles al retardo pero sensibles a las pérdidas; otras más, como gráficos interactivos o aplicaciones de cómputo interactivo, son sensibles tanto al retardo como a las pérdidas. Por otra parte, hay que señalar que flujos de tráfico distintos tienen prioridades diferentes; por ejemplo, el tráfico de gestión de red, en particular durante la ocurrencia de congestión o fallos, es más importante que el tráfico de aplicación.

Esto es especialmente importante durante aquellos periodos de congestión en los que los flujos de tráfico con distintos requisitos se tratan de forma diferente y se les asigna una calidad de servicio (QoS, quality of service) diferente. Por ejemplo, un nodo puede transmitir en la misma cola paquetes de alta prioridad en preferencia sobre paquetes con prioridad menor; o un nodo puede mantener diferentes colas con distintos niveles QoS y dar prioridad a los niveles superiores.

RESERVAS

Una forma de evitar la congestión y asegurar al mismo tiempo un servicio de calidad dada para aplicaciones es el uso de un esquema de reserva. Un esquema de este tipo es una parte integral de las redes ATM. Cuando se establece una conexión lógica, la red y el usuario llevan a cabo un acuerdo de tráfico que especifica una velocidad de transmisión además de otras características del flujo de tráfico. La red

acuerda proporcionar una QoS particular mientras el tráfico se encuentre dentro de los parámetros acordados, descartándose o gestionándose según el criterio de mínimo esfuerzo además de ser susceptible de rechazo aquel tráfico que exceda estos parámetros. Las reservas a realizar son denegadas si los recursos de la red resultan inadecuados para satisfacerlas. Un tipo de esquema similar ha sido desarrollado para internets IP (RSVP, discutido en el Capítulo 16).

Un aspecto importante del esquema de reservas hace referencia a la política de tráfico (Figura 12.5). Un nodo de la red, generalmente el nodo al que se encuentra conectado el sistema final, supervisa el flujo de tráfico y lo compara con el acuerdo realizado, de forma que se descarta o se marca el exceso de tráfico para indicar que es susceptible de ser rechazado o de sufrir retardo.

12.4. CONTROL DE CONGESTIÓN EN REDES DE CONMUTACIÓN DE PAQUETES

Se han propuesto y experimentado un gran número de mecanismos de control de congestión en redes de conmutación de paquetes. Los siguientes son algunos ejemplos:

1. Envío de un paquete de control desde un nodo congestionado hacia todos o algunos nodos emisores. Este paquete de obstrucción frenará total o parcialmente la velocidad de transmisión de los emisores, limitando así el número total de paquetes en la red. Esta aproximación requiere tráfico adicional en la red mientras dure la congestión.
2. Consideración de la información de encaminamiento. Los algoritmos de encaminamiento, tales como los de ARPANET, informan a otros nodos acerca del retardo de una línea, lo que influye en las decisiones de encaminamiento. Esta información se puede usar también para actuar sobre la velocidad de generación de nuevos paquetes. Dado que estos retardos se encuentran influenciados por las decisiones de encaminamiento, pueden cambiar tan rápidamente que no puedan usarse de forma efectiva en el control de la congestión.
3. Uso de paquetes de prueba extremo a extremo. Estos paquetes pueden llevar un sello de tiempo para determinar el retardo entre dos extremos particulares. Presenta el inconveniente de introducir datos suplementarios en la red.
4. Permiso a los nodos de conmutación para añadir información de congestión a los paquetes que los atraviesan. Existen dos posibles aproximaciones. Un nodo puede añadir esta información a los paquetes que vayan en dirección contraria a la de la congestión; esta información alcanzará rápidamente el nodo origen, que puede reducir el flujo de paquetes en la red. Alternativamente, esta información podría añadirse a los paquetes en la misma dirección de la congestión, en cuyo caso el destino requiere del nodo origen un ajuste de la carga o bien devuelve a éste una señal en los paquetes (o confirmaciones) en dirección opuesta.

12.5. GESTIÓN DE TRÁFICO EN ATM

Debido a su alta velocidad y al pequeño tamaño de celda usado, las redes ATM presentan dificultades no existentes en otros tipos de redes para el control efectivo de la congestión. La complejidad del problema se debe al reducido número de bits suplementarios disponibles para llevar a cabo el control sobre el flujo de celdas de usuario. Este campo es en la actualidad un tema de intensa investigación, encontrándose aún en desarrollo diversas técnicas para el control de tráfico y de congestión. ITU-T, en el documento I.371, ha definido un conjunto restringido inicial de capacidades de control de tráfico y de congestión encaminadas hacia la consecución de mecanismos sencillos y eficiencias de red realistas. El Foro ATM ha publicado una versión algo más avanzada de este conjunto de capacidades en su especificación de gestión de tráfico 4.0 [ATM96]. Esta sección se centra en las especificaciones dadas por el Foro ATM.

Comenzaremos con una revisión del problema de congestión y el sistema adoptado por ITU-T y ATM. Tras esto se discutirán algunas de las técnicas específicas desarrolladas para la gestión de tráfico y el control de congestión.

REQUISITOS PARA EL CONTROL DE TRÁFICO Y DE CONGESTIÓN EN ATM

Tanto los tipos de modelo de tráfico impuestos en redes ATM como las características de transmisión de este tipo de redes difieren en gran medida de los de otras redes de conmutación. La mayor parte de las redes de conmutación de paquetes y de retransmisión de tramas no transportan tráfico de datos de tiempo real. Generalmente, el tráfico sobre circuitos virtuales individuales o sobre conexiones de retransmisión de tramas es de naturaleza a ráfagas, esperando el sistema receptor la llegada del tráfico sobre cada conexión de esta forma. En consecuencia:

- La red no necesita replicar exactamente el patrón de tiempo del tráfico de entrada sobre el nodo de salida.
- Por tanto, se puede usar una simple multiplexación estadística para dar cabida a varias conexiones lógicas sobre la interfaz física entre el usuario y la red. La velocidad de transmisión media necesaria en cada conexión es menor que la tasa de ráfagas para la conexión en cuestión, y la interfaz usuario-red (UNI) sólo precisa estar diseñada para una capacidad ligeramente superior a la suma de las velocidades promedio para todas las conexiones.

Existen numerosas herramientas para el control de congestión en redes de conmutación de paquetes y de retransmisión de tramas, algunas de las cuales se presentan a lo largo de este capítulo. Estos tipos de esquemas de control de congestión no son adecuados para redes ATM, citándose para ello en [GERS91] varias razones:

- La mayor parte del tráfico no está sujeto a control de flujo alguno. Por ejemplo, las fuentes de tráfico de voz y de vídeo no pueden parar de generar celdas aun cuando la red se encuentre congestionada.
- La realimentación es lenta debido a lo drásticamente reducido del tiempo de transmisión de celdas en comparación con los retardos de propagación a través de la red.
- Las redes ATM soportan generalmente una amplia variedad de aplicaciones, las cuales requieren capacidades comprendidas entre unos pocos kbps y varias centenas de Mbps. Los esquemas de control de congestión relativamente simples generalmente acaban castigando uno u otro extremo del espectro.
- Las aplicaciones sobre redes ATM pueden dar lugar a diversos patrones de tráfico (por ejemplo, fuentes de velocidad constante frente a fuentes de velocidad variable). De nuevo, resulta difícil para las técnicas de control de congestión convencionales gestionar adecuadamente este tráfico.
- Aplicaciones distintas sobre redes ATM necesitan servicios de red diferentes (por ejemplo, servicio sensible al retardo para voz y vídeo y servicio sensible a las pérdidas para datos).
- Las elevadas velocidades en conmutación y transmisión hacen que las redes ATM sean más volubles en términos de control de congestión y de tráfico. Un esquema que dependa de las condiciones cambiantes producirá fluctuaciones extremas y desastrosas en la política de encaminamiento y en el control de flujo.

Dos cuestiones clave del funcionamiento relacionadas con los puntos anteriores son los efectos de latencia/velocidad y la variación del retardo de celdas, las cuales pasamos a describir a continuación.

EFECTOS DE LATENCIA/VELOCIDAD

Considérese la transferencia de celdas ATM sobre una red con una velocidad de 150 Mbps. A dicha velocidad se tardará $(53 \times 8 \text{ bits}) / (150 \times 10^6 \text{ bps}) \approx 2{,}8 \times 10^6$ segundos en insertar una sola celda en

la red. El tiempo que se tarda en transmitir la celda desde el origen hasta el usuario destino dependerá del número de conmutadores ATM intermedios, del tiempo de conmutación en cada conmutador y del tiempo de propagación a lo largo de todos los enlaces que componen el camino entre el origen y el destino. Por sencillez, ignoremos los retardos de conmutación ATM y supongamos que la propagación se realiza a una velocidad igual a dos tercios la de la luz. Así, si el origen y el destino se encuentran situados en las costas opuestas de los Estados Unidos, el retardo de propagación del viaje de ida y vuelta será de 48×10^{-3} segundos.

En estas condiciones, supóngase que un emisor A lleva a cabo la transferencia de un fichero largo hacia un destino B y que se hace uso de control implícito de la congestión (es decir, no existen notificaciones explícitas de congestión, sino que el emisor deduce la ocurrencia de congestión a partir de la pérdida de datos). Si la red pierde una celda debido a la congestión, B puede devolver un mensaje de rechazo a A, que debe retransmitir la celda perdida y, posiblemente, todas las celdas siguientes. Pero debido al tiempo que tarda la notificación en llegar a A, éste ha transmitido N celdas adicionales, donde

$$N = \frac{48 \times 10^{-3} \text{ segundos}}{2{,}8 \times 10^{-6} \text{ segundos/celda}} = 1{,}7 \times 10^{4} \text{ celdas} = 7{,}2 \times 10^{6} \text{ bits}$$

Es decir, antes de que A pueda reaccionar ante la indicación de congestión se han transmitido por encima de 7 megabits de datos.

Este cálculo ayuda a explicar por qué las técnicas que son adecuadas para la mayoría de las redes tradicionales no funcionan cuando se aplican a redes WAN ATM.

VARIACIÓN DEL RETARDO DE CELDAS

Para una red ATM, las señales de voz y de vídeo se pueden digitalizar y transmitir como una secuencia de celdas, lo que requiere, especialmente para voz, que los retardos en la red sean pequeños. Éste es generalmente el caso de las redes ATM, que, como ya se ha discutido, están diseñadas para minimizar el coste de transmisión y el procesamiento interno a la red, de forma que sea posible una conmutación de celdas y un encaminamiento muy rápidos.

Existe otro importante requisito que entra en conflicto a veces con el anterior: la velocidad de envío de celdas al usuario destino debe ser constante. Ahora bien, es inevitable que exista alguna variabilidad en la velocidad de transmisión de celdas debido a efectos internos a la red y en la UNI origen. A continuación se resumen estos efectos, considerándose en primer lugar cómo podría hacer frente el usuario destino a las variaciones del retardo de celdas en tránsito hacia él desde el usuario origen.

En la Figura 12.6 se muestra un procedimiento general para conseguir una velocidad constante (CBR). Sea $D(i)$ el retardo extremo a extremo experimentado por la celda i-ésima. El sistema destino no conoce el retardo exacto dado que no existe sello de tiempo asociado a cada celda y, aun en el caso de que lo hubiese, es imposible mantener perfectamente sincronizados los relojes del emisor y del receptor. Cuando se recibe en un instante de tiempo t_0 la primera celda de una conexión, el usuario retarda la celda una cantidad adicional $V(0)$ antes de enviarla a la aplicación. Esta cantidad, $V(0)$, es una estimación de la variación del retardo de celdas que puede tolerar la aplicación y que es probable que ocasione la red.

Las siguientes celdas se retrasan de manera que se transmiten hacia el usuario a una velocidad constante de R celdas por segundo, siendo por tanto $\delta = 1/R$ el tiempo de envío de una celda a la aplicación (tiempo transcurrido entre el comienzo del envío de una celda y el comienzo del envío de la siguiente). Para conseguir una velocidad constante, la siguiente celda se retrasa una cantidad variable $V(1)$ de modo que se satisfaga:

$$t_1 + V(1) = t_0 + V(0) + \delta$$

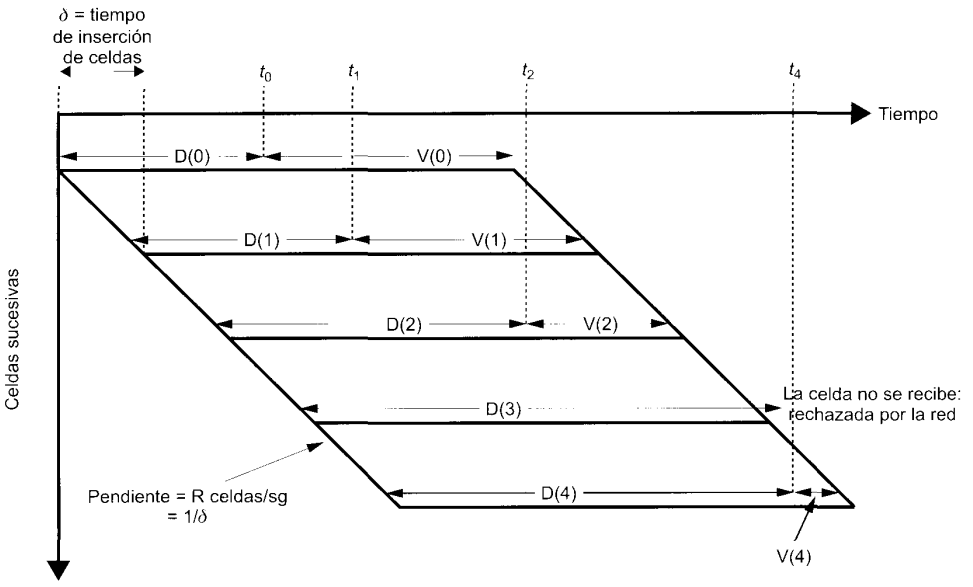


Figura 12.6. Tiempo de ensamblado de celdas CBR.

Así,

$$V(1) = V(0) - [t_1 - (t_0 + \delta)]$$

En general,

$$V(i) = V(0) - [t_i - (t_0 + i \times \delta)]$$

que se puede expresar también como

$$V(i) = V(i-1) - [t_i - (t_{i-1} + \delta)]$$

Si el valor de $V(i)$ obtenido es negativo, se rechaza la celda. El resultado es que los datos se envían a la capa superior a una velocidad constante, con espaciados ocasionales debido a la pérdida de celdas.

El retardo inicial $V(0)$, que es también el retardo medio aplicado a todas las celdas entrantes, es función de la variación de retardo de celdas esperada. Para minimizar este retardo, un abonado debe solicitar del proveedor de la red una variación del retardo de celdas mínima, lo que nos lleva al siguiente compromiso: la variación del retardo de celdas se puede reducir aumentando la velocidad en la UNI relativa a la carga e incrementando los recursos en la red.

Contribución de la red a la variación del retardo de celdas

Una componente de la variación del retardo de celdas se debe a sucesos internos a la red. La variación del retardo de paquetes en redes de conmutación de paquetes puede ser considerable debido a los efectos de puesta en cola en cada uno de los nodos de conmutación intermedios y al tiempo de procesamiento necesario para analizar las cabeceras de los paquetes y llevar a cabo el encaminamiento. En menor medida, esto mismo ocurre con la variación del retardo de tramas en redes de retransmisión de tramas.

Por su parte, en el caso de redes ATM es probable que las variaciones del retardo de celdas debidas a los efectos de la red sean inferiores incluso que en retransmisión de tramas. Las principales razones para ello son las siguientes:

- El protocolo ATM está diseñado para minimizar el procesamiento suplementario en los nodos de conmutación intermedios. Las celdas son de tamaño fijo con formatos de cabecera también fijos, no siendo necesarios procedimientos de control de errores ni de flujo.
- Para dar cabida a las altas velocidades de las redes ATM, los conmutadores ATM se han diseñado para ofrecer un rendimiento extremadamente alto. Así, el tiempo de procesamiento en un nodo para una celda individual es despreciable.

La congestión es el único factor que podría provocar variaciones importantes en el retardo de celdas. Si la red comienza a congestionarse, las celdas se pueden descartar o bien pueden ser puestas en cola en los conmutadores afectados. En consecuencia, es importante que la carga aceptada por la red en cualquier instante de tiempo sea tal que no cause congestión.

Variación del retardo de celdas en la UNI

Incluso si la aplicación transmite datos a una velocidad constante, la variación en el retardo de celdas puede producirse en el origen debido al procesamiento que tiene lugar en las tres capas del modelo ATM.

En la Figura 12.7 se ilustran las posibles causas de la variación del retardo de celdas. En este ejemplo, las conexiones ATM A y B soportan velocidades de transmisión de datos de usuario de X e Y Mbps, respectivamente ($X > Y$). Los datos se segmentan en el nivel AAL en bloques de 48 octetos. Obsérvese que, en un diagrama de tiempo, los bloques parecen de tamaño diferente para las dos conexio-

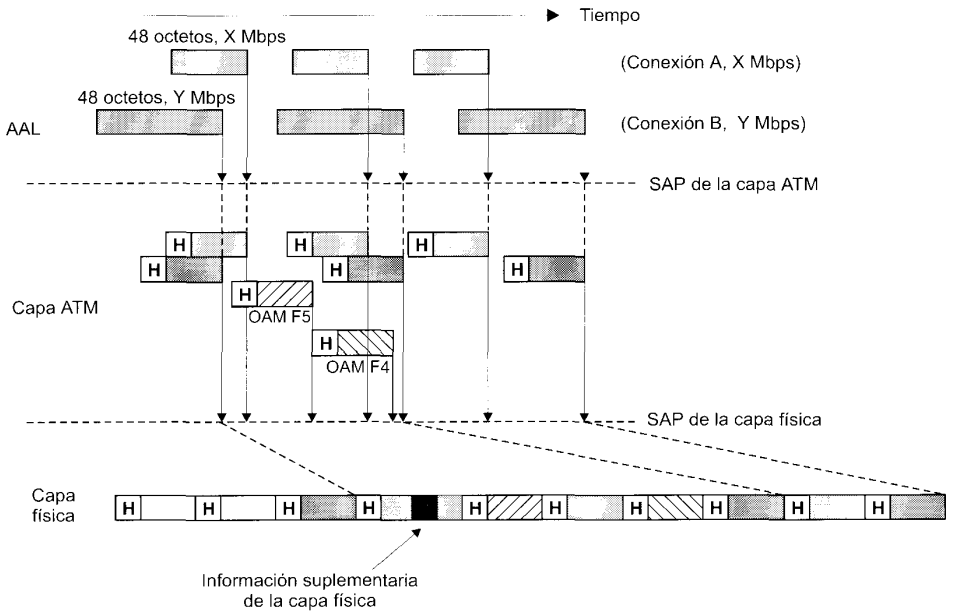


Figura 12.7. Orígenes de la variación del retardo de celdas (I.371).

nes; concretamente, el tiempo, en microsegundos, necesario para generar un bloque de 48 octetos de datos es:

$$\text{Conexión A: } \frac{48 \times 8}{X}$$

$$\text{Conexión B: } \frac{48 \times 8}{Y}$$

La capa ATM encapsula cada segmento en una celda de 53 octetos. Estas celdas se deben mezclar y enviar a la capa física para transmitirlas a la velocidad de transmisión del enlace. El retardo se debe al proceso de entremezclado: si dos celdas de diferentes conexiones llegan a la capa ATM en tiempos solapados, una de las celdas debe ser retrasada en una cantidad igual al solapamiento. Además, la capa ATM genera celdas OAM (operación y mantenimiento) que deben ser mezcladas con celdas de usuario.

Es posible introducir retardos de celda adicionales en la capa física. Por ejemplo, si las celdas se transmiten en tramas SDH (jerarquía digital síncrona), los bits suplementarios de estas tramas se insertarán en el enlace físico, provocando un retardo en los bits de la capa ATM.

Ninguno de los retardos enunciados se puede predecir de forma exacta, y ninguno de ellos sigue un patrón repetitivo. En consecuencia, existe una componente aleatoria en el intervalo de tiempo entre la recepción de datos en la capa ATM desde la capa AAL y la transmisión de esos datos en una celda a través de la UNI.

CONTROL DE TRÁFICO Y DE CONGESTIÓN

El documento I.371 especifica los siguientes objetivos en el control de tráfico y de congestión en ATM:

- El control de tráfico y de congestión en la capa ATM debería permitir un número suficiente de clases de calidad de servicio (QoS) de la capa ATM para todos los servicios de red posibles; la especificación de estas clases de QoS debe ser consistente con las prestaciones de la red en estudio.
- El control de tráfico y de congestión en la capa ATM no debería depender de protocolos AAL específicos del servicio de red ni de protocolos de capa superior que sean específicos de la aplicación. Los protocolos de capas superiores a la capa ATM pueden hacer uso de información proporcionada por esta capa para mejorar la utilidad que dichos protocolos pueden obtener de la red.
- El diseño de un conjunto óptimo de controles de tráfico y de congestión en la capa ATM debería minimizar la complejidad de la red y de los sistemas finales al tiempo que se maximiza la utilización de la red.

Para conseguir estos objetivos, ITU-T y el Foro ATM han definido una serie de funciones de control de tráfico y de congestión que operan en un rango dado de intervalos de tiempo. En la Tabla 12.1 se listan estas funciones con respecto a los tiempos de respuesta en los que operan. Se consideran cuatro niveles de tiempo:

- **Tiempo de inserción de celdas:** las funciones de este nivel reaccionan inmediatamente ante celdas transmitidas.
- **Tiempo de propagación de ida y vuelta:** en este nivel la red responde dentro del tiempo de vida de una celda en la red y puede realizar indicaciones al origen en forma de realimentación.
- **Duración de la conexión:** la red determina en este nivel si se puede establecer una nueva conexión con una QoS dada y qué nivel de prestaciones se fijará.
- **Término de larga duración:** son controles que afectan a más de una conexión ATM y se establecen para uso de larga duración.

Tabla 12.1. Funciones de control de tráfico y de congestión.

Tiempo de respuesta	Funciones de control de tráfico	Funciones de control de congestión
Término de larga duración	• Gestión de recursos usando caminos virtuales	
Duración de conexión	• Control de admisión de conexiones (CAC)	
Tiempo de propagación de ida y vuelta	• Gestión rápida de recursos	• Indicación explícita de congestión hacia adelante (EFCI) • Control de flujo ABR
Tiempo de inserción de celdas	• Control de los parámetros de uso (UPC) • Control de prioridad • Adaptación de tráfico	• Rechazo selectivo de celdas

La esencia de la estrategia de control de tráfico se basa en (1) la determinación de si se puede dar cabida a una nueva conexión ATM y en (2) el acuerdo con el abonado acerca de los parámetros de prestaciones tolerados. En efecto, el abonado y la red llevan a cabo un contrato o acuerdo de tráfico: la red acepta tolerar un tráfico con un nivel de prestaciones dado sobre esa conexión y el abonado acepta no exceder los límites de los parámetros de tráfico fijados. Las funciones de control de tráfico están relacionadas con el establecimiento y cumplimiento de estos parámetros de tráfico, por lo que están relacionados con la prevención de la congestión. Si el control de tráfico falla en algunas situaciones se puede producir congestión, en cuyo caso se invocan las funciones de control de congestión para responder y solventar el problema de la congestión.

TÉCNICAS DE GESTIÓN DE TRÁFICO Y DE CONTROL DE CONGESTIÓN

ITU-T y el Foro ATM han definido un conjunto de funciones de gestión de tráfico para mantener la calidad del servicio (QoS) de las conexiones ATM. Las funciones de gestión de tráfico ATM hacen referencia al conjunto de acciones tomadas por la red para evitar las condiciones de congestión o minimizar los efectos de ésta. En esta sección se presentan las siguientes técnicas:

- Gestión de recursos haciendo uso de caminos virtuales.
- Control de admisión de conexiones.
- Control de los parámetros de uso.
- Rechazo selectivo de celdas.
- Adaptación del tráfico.

Gestión de recursos haciendo uso de caminos virtuales

El concepto fundamental en la gestión de recursos de red es la reserva de dichos recursos de manera que se separan los flujos de tráfico de acuerdo con las características del servicio. Hasta ahora, la única función de control de tráfico específica basada en la gestión de recursos de red definida por el Foro ATM hace uso de caminos virtuales.

Como se vio en el Capítulo 11, una conexión de camino virtual (VPC) proporciona una forma adecuada para llevar a cabo la agrupación de conexiones de canales virtuales similares (VCC). La red ofre-

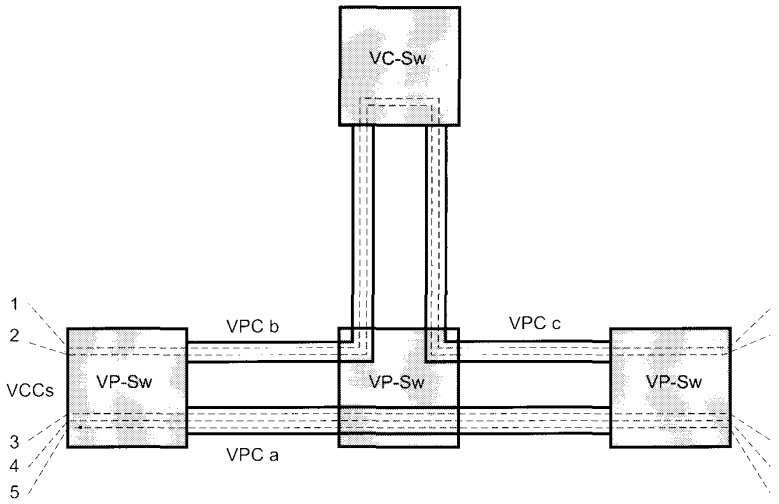
ce características conjuntas de prestaciones y capacidad en el camino virtual, siendo compartidas por las conexiones virtuales. Se deben considerar tres casos:

- **Aplicación usuario-usuario:** la VPC se extiende entre un par de UNI. En este caso, la red no conoce la QoS de las VCC individuales en la VPC, de modo que es responsabilidad del usuario asegurar que la VPC pueda dar cabida a la demanda conjunta de las VCC.
- **Aplicación del usuario a la red:** la VPC se extiende entre una UNI y un nodo de la red. En este caso, la red conoce la QoS de las VCC en una VPC y debe darles cabida.
- **Aplicación red-red:** la VPC se extiende entre dos nodos de red. De nuevo, la red conoce la QoS de las VCC en la VPC y debe darles cabida.

Los parámetros de QoS más importantes relacionados con la gestión de los recursos de red son la tasa de pérdida de celdas, el retardo de transferencia de celdas y la variación del retardo de celdas, estando todos ellos afectados por la cantidad de recursos dedicados por la red a la VPC. Si una VCC se extiende a través de varias VPC, las prestaciones de las VCC dependen de las prestaciones de las VPC consecutivas y de cómo se gestiona la congestión en cualquier nodo que realice funciones relacionadas con las VCC. Este nodo puede ser un conmutador, un concentrador u otro equipo de red. Las prestaciones de cada VPC dependen de la capacidad de la VPC y de las características de tráfico de las VCC contenidas en la VPC. Las prestaciones de cada una de las funciones relacionadas con las VCC dependen de la velocidad de conmutación/procesamiento en el nodo y de la prioridad relativa con que se gestionan las distintas celdas.

En la Figura 12.8 se muestra un ejemplo. Las VCC 1 y 2 presentan unas prestaciones que dependen de las VPC b y c y de cómo se gestionan estas VCC en los nodos intermedios. Esto puede diferir de las prestaciones observadas en las VCC 3, 4 y 5.

Existen varias alternativas en la manera de agrupar VCC y en el tipo de prestaciones que presentan. Si todas las VCC en una VPC se gestionan de forma similar, deberían experimentar prestaciones de red



VPC = conexión de camino virtual
VCC = conexión de canal virtual
VP-Sw = función de conmutación de camino virtual
VC-Sw = función de conmutación de canal virtual

Figura 12.8. Configuración de VCC y VPC.

similares en términos de tasa de pérdida de celdas, de retardo de transferencia de celdas y de variación del retardo de celdas. Alternativamente, cuando VCC diferentes en la misma VPC requieren una QoS diferente, las prestaciones de la VPC acordadas entre la red y el abonado deberían ser alcanzables para la mayor parte de los requisitos VCC demandados.

En cualquier caso, cuando existen varias VCC en la misma VPC, la red tiene dos opciones para reservar capacidad para la VPC:

- **Demanda conjunta de pico:** la red puede establecer la capacidad (velocidad) de la VPC a un valor igual a la suma de las velocidades de pico de todas las VCC en la VPC. La ventaja de esta aproximación es que cada VCC puede presentar una QoS que dé cabida a su demanda de pico. Por contra, la desventaja radica en que la capacidad de la VPC no se utiliza completamente durante la mayor parte del tiempo y, en consecuencia, algunos recursos de la red estarán infrautilizados.
- **Multiplexación estadística:** si la red especifica la capacidad de la VPC a un valor mayor o igual que la suma de las velocidades promedio de las VCC pero menor que la demanda de pico conjunta, se ofrece un servicio de multiplexación estadística. Con esta técnica de multiplexación, las VCC experimentan una variación del retardo de celdas y un retardo de transferencia de celdas superiores. Dependiendo del tamaño de las memorias temporales usadas en las colas de transmisión de celdas, las VCC pueden experimentar también una mayor tasa de pérdida de celdas. Esta aproximación tiene la ventaja de utilizar la capacidad de forma más eficiente, resultando atractiva si las VCC pueden tolerar la QoS inferior.

Cuando se usa multiplexación estadística es preferible agrupar las VCC en varias VPC bajo la consideración de características de tráfico y necesidad de QoS similares. Si VCC diferentes comparten la misma VPC y se usa multiplexación estadística, es difícil ofrecer un acceso adecuado simultáneamente a las secuencias de bajo y de alto tráfico.

Control de admisión de conexiones

El control de admisión de conexiones es la primera línea de defensa de autoprotección de la red ante una carga excesiva. En esencia, cuando un usuario solicita una VCC o una VPC nuevas, debe especificar (implícita o explícitamente) las características de tráfico para la conexión en ambos sentidos. El usuario selecciona las características de tráfico mediante la elección de una QoS de entre las clases que ofrece la red. La red acepta la conexión sólo si puede conseguir los recursos necesarios para admitir el nivel de tráfico, al tiempo que mantiene la QoS convenida en las conexiones existentes. Al aceptar la conexión, la red establece un *contrato de tráfico* con el usuario. Una vez aceptada la conexión, la red continúa ofreciendo la QoS convenida mientras el usuario respete el acuerdo de tráfico.

El acuerdo o contrato de tráfico puede consistir en los cuatro parámetros definidos en la Tabla 12.2: velocidad de pico de celdas (PCR), variación del retardo de celdas (CDV), velocidad sostenible de celdas (SCR) y tolerancia a ráfagas. Con fuentes de velocidad constante (CBR) sólo son relevantes los dos primeros parámetros, pudiéndose utilizar los cuatro cuando se trabaja con fuentes de velocidad variable (VBR).

Como sugiere el nombre, la velocidad de pico de celdas es la máxima velocidad a la que se generan en el origen las celdas para una conexión dada. Sin embargo, hemos de tener en consideración la variación del retardo de celdas. Aunque un emisor puede generar celdas a una velocidad de pico constante, las variaciones del retardo de celdas debidas a diversos factores (véase Figura 12.7) afectarán a la evolución temporal, provocando la agrupación y separación de celdas. Así pues, una fuente puede exceder temporalmente la velocidad de pico de celdas debido a la agrupación. Para que la red reserve adecuadamente recursos para esta conexión, debe conocer no sólo la velocidad de pico de celdas, sino también la CDV.

La relación exacta entre la velocidad de pico de celdas y la CDV depende de las definiciones operacionales de estos dos términos. El estándar establece estas definiciones en términos de un algoritmo de

Tabla 12.2. Parámetros de tráfico usados en la definición de la QoS de VCC/VPC.

Parámetro	Descripción	Tipo de tráfico
Velocidad de pico de celdas (PCR)	Límite superior de tráfico que puede presentarse en una conexión ATM	CBR, VBR
Variación del retardo de celdas (CDV)	Límite superior de la variabilidad en el patrón de recepción de celdas observado en un único punto de medida en referencia a la velocidad de pico de celdas	CBR, VBR
Velocidad sostenible de celdas (SCR)	Límite superior de la velocidad media de una conexión ATM, calculado sobre la duración de la conexión	VBR
Tolerancia a ráfagas	Límite superior de la variabilidad en el patrón de recepción de celdas observado en un único punto de medida en referencia a la velocidad sostenible de celdas	VBR

CBR = velocidad constante
VBR = velocidad variable

velocidad de celdas. Dado que el algoritmo se puede usar para el control de los parámetros de uso, pospondremos su estudio hasta el siguiente apartado.

Los parámetros PCR y CDV deben especificarse para cada conexión. Como opción para fuentes de velocidad variable, el usuario puede especificar también una velocidad sostenible de celdas y una tolerancia a la aparición de ráfagas. Estos parámetros son análogos a PCR y CDV, respectivamente, pero aplicados a una velocidad de generación de celdas promedio en lugar de a una velocidad de pico. El usuario puede describir el flujo futuro de celdas en mayor detalle mediante el uso de los parámetros SCR y tolerancia a ráfagas así como mediante PCR y CDV. Con esta información adicional, la red podría utilizar más eficientemente sus recursos; por ejemplo, si se multiplexan estadísticamente varias VCC sobre una VPC, el conocimiento de las velocidades promedio y de pico de celdas posibilita a la red la reserva de memoria temporal de capacidad suficiente para la gestión eficaz del tráfico sin pérdida de celdas.

Para una conexión dada (VPC o VCC), los cuatro parámetros de tráfico se pueden especificar de formas distintas según se ilustra en la Tabla 12.3. Los valores de los parámetros se pueden definir implí-

Tabla 12.3. Procedimientos usados para establecer los valores de los parámetros de tráfico contratados.

	Parámetros especificados explícitamente		**Parámetros especificados implícitamente**
	Valores de parámetros especificados en el momento del establecimiento *de la conexión*	**Valores de parámetros especificados en el momento de la suscripción**	**Valores de parámetros especificados usando reglas por defecto**
	Requerido por el usuario/NMS	**Asignados por el operador de la red**	
SVC	Señalización	Mediante suscripción	Reglas por defecto red-operador
PVC	NMS	Mediante suscripción	Reglas por defecto red-operador

SVC = conexión virtual conmutada
PVC = conexión virtual permanente
NMS = sistema de gestión de red

citamente mediante reglas impuestas por el operador de la red. En este caso se les asignan los mismos valores a todas las conexiones, o a todas las conexiones de una misma clase se les asigna el valor de esta clase. El operador de red puede asociar también valores de parámetros a un abonado dado y asignarlos en el momento de la suscripción; asimismo, los valores de los parámetros para una conexión particular, se pueden asignar en el momento de la conexión. En el caso de una conexión virtual permanente, estos valores se asignan por la red cuando se establece la conexión. Para una conexión virtual conmutada, los parámetros son negociados entre el usuario y la red mediante un protocolo de señalización.

Otro aspecto de la calidad del servicio que se puede solicitar o asignar para una conexión dada es la prioridad de pérdida de celdas. Un usuario puede solicitar dos niveles de prioridad de pérdida de celdas para una conexión ATM, indicándose la prioridad de una celda individual mediante el bit CLP existente en su cabecera (Figura 11.4). Cuando se usan dos niveles de prioridad se deben especificar los parámetros de tráfico para ambos flujos de celdas. Esto se realiza generalmente mediante la especificación de un conjunto de parámetros de tráfico para tráfico de alta prioridad (CLP = 0) y un conjunto de parámetros de tráfico para todo tipo de tráfico (CLP = 0 o 1). Basándose en este análisis, la red puede llevar a cabo la reserva de recursos de forma más eficiente.

Control de los parámetros de uso

Una vez que la conexión ha sido aceptada por la función de control de admisión de conexiones, la función de control de parámetros de uso (UPC) de la red supervisa la conexión para determinar si el tráfico está en concordancia con el contrato de tráfico acordado. El objetivo principal del control de los parámetros de uso es proteger los recursos de la red ante la producción de una sobrecarga en una conexión, lo que afectaría adversamente la QoS en otras conexiones, a través de la detección de violaciones en los parámetros asignados y tomando las medidas oportunas.

El control de los parámetros de uso se puede realizar tanto a nivel de camino virtual como a nivel de canal virtual. El más importante de ellos es el control a nivel VPC, ya que los recursos de la red se reservan inicialmente, en general, en base a caminos virtuales, con la capacidad del camino virtual compartida entre los diferentes canales virtuales miembros.

Existen dos funciones distintas asociadas al control de los parámetros de uso:

- Control de la velocidad de pico de celdas y de la variación del retardo de celdas asociada (CDV).
- Control de la velocidad sostenible de celdas y de la tolerancia a la aparición de ráfagas.

Consideremos en primer lugar la velocidad de pico de celdas y la variación del retardo de celdas asociada. En términos sencillos, se dice que un tráfico es adecuado si la velocidad de pico de transmisión de celdas no excede la velocidad de pico de celdas acordada, sujeta a la posibilidad de que la variación del retardo de celdas se encuentre en el rango establecido. El documento I.371 define un algoritmo, el algoritmo de velocidad de pico de celdas, que supervisa el acuerdo en base a dos parámetros: la velocidad de pico de celdas, R, y el límite de tolerancia CDV, τ. Así, $T = 1/R$ es el intervalo de tiempo de llegada entre celdas si no hay CDV. En caso de que exista CDV, T es el tiempo promedio de llegada entre celdas a la velocidad de pico. El algoritmo se ha definido para supervisar la velocidad a la que llegan las celdas y para asegurar que el tiempo de llegada entre celdas no es demasiado pequeño para provocar que el flujo exceda la velocidad de pico de celdas en una cantidad superior al límite de tolerancia.

El mismo algoritmo, con parámetros distintos, se puede usar para supervisar la velocidad sostenible de celdas R_s y la tolerancia de aparición de ráfagas asociada τ_s.

El algoritmo de velocidad de celdas es bastante complejo, pudiéndose encontrar los detalles en [STAL99b]. Este algoritmo define simplemente una forma de supervisar el cumplimiento del contrato de tráfico. Para llevar a cabo el control de los parámetros de uso, la red debe actuar de acuerdo con los

resultados del algoritmo, consistiendo la estrategia más sencilla en aceptar las celdas que cumplen con los parámetros, descartándose por la función UPC aquellas que no los cumplen.

Las celdas que no cumplen con el contrato de tráfico pueden ser marcadas a opción de la red. En este caso, una celda que no cumple con el contrato se puede marcar con CLP = 1 (baja prioridad) y aceptarse, pudiendo ser descartada de la red posteriormente en caso de congestión.

La situación resulta más compleja en caso de que el usuario haya negociado dos niveles de prioridad de pérdida de celdas para una red. Recordemos que el usuario puede negociar un contrato para tráfico de alta prioridad (CLP = 0) y un contrato distinto para tráfico conjunto (CLP 0 o 1). Se aplican las siguientes reglas:

1. Una celda con CLP = 0 que cumple el contrato de tráfico para CLP = 0 es aceptada.
2. Una celda con CLP = 0 que no cumple el contrato para tráfico (CLP = 0) pero sí para tráfico (CLP 0 o 1) es marcada y aceptada.
3. Una celda con CLP = 0 que no cumple el contrato para tráfico (CLP = 0) ni para tráfico (CLP 0 o 1) es rechazada.
4. Una celda con CLP = 1 que cumple el contrato para tráfico (CLP = 0 o 1) es aceptada.
5. Una celda con CLP = 1 que no cumple el contrato para tráfico (CLP = 0 o 1) es rechazada.

Rechazo selectivo de celdas

El rechazo selectivo de celdas se lleva a cabo cuando la red, de forma independiente a la función UPC, rechaza celdas (CLP = 1). El objetivo es el rechazo de celdas de prioridad baja durante la congestión para salvaguardar las prestaciones de las celdas de prioridad superior. Obsérvese que la red no tiene forma de discriminar entre celdas marcadas como de baja prioridad por el emisor y celdas marcadas por la función UPC.

Adaptación del tráfico

El algoritmo UPC es una forma de **política de tráfico**, que se produce cuando se regula un flujo de datos de manera que las celdas (o las tramas o los paquetes) que superen un cierto nivel de prestaciones sean rechazadas o marcadas. Puede ser deseable complementar una política de tráfico con una de **adaptación del tráfico,** usada para suavizar el flujo de tráfico y reducir la agrupación de celdas. Esto puede dar lugar a una reserva de recursos más adecuada y a un tiempo de retardo medio reducido.

Una aproximación sencilla para llevar a cabo la adaptación del tráfico consiste en usar una variante del algoritmo UPC conocida como cubo de permisos. En contraste con el algoritmo UPC, que se limita a supervisar el tráfico y marcar o rechazar las celdas que no cumplen el contrato, la adaptación del tráfico mediante una cesta de permisos controla el flujo de celdas que sí cumplen el contrato de tráfico.

En la Figura 12.9 se ilustra el principio básico del método de la cesta de permisos. Un generador de permisos produce éstos a una velocidad de ρ permisos por segundo y los coloca en la cesta de permisos, que tiene una capacidad máxima de β permisos. Las celdas recibidas desde el emisor se sitúan en una memoria temporal con una capacidad máxima de K celdas. Para llevar a cabo la transmisión de una celda a través de un servidor es necesario coger un permiso de la cesta, de modo que si se encuentra vacía, la celda se pone en cola en espera del siguiente permiso. El resultado de este esquema es que si existe un exceso de celdas y la cesta está vacía, las celdas se emiten con un flujo homogéneo de ρ celdas por segundo sin variación en el retardo de celdas hasta que se elimine el exceso. Por tanto, la cesta de permisos suaviza las ráfagas de celdas.

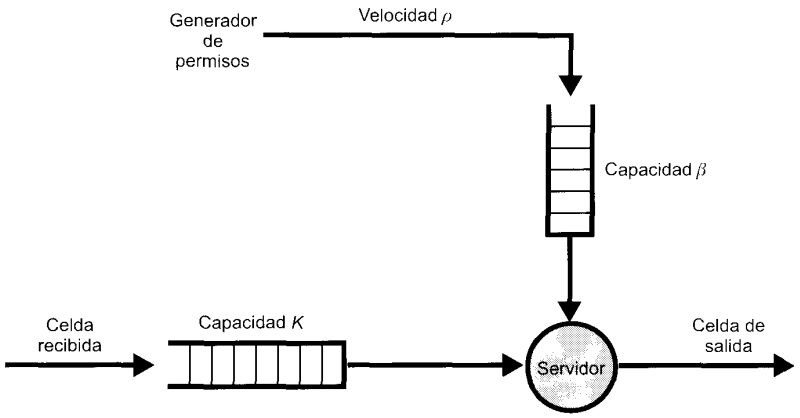


Figura 12.9. Cubo de permisos para adaptación del tráfico.

12.6. GESTIÓN DE TRÁFICO ABR EN ATM

La QoS proporcionada por los tráficos CBR, rt-VBR y nrt-VBR se basa en (1) un contrato de tráfico que especifica las características del flujo de celdas y en (2) el UPC realizado por la red para hacer cumplir el flujo. Durante el proceso de admisión de una conexión, la red usa el contrato de tráfico propuesto para determinar si se encuentran disponibles los recursos para la nueva conexión. Si es así, y una vez establecida la conexión, UPC puede rechazar o marcar como de baja prioridad cualquier celda que exceda los parámetros del contrato de tráfico. No existe realimentación hacia el emisor relativa a la congestión, por lo que la aproximación descrita se conoce como **control en bucle abierto.**

Este tipo de aproximación no es adecuado para muchas de las aplicaciones de datos. Las aplicaciones típicas correspondientes a tráfico no de tiempo real, tales como transferencia de ficheros, acceso a Web, llamadas a procedimientos remotos, servicio de ficheros distribuidos, etc., no tienen características de tráfico bien definidas salvo quizá una velocidad de pico de celdas, si bien la PCR no es por sí misma suficiente para que la red reserve recursos de forma efectiva. Además, este tipo de aplicaciones puede tolerar generalmente retardos impredecibles y un rendimiento variable en el tiempo.

Estas aplicaciones se pueden gestionar de dos formas posibles. Una posibilidad es permitir que estas aplicaciones compartan la capacidad no utilizada de manera relativamente incontrolada. Conforme aumenta la congestión se pierden celdas, de modo los distintos emisores reducirán sus velocidades de datos; esta forma de transmisión encaja bien con las técnicas de control de congestión de TCP (descritas en el Capítulo 17), y es el modo de funcionamiento del servicio UBR. Esta aproximación se denomina de **mínimo esfuerzo,** siendo su principal desventaja su ineficiencia: las celdas se pierden, provocando retransmisiones.

La otra forma de gestionar las aplicaciones no de tiempo real es permitir que varios emisores compartan la capacidad no usada por los tráficos CBR y VBR pero sin realimentación hacia los emisores para poder adaptar dinámicamente la carga y evitar así la pérdida de celdas y el compartimiento adecuado de la capacidad. Esta aproximación se conoce como **control en bucle cerrado** debido al uso de realimentación, y se usa para el servicio ABR.

En esta sección se presenta el servicio ABR y los mecanismos utilizados para el control del flujo de celdas.

En [CHEN96] se especifican las siguientes características como las principales del servicio ABR:

1. Las conexiones ABR comparten la capacidad disponible, teniendo acceso a la capacidad instantánea no utilizada por las conexiones CBR/VBR. Por tanto, ABR puede aumentar la utilización de la red sin afectar a la QoS de las conexiones CBR/VBR.
2. El compartimiento de la capacidad disponible usada por una sola conexión ABR es dinámico y varía entre una velocidad de celdas mínima acordada (MCR) y PCR. La MCR asignada a una conexión particular puede ser cero. Con un valor de MCR distinto de cero la red asegura un rendimiento mínimo; sin embargo, un emisor puede transmitir a una velocidad inferior a una MCR distinta de cero durante un periodo de tiempo dado.
3. La red proporciona realimentación a las fuentes ABR de forma que este flujo está limitado a la capacidad disponible. Los retardos temporales inherentes a la realimentación implican el uso de memorias temporales a lo largo de un camino de conexión; estas memorias absorben el exceso de tráfico generado antes de la llegada de la realimentación al emisor. Dada la alta velocidad y el relativamente elevado retardo de propagación a través de la red, estas memorias pueden ser grandes, dando lugar a retardos elevados. En consecuencia, el servicio ABR es apropiado para aplicaciones que pueden tolerar ajustes en sus velocidades de transmisión y retardos de celdas impredecibles.
4. Para las fuentes ABR que adaptan su velocidad de transmisión de acuerdo con la realimentación recibida, se garantiza una tasa de pérdida de celdas baja. Ésta es una diferencia importante entre el servicio ABR y el UBR.

MECANISMOS DE REALIMENTACIÓN

La velocidad de transmisión de celdas sobre una conexión ABR desde un emisor dado se caracteriza por cuatro parámetros:

- **Velocidad de celdas permitida (ACR):** es la velocidad actual a la que se permite que transmita celdas el emisor. Éste puede transmitir a cualquier velocidad comprendida entre cero y ACR.
- **Velocidad de celdas mínima (MCR):** valor mínimo que puede tomar ACR (es decir, la red no restringirá el flujo del emisor a un valor menor que MCR). MCR se puede fijar a cero para una conexión dada.
- **Velocidad de pico de celdas (PCR):** valor máximo que puede tomar ACR.
- **Velocidad de celdas inicial (ICR):** valor asignado inicialmente a ACR.

Un emisor comienza con ACR = ICR y ajusta ACR de forma dinámica de acuerdo con la realimentación desde la red. Dicha realimentación tiene lugar periódicamente en forma de una secuencia de celdas de gestión de los recursos (RM), cada una de las cuales contiene tres campos que sirven de realimentación al emisor: un bit *indicador de congestión* (CI), un bit de *no incremento* (NI) y un campo de *velocidad explícita de celdas* (ER). El emisor reacciona de acuerdo con las siguientes reglas:

```
if CI = 1
     reducir ACR en una cantidad proporcional a su
        valor actual, pero no a uno menor que MCR
else if NI = 0 incrementar ACR en una cantidad proporcional a PCR,
        pero no exceder el valor de PCR
if ACR > ER hacer ACR ← max [ER, MCR]
```

El emisor comprueba primero los dos bits de realimentación. Si se desea un incremento, éste es fijo e igual a RIF × PCR, donde RIF es un *factor de incremento de velocidad* fijo. Si se lleva a cabo un decremento, éste es exponencial en una cantidad RDF × ACR, siendo RDF un *factor de decremento de velocidad* fijo. Por último, si ER es menor que ACR, el emisor reduce ACR a ER. Todos estos ajustes están sujetos a la condición de que ACR varíe en el rango de límites MCR y PCR. La tabla siguiente resume estas reglas:

NI	CI	Acción
0	0	ACR ← max[MCR, min[ER, PCR, ACR + RIF × PCR]]
0	1	ACR ← max[MCR, min[ER, ACR(1 − RDF)]]
1	0	ACR ← max[MCR, min[ER, ACR]]
1	1	ACR ← max[MCR, min[ER, ACR(1 − RDF)]]

En la Figura 12.10 se ilustra el efecto de la realimentación sobre ACR. En este ejemplo se hace uso de un valor de RIF igual a 1/16, que es el valor por defecto; como se puede ver, cada incremento es por una cantidad constante. El valor por defecto para RDF es también 1/16, pero en la Figura 12.10 usa un valor igual a 1/4 para resaltar el efecto exponencial de RDF: el decremento es proporcional al valor actual de ACR. Con este incremento lineal y decremento exponencial, la fuente incrementará lentamente su velocidad cuando no exista evidencia de congestión, pero decrementará rápidamente su velocidad cuando ésta es elevada y se indica la ocurrencia de congestión.

FLUJO DE CELDAS

Una vez vista la forma en que reacciona un emisor ante la realimentación, a continuación se describe el modo en que ésta se lleva a cabo. En la Figura 12.11 se ilustra el mecanismo. En esta figura se mues-

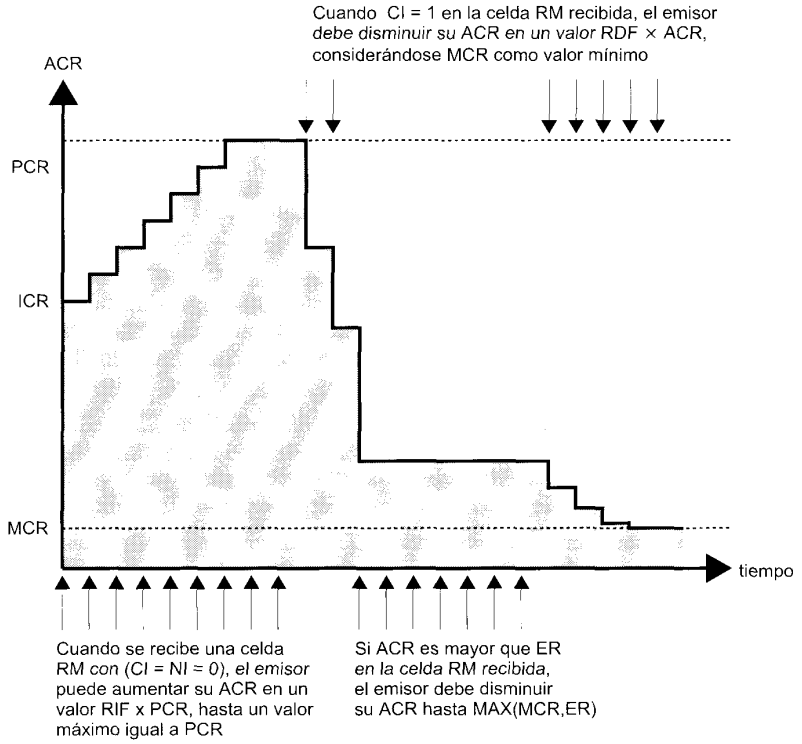


Figura 12.10. Variaciones en la velocidad de celdas permitida (basado en [SAIT96]).

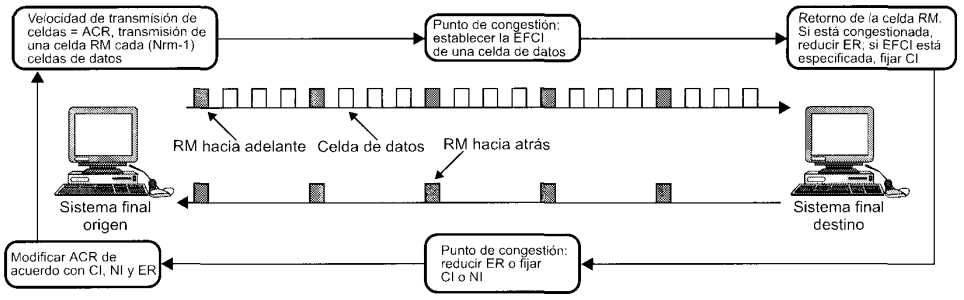


Figura 12.11. Flujo de datos y de celdas RM en una conexión ABR (basado en [SAIT96]).

tra un flujo de datos en cada sentido sobre una conexión ATM para una comunicación de datos bidireccional.

Existen dos tipos de celdas ATM sobre una conexión ABR: celdas de datos y celdas de gestión de recursos (RM). Un emisor recibe una secuencia regular de celdas RM que proporcionan realimentación para permitirle adaptar su velocidad de transmisión de celdas. La mayoría de las celdas RM se generan por parte del emisor, transmitiéndose una **celda RM hacia adelante (FRM)** cada (Nrm − 1) celdas de datos, donde Nrm es un parámetro preestablecido (generalmente igual a 32). Conforme se recibe en el destino cada una de las celdas FRM, éstas se devuelven hacia el emisor como **celdas RM hacia atrás (BRM).**

Cada FRM contiene los campos CI, NI y ER. Generalmente, el emisor hace CI = 0, NI = 0 o 1 y ER igual a una velocidad de transmisión deseada en el rango ICR $\leqslant$ ER $\leqslant$ PCR. Un conmutador ATM o el sistema destino pueden cambiar cualquiera de estos campos antes de que la correspondiente celda BRM vuelva al emisor.

Un conmutador ATM dispone de varias formas para llevar a cabo la realimentación de control de velocidad sobre el emisor:

- **Marca EFCI:** el conmutador puede activar la condición EFCI (indicación explícita de congestión hacia adelante) en la cabecera de una celda de datos ATM (usando el campo de tipo de carga útil) cuando ésta pasa a través suyo en la dirección hacia adelante. Esto provocará que el sistema final de destino active el bit CI en una celda BRM.
- **Marca de velocidad relativa:** el conmutador puede activar directamente el bit CI o el bit NI de una celda RM que lo atraviesa. Si el bit se activa en una celda FRM, éste permanecerá activo en la celda BRM correspondiente en el destino. Activando uno de estos bits en una celda BRM que atraviesa el nodo se consiguen resultados más rápidos, correspondiendo el más rápido de ellos a la generación de una celda BRM con los bits CI o NI activos por parte del conmutador en lugar de esperar a que pase una celda BRM.
- **Marca de velocidad explícita:** el conmutador puede reducir el valor del campo ER de una celda FRM o de una BRM.

Estas acciones permiten a un conmutador ATM indicar a un emisor que se está produciendo congestión y reducir su velocidad de celdas. El sistema destino puede también indicar la ocurrencia de congestión. En condiciones normales, un sistema destino se limita a convertir cada celda FRM entrante en una celda BRM sin modificar los campos NI, CI ni ER, excepto que el bit CI esté activo si se ha recibido una señal EFCI en la celda de datos anterior. Sin embargo, si el destino sufre congestión, éste puede activar el bit CI o el bit NI o reducir el valor de ER cuando convierte una celda FRM en una BRM.

Los primeros conmutadores ATM que soportaban ABR hacían uso de los bits EFCI, NI y CI, ofreciendo un sencillo mecanismo de control de velocidad relativa. Los controles más complejos en que se hace uso de una velocidad explícita constituyen una segunda generación de servicios ABR.

12.7. CONTROL DE CONGESTIÓN EN RETRANSMISIÓN DE TRAMAS

El documento I.370 define los siguientes objetivos del control de congestión en retransmisión de tramas:

- Minimización del rechazo de celdas.
- Mantenimiento, con alta probabilidad y mínima varianza, de una calidad de servicio acordada.
- Minimización de la posibilidad de que un usuario final pueda monopolizar los recursos de la red a expensas de otros usuarios finales.
- Sencillez de implementación y de poco coste adicional tanto desde el punto de vista del usuario final como desde el de la red.
- Generación de mínimo tráfico adicional de red.
- Distribución adecuada de los recursos de red entre los usuarios finales.
- Limitación la expansión de la congestión hacia otras redes y elementos de la red.
- Funcionamiento efectivo independientemente del flujo de tráfico en ambos sentidos entre los usuarios finales.
- Mínima interacción o impacto en otros sistemas en la red de retransmisión de tramas.
- Minimización de la varianza de la calidad del servicio suministrado a conexiones de retransmisión de tramas individuales durante la congestión (por ejemplo, las conexiones lógicas individuales no deberían experimentar una degradación brusca cuando se avecina la congestión o ésta ya se ha producido).

El control de congestión resulta difícil en redes de retransmisión de tramas debido a la limitación de herramientas disponibles en los gestores de tramas (nodos de conmutación de tramas). Se ha mejorado el protocolo de retransmisión de tramas con objeto de maximizar el rendimiento y la eficiencia. Una consecuencia de este hecho es que el gestor de tramas no puede controlar el flujo de tramas de un suscriptor o un gestor de tramas adyacente usando el protocolo de control de flujo de ventana deslizante típico, como el empleado en HDLC.

El control de congestión es responsabilidad conjunta de la red y de los usuarios finales. La red (esto es, el conjunto de gestores de tramas) es el mejor lugar para llevar a cabo la supervisión del grado de congestión, mientras que los usuarios finales constituyen el mejor punto para el control de la congestión mediante la limitación del flujo de tráfico.

En la Tabla 12.4 se enumeran las técnicas de control de congestión definidas en los diversos documentos de ITU-T y ANSI. La **estrategia de rechazo** es la respuesta más básica ante la congestión: cuando ésta llega a ser severa, la red se ve forzada a rechazar tramas. Sería deseable hacer esto de manera adecuada para todos los usuarios.

Los procedimientos de **prevención de congestión** se usan con el fin de minimizar el efecto de la congestión en la red. De este modo, estos procedimientos serían iniciados en o antes del punto A en la Figura 12.4 para prevenir que la congestión alcance el punto B. Cerca del punto A existe poca evidencia para los usuarios finales de que la congestión está aumentando, por lo que debe existir algún mecanismo de **señalización explícita** de la red que ponga en marcha la prevención de congestión.

Los procedimientos de **recuperación de congestión** se usan para prevenir el colapso de la red ante la ocurrencia de una congestión severa. Estos procedimientos se inician generalmente cuando la red ha comenzado a perder tramas debido a la congestión. Esta pérdida de tramas se indica mediante algún software de capas superiores (por ejemplo, el protocolo de control LAPF o TCP), y sirve como mecanismo de **señalización implícita**. Tal como se muestra en la Figura 12.4, las técnicas de recuperación de congestión operan en torno al punto B y en la región de congestión severa.

ITU-T y ANSI consideran la prevención de congestión mediante señalización explícita y la recuperación de congestión mediante señalización implícita como métodos complementarios del control de congestión en el servicio de retransmisión de tramas.

Tabla 12.4. Técnicas de control de congestión en retransmisión de tramas.

Técnica	Tipo	Función	Elementos clave
Control de rechazo	Estrategia de rechazo	Proporciona ayuda a la red sobre las tramas a rechazar	Bit DE
Notificación explícita de congestión hacia atrás	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	Bit BECN o mensaje CLLM
Notificación explícita de congestión hacia adelante	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	Bit FECN
Notificación implícita de congestión	Recuperación de congestión	Un sistema final infiere la existencia de congestión a partir de la pérdida de tramas	Números de secuencia en las PDU de capas superiores

GESTIÓN DE LA TASA DE TRÁFICO

Como último método, una red de retransmisión de tramas debe descartar tramas para combatir la congestión, no avisando de este hecho. Dado que los gestores de tramas en la red disponen de una cantidad finita de memoria para la puesta en cola de las tramas (Figura 12.2), es posible la saturación de una cola, siendo por tanto necesario el rechazo de las tramas más recientes u otras tramas.

La forma más sencilla de luchar contra la congestión es que la red de retransmisión de tramas rechace tramas arbitrariamente, independientemente del origen de una trama dada. En este caso, dado que no importa la limitación, la mejor estrategia para cualquier sistema final individual consiste en transmitir tramas tan rápido como sea posible, lo cual, claro está, empeora la congestión.

Para mejorar la reserva de los recursos, el servicio de retransmisión de tramas incluye el concepto de tasa de información contratada (CIR). Este parámetro es una velocidad, en bits por segundo, que acuerda la red para dar soporte a una conexión particular en modo trama. Cualquier dato transmitido a una velocidad superior a la CIR es susceptible de ser rechazado cuando se produce congestión. A pesar del uso de término *contratado* no existe garantía de que se alcance la CIR, pudiéndose ver forzada la red a proporcionar un servicio menor a la CIR para una conexión dada en caso de congestión extrema. Sin embargo, cuando llega la hora de descartar tramas, la red decidirá eliminar las tramas de aquellas conexiones que excedan su CIR antes de descartar tramas que respeten la CIR contratada.

En teoría, cada nodo de retransmisión de tramas debería gestionar sus recursos de manera que la suma de las CIR de todas las conexiones de todos los sistemas finales conectados al nodo no supere la capacidad del mismo. Además, la suma de las CIR no debería superar la velocidad de datos física de la interfaz usuario-red, conocida como tasa o velocidad de acceso. La limitación impuesta por la velocidad de acceso se puede expresar como sigue:

$$\sum_i \text{CIR}_{i,j} \leqslant \text{VelocidadAcceso}_j \tag{12.1}$$

donde

$\text{CIR}_{i,j}$ = tasa de información contratada para la conexión i del canal j
VelocidadAcceso_j = velocidad de datos del canal de acceso de usuario i, entendiendo por canal un canal TDM de velocidad fija entre el usuario y la red

La consideración de la capacidad del nodo puede provocar la selección de valores menores para algunas de las CIR.

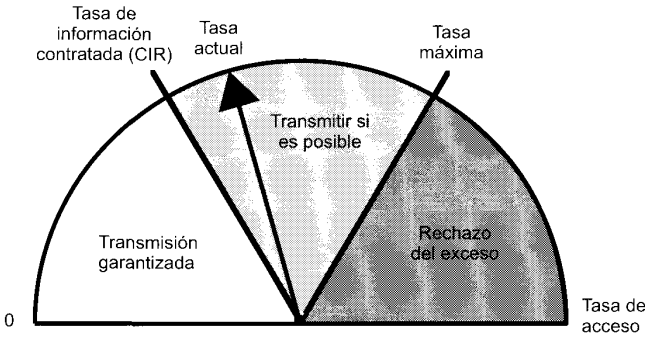


Figura 12.12. Funcionamiento de la CIR.

Para conexiones de retransmisión de tramas permanentes, la CIR de cada conexión se puede establecer en el momento en que se acepta dicha conexión entre el usuario y la red. Para conexiones conmutadas, el parámetro CIR se negocia en la fase de configuración del protocolo de control de llamadas.

La CIR provee de un mecanismo de discriminación acerca de qué tramas rechazar cuando se produce congestión. La discriminación se indica mediante el uso del bit de conveniencia de rechazo (DE) en las tramas LAPF (Figura 11.18). El gestor de tramas al que se conecta la estación del usuario realiza una función medidora (Figura 12.12). Si el usuario está enviando datos en una cantidad inferior a la CIR, el gestor de tramas entrantes no altera el bit DE; si, por contra, la velocidad excede la CIR, el gestor de tramas entrantes activa el bit DE en las tramas en exceso y las transmite, de modo que estas tramas pueden ser procesadas o, si se produce congestión, rechazadas. Finalmente, se define una velocidad de transmisión máxima de manera que cualquier trama por encima del máximo es descartada cuando llega al gestor de tramas.

La CIR, por sí misma, no proporciona demasiada flexibilidad en la gestión de las tasas de tráfico. En la práctica, un gestor de tramas mide el tráfico sobre cada conexión lógica durante un intervalo de tiempo dado, y después toma la decisión en base a la cantidad de datos recibidos durante el intervalo. Son necesarios dos parámetros adicionales, asignados en el caso de conexiones permanentes y negociados para conexiones conmutadas:

- **Tamaño de ráfaga contratado (B_c):** es la máxima cantidad de datos que la red acuerda transmitir, en condiciones normales, en un intervalo de medida T. Estos datos pueden ser o no contiguos (es decir, pueden aparecer en una o en varias tramas).
- **Tamaño de ráfaga en exceso (B_e):** es la máxima cantidad de datos en exceso de B_c que intentará transmitir la red, en condiciones normales, en un intervalo de medida T. Estos datos no se contratan en el sentido de que la red no se compromete a proporcionarlos en condiciones normales. Dicho de otra forma, los datos que representan B_e se envían con menor probabilidad que los datos en B_c.

Las cantidades B_e y CIR están relacionadas. Dado que B_c es la cantidad contratada de datos que puede transmitir el usuario en un tiempo T y CIR es la velocidad a la que se pueden transmitir dichos datos, se tiene que:

$$T = \frac{B_c}{\text{CIR}} \tag{12.2}$$

En la Figura 12.13, basada en una figura de la recomendación I.370 de ITU-T, se ilustra la relación entre estos parámetros. La línea continua en cada gráfica representa el número acumulado de bits de información a través de una conexión desde el instante de tiempo $T = 0$. La línea discontinua rotulada con «tasa de acceso» representa la velocidad de datos del canal correspondiente a esta conexión. La

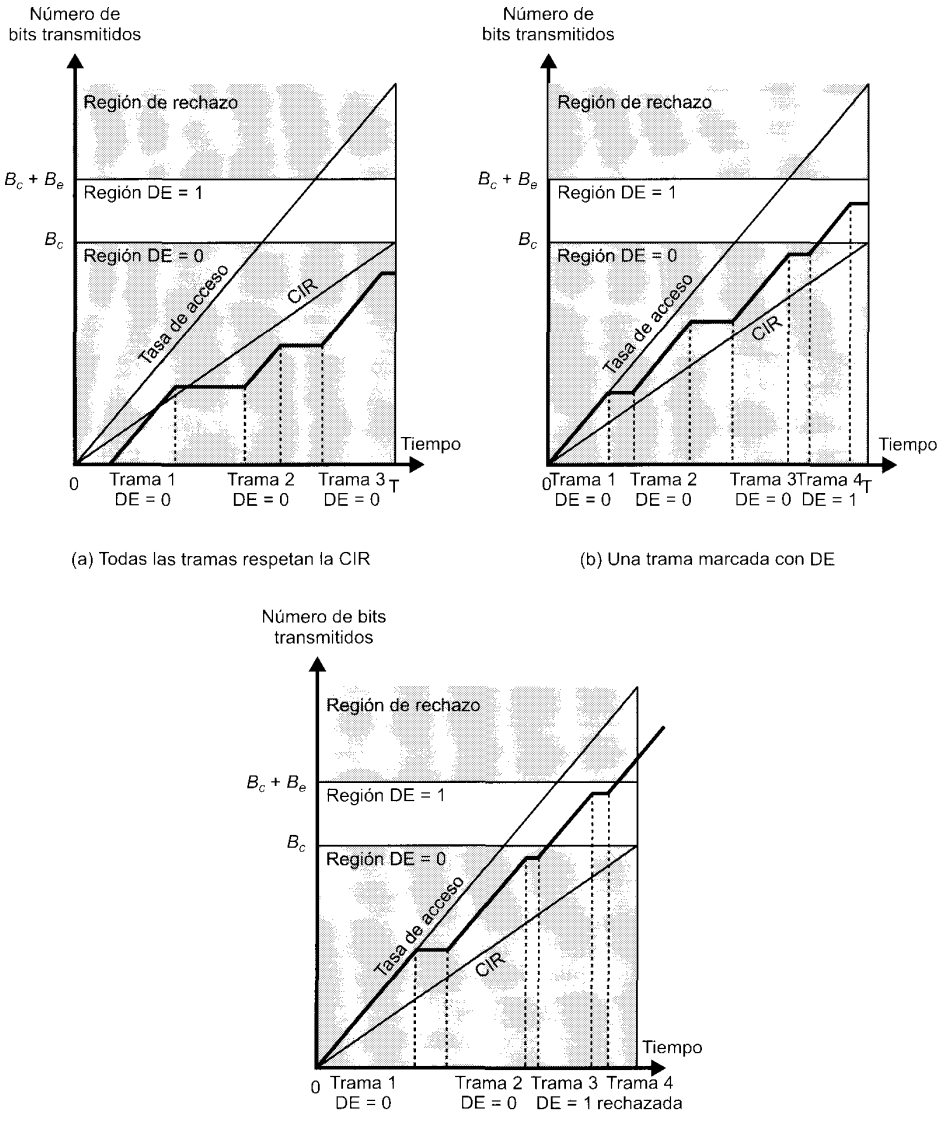


Figura 12.13. Ilustración de las relaciones entre los parámetros de congestión.

línea discontinua rotulada con «CIR» es la tasa de información contratada en el intervalo de medida T. Obsérvese que cuando se va a transmitir una trama, la línea continua es paralela a la línea de tasa de acceso; cuando se transmite una trama a través de un canal, éste se dedica a la transmisión de dicha trama. Cuando no hay tramas que transmitir, la línea continua es horizontal.

En la parte (a) de la Figura 12.13 se muestra un ejemplo en el que se transmiten tres tramas durante el intervalo de medida, y el número total de bits en las tres tramas es menor que B_c. Fijémonos en el

hecho de que durante la transmisión de la primera trama la velocidad de transmisión real supera temporalmente la CIR. Esto no tiene consecuencias, ya que el gestor de tramas está relacionado sólo con el número acumulado de bits transmitidos durante el intervalo completo. En la parte (b) de la figura, la última trama transmitida durante el intervalo provoca que el número acumulado de bits transmitidos supere B_c, por lo que el gestor de tramas activa el bit DE de la trama. En la parte (c) de la figura, la tercera trama excede B_c y se marca para su potencial rechazo, mientras que la cuarta trama excede $B_c + B_e$ y es descartada.

PREVENCIÓN DE CONGESTIÓN MEDIANTE SEÑALIZACIÓN EXPLÍCITA

Es deseable hacer tanto uso como sea posible de la capacidad disponible en una red de retransmisión de tramas para reaccionar de manera adecuada y controlada ante la congestión. Éste es el objetivo de las técnicas de prevención explícita de congestión. En términos generales, para llevar a cabo esta prevención, la red alerta a los sistemas finales acerca del aumento de la congestión en la red, de modo que éstos toman las medidas oportunas para reducir la carga introducida en la red.

Mientras se desarrollaban los estándares de prevención explícita de congestión, se consideraban dos estrategias generales [BERG91]. Algunos creían que la congestión se producía siempre de forma lenta y casi siempre en los nodos de salida. Otros observaron casos en los que la congestión aumentaba muy rápidamente en los nodos intermedios, precisándose acciones decisivas rápidas para prevenir la congestión de la red. Veremos que estas aproximaciones se corresponden, respectivamente, con las técnicas de prevención explícita de congestión hacia adelante y hacia atrás.

En la señalización explícita se usan dos bits en el campo de direcciones de cada trama, pudiendo ser activado cada uno de ellos por cualquier gestor de tramas que detecte la congestión. Si un gestor de tramas recibe una trama en la que uno de estos bits o los dos están activados, no debe desactivar los bits antes de retransmitir la trama. Así pues, los bits constituyen señales desde la red hacia el usuario final. Estos dos bits son:

- **Notificación explícita de congestión hacia atrás (BECN):** notifica al usuario acerca de la conveniencia de poner en marcha los procedimientos para evitar la congestión allí donde son aplicables para el tráfico en dirección opuesta a la de la trama recibida. Indica que las tramas que transmita el usuario a través de esta conexión lógica pueden encontrar recursos congestionados.
- **Notificación explícita de congestión hacia adelante (FECN):** notifica al usuario acerca de la conveniencia de poner en marcha los procedimientos para evitar la congestión allí donde son aplicables para el tráfico en la misma dirección que la de la trama recibida. Indica que la trama, sobre su conexión lógica, ha encontrado recursos congestionados.

Veamos cómo se usan estos bits por parte de la red y del usuario. En primer lugar, para la **respuesta de la red,** es necesario que cada gestor de tramas supervise el comportamiento de sus colas. Si el tamaño de éstas comienza a crecer de forma peligrosa, se deberían activar los bits FECN o BECN, o una combinación de ellos, para tratar de reducir el flujo de tramas a través del gestor de tramas. La elección de los bits FECN o BECN puede estar determinada por el hecho de que los usuarios finales de una conexión lógica dada estén preparados para responder a uno o al otro, lo cual se puede definir en el momento de la configuración. Si la congestión se hace más seria se podría notificar a todas las conexiones lógicas a través de un gestor de tramas. En las etapas más tempranas de la congestión, el gestor de tramas podría notificarlo sólo a aquellos usuarios cuyas conexiones generan la mayor parte del tráfico.

La **respuesta de usuario** se determina en base a la recepción de las señales BECN o FECN. El procedimiento más sencillo consiste en responder a la señal BECN: el usuario simplemente reduce la velocidad a la que transmite las tramas hasta que la señal cesa. La respuesta a la señal FECN es más compleja, ya que es necesario que el usuario notifique a su usuario paritario sobre esa conexión para que reduzca su flujo de tramas. Las funciones centrales usadas en el protocolo de retransmisión de tramas no contemplan esta notificación, por lo que debe ser realizada en una capa superior, como la de transporte. El control de flujo se podría también complementar con el protocolo de control LAPF o con algún otro

protocolo de control de enlace implementado encima de la subcapa de retransmisión de tramas. El protocolo de control LAPF es especialmente útil dado que incluye una mejora a LAPD que permite al usuario ajustar el tamaño de la ventana.

12.8. LECTURAS RECOMENDADAS

En [YANG95] se lleva a cabo una revisión exhaustiva de las técnicas de control de congestión. Por su parte, [JAIN90] y [JAIN92] proporcionan una discusión excelente acerca de los requisitos del control de congestión, de los distintos enfoques que se pueden hacer y acerca de distintas consideraciones sobre prestaciones.

[GARR96] presenta una exposición razonada de las clases de servicios ATM y discute las implicaciones de cada una de ellas en la gestión de tráfico. En [MCDY99] se realiza una descripción detallada del control de tráfico en ATM para los servicios CBR y VBR. Por su parte, los textos [SCHW96] y [PITT96] constituyen sendos excelentes tratamientos de las características y prestaciones del tráfico ATM.

En [CHEN96] se ofrece una buena revisión del servicio ABR en contraposición con los servicios CBR y VBR y describe el mecanismo de control de tráfico. [JAIN96] proporciona una explicación detallada del comportamiento de sistemas emisores y receptores en la transmisión de celdas de datos y celdas RM. En [ARUL96] se presentan de forma extensa los esquemas de reserva de capacidad para el servicio ABR. [SAIT96] constituye una discusión útil acerca de las implicaciones que sobre las prestaciones tienen las distintas componentes del mecanismo de control de tráfico ABR. Otros dos análisis de prestaciones de interés se pueden encontrar en [BONO95] y [OSHA95].

Finalmente, en [CHEN89] y [DOSH88] se presenta un interesante estudio de cuestiones relativas al control de congestión en retransmisión de tramas.

ARUL96 Arulambalam, A.; Chen, X.; y Ansari, N. «Allocating Fair Rates for Available Bit Rate Service in ATM Networks.» *IEEE Communications Magazine*, November 1996.

BONO95 Bonomi, F., y Fendick, K. «The Rate-Based Flow Control Framework for the Available Bit Rate ATM Service.» *IEEE Network*, March/April 1995.

CHEN89 Chen, K.; Ho, K.; y Saksena, V. «Analysis and Design of a Highly Reliable Transport Architecture for ISDN Frame-Relay Networks.» *IEEE Journal on Selected Areas in Communications*, October 1989.

CHEN96 Chen, T.; Liu, S.; y Samalam, V. «The Available Bit Rate Service for Data in ATM Networks.» *IEEE Communications Magazine*, May 1996.

DOSH88 Doshi, B., y Nguyen, H. «Congestion Control in ISD Frame-Relay Networks.» *AT&T Technical Journal*, November/December 1988.

GARR96 Garrett, M. «A Service Architecture for ATM: From Applications to Scheduling.» *IEEE Network*, May/June 1996.

JAIN90 Jain, R. «Congestion Control in Computer Networks: Issues and Trends.» *IEEE Network Magazine*, May 1990.

JAIN92 Jain, R. «Myths About Congestion Management in High-Speed Networks.» *Internetworking: Research and Experience*, Volume 3, 1993.

JAIN96 Jain R., et al. «Source Behavior for ATM ABR Traffic Management: An Explanation. *IEEE Communications Magazine*, November 1996.

MCDY99 McDysan, D., y Spohn, D. *ATM: Theory and Application.* New York: McGraw-Hill, 1999.

OSHA95 Oshaki, H., et al. «Rate-Based Congestion Control for ATM Networks.» *Computer Communication Review*, April 1995.

PITT96 Pitts, J., y Schormans, J. *Introduction to ATM Design and Performance*. New York: Wiley, 1996.

SAIT96 Saito, J., et al. «Performance Issues in Public ABR Service.» *IEEE Communications Magazine*, November 1996.

SCHW96 Schwartz, M. *Broadband Integrated Networks*. Upper Saddle River, NJ: Prentice Hall PTR, 1996.

YANG95 Yang, C., y Reddy, A. «A Taxonomy for Congestion Control Algorithms in Packet Switching Networks.» *IEEE Network*, July/August 1995.

12.9. PROBLEMAS

12.1. Una técnica de control de congestión propuesta es la conocida como control isarrítmico. En este método se fija un número total de tramas en tránsito mediante la inserción en la red de un número fijo de permisos. Estos permisos circulan de forma aleatoria a través de la red de retransmisión de tramas. Cuando un gestor de tramas desea transmitir una trama procedente de un usuario conectado a él, debe primero capturar y destruir un permiso. Una vez que la trama se ha enviado hacia el usuario destino por el gestor de tramas al que éste se encuentra conectado, dicho gestor restituye el permiso. Indique tres problemas potenciales de esta técnica.

12.2. En el estudio de los efectos de latencia/velocidad presentado en la Sección 12.5 se vio un ejemplo en el que se transmitían 7 megabits antes de que el emisor pudiese reaccionar. ¿Es que no es una técnica de control de flujo de ventana deslizante, como la descrita para HDLC, diseñada para solucionar los elevados retardos de propagación?

12.3. Considere la red de retransmisión de tramas mostrada en la Figura 12.14. C es la capacidad de un enlace en tramas por segundo. El nodo A presenta una carga constante de 0,8 tramas por segundo con destino a A′. Por su parte, el nodo B presenta una carga λ hacia B′. El nodo S dispone de un conjunto de memorias temporales comunes usadas tanto para el tráfico hacia A′ como para el tráfico hacia B′. Cuando se llena la memoria temporal, las tramas se rechazan y se retransmiten posteriormente por el usuario origen. S tiene una capacidad de 2. Dibuje el ren-

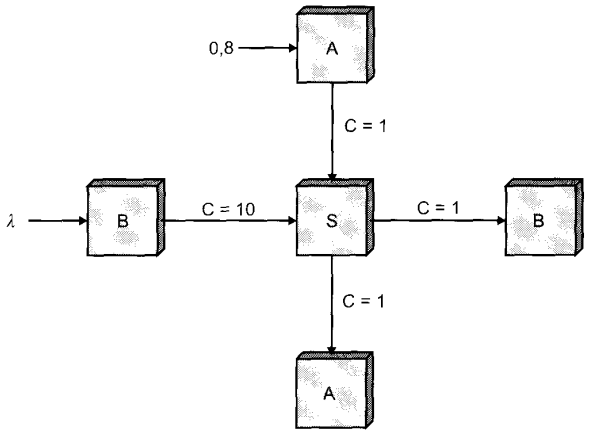


Figura 12.14. Red de nodos.

dimiento total (es decir, la suma de tráfico entre A y A′ y entre B y B′) en función de λ. ¿Qué fracción de rendimiento corresponde a tráfico A − A′ para $\lambda > 1$?

12.4. Compare la velocidad sostenible de celdas y la tolerancia a la aparición de ráfagas, tal como se usan en redes ATM, con la tasa de información contratada y el tamaño de ráfaga en exceso, tal como se usan en redes de retransmisión de tramas. ¿Representan los respectivos términos los mismos conceptos?

PARTE IV

REDES DE ÁREA LOCAL

CUESTIONES A TRATAR EN LA CUARTA PARTE

La tendencia de las redes de área local (LAN) implica el uso de medios de transmisión compartido o conmutación compartida, para lograr velocidades de transmisión de datos altas en distancias relativamente cortas. Varios conceptos clave se presentan por sí mismos. Uno es la elección de medio de transmisión. Así como el cable coaxial ha sido el medio tradicionalmente más usado, las instalaciones LAN actuales enfatizan el uso de pares trenzados o fibra óptica. En caso de pares trenzados, se necesitan esquemas de codificación eficientes para lograr alta velocidad de transmisión a través del medio. Las redes LAN inalámbricas también están consiguiendo un importante incremento. Otro problema de diseño es cómo realizar el control de acceso. Con un medio o conmutador compartidos resulta necesario algún mecanismo para regular el acceso al medio de forma eficiente y rápida. Los dos esquemas más comunes son CSMA/CD tipo Ethernet y anillo con paso de testigo.

ESQUEMA DE LA PARTE IV

CAPÍTULO 13. TECNOLOGÍA LAN

La tecnología esencial subyacente a todas las formas de LAN incluye: topología, medio de transmisión, y técnica de control de acceso al medio. El Capítulo 13 analiza los dos primeros elementos citados. Usualmente se utiliza una de estas cuatro topologías: bus, árbol, anillo o estrella. El medio de transmisión más común para interconexión en redes locales es par trenzado (blindado, o no), cable coaxial (en banda base y banda ancha), fibra óptica, e inalámbrico (microondas o infrarrojo). En el capítulo se describen estas topologías y medios de transmisión así como sus combinaciones más prometedoras.

La creciente difusión de las redes LAN ha conducido a incrementar la necesidad de interconexión de LAN, entre ellas y con redes WAN. El Capítulo 13 también discute un dispositivo clave usado para interconectar redes LAN: el puente.

CAPÍTULO 14. SISTEMAS LAN

El Capítulo 14 examina en detalle las topologías, medios de transmisión, y protocolos MAC de los sistemas LAN usuales más importantes: todos ellos han sido definidos en documentos de estandarización. El más importante de ellos es Ethernet, que se ha desarrollado en versiones de 10 Mbps, 100 Mbps, y 1 Gbps. Después el capítulo examina las LAN de paso de testigo, incluyendo la IEEE 802.5 de anillo y FDI. También se analizan las redes LAN normalizadas de fibra óptica e inalámbricas.

CAPÍTULO 13

Tecnologías LAN

- Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo. Las topologías usadas para LAN son anillo, bus, árbol y estrella. Las topologías en bus y en árbol son secciones pasivas de cable a las que se encuentran conectadas las estaciones, de modo que la transmisión de una trama por parte de una estación puede ser escuchada por cualquier otra estación. Una LAN en anillo consiste en un bucle cerrado de repetidores que permite la circulación de los datos alrededor del anillo. Un repetidor puede funcionar también como un punto de conexión de dispositivo, realizándose la transmisión generalmente en forma de tramas. Por su parte, una red LAN en estrella incluye un nodo central al que se conectan las estaciones.
- Los medios de transmisión empleados en redes LAN son par trenzado, cable coaxial, fibra óptica y medios inalámbricos. Por lo que se refiere a los pares trenzados, éstos pueden ser tanto apantallados como no apantallados, utilizándose para la transmisión inalámbrica infrarrojos o microondas.
- Se ha definido un conjunto de estándares LAN que especifica un rango de velocidades distintas y comprende todas las topologías y medios de transmisión mencionados. Los estándares IEEE 802 y FDDI (interfaz de datos distribuida de fibra) están ampliamente aceptados y la mayor parte de los productos existentes en el mercado se ajusta a uno de ellos.
- En la mayoría de los casos, un organismo cuenta con varias LAN que precisan estar interconectadas. La solución más sencilla para satisfacer este requisito es el uso de puentes.

A continuación se examinan las redes de área local (LAN, local area networks). Mientras que las redes de área amplia o extensa pueden ser tanto públicas como privadas, las LAN son propiedad generalmente de un organismo que utiliza la red para interconectar equipos. Las redes LAN tienen mucha mayor capacidad que las de área amplia, permitiendo el transporte de un tráfico de comunicaciones interno generalmente superior.

En la Figura 1.3 se mostró un sencillo ejemplo de red LAN que resaltaba algunas de las características de este tipo de redes. Todos los dispositivos están conectados a un medio de transmisión compartido, de forma que una transmisión realizada desde un dispositivo se puede recibir en los restantes dispositivos conectados a la red. Las LAN han proporcionado tradicionalmente velocidades en torno al rango de 1 a 20 Mbps, las cuales, aunque elevadas, resultan cada vez más inadecuadas debido a la proliferación de dispositivos, al crecimiento de aplicaciones multimedia y al creciente uso de la arquitectura cliente/servidor. Así pues, los trabajos recientes se han centrado en el desarrollo de redes LAN de alta velocidad con velocidades comprendidas entre 100 Mbps y 1 Gbps.

Este capítulo inicia el estudio de redes LAN[1] con una discusión sobre sus campos de aplicación. A continuación se describe la arquitectura de protocolos comúnmente usada en la implementación de este tipo de redes. Esta arquitectura es también la base de trabajos de normalización. Nuestro estudio trata los niveles físico, de control de acceso al medio (MAC) y de control de enlace lógico (LLC).

Los aspectos tecnológicos principales que determinan la naturaleza de una red LAN o una MAN son:

- Topología.
- Medio de transmisión.
- Técnica de control de acceso al medio.

[1] Por comodidad, el capítulo habla a veces de redes LAN para referirse tanto a redes LAN como a redes de área metropolitana (MAN). El contexto aclarará si nos referimos sólo a LAN o a LAN y MAN.

Este capítulo presenta las topologías y medios de transmisión más comúnmente usados en redes LAN. El control de acceso se trata de forma breve, estudiándose con mayor detalle en el Capítulo 14. Por su parte, el concepto de puente («bridge»), que juega un papel crítico en la amplitud de la cobertura de una red LAN, se discutirá en la Sección 13.7.

13.1. APLICACIONES DE REDES LAN

La variedad de aplicaciones de las redes LAN es amplia. En esta sección se ofrece una breve discusión acerca de algunas de las áreas de aplicación generales más importantes de este tipo de redes.

LAN DE COMPUTADORES PERSONALES

Una configuración común de red LAN es aquella que consta de computadores personales. Dado el relativo bajo coste de estos sistemas, algunos gerentes/administradores de organismos adquieren frecuentemente computadores personales para aplicaciones departamentales tales como hojas de cálculo y herramientas de gestión de proyectos, y acceso Internet.

Pero un conjunto de procesadores departamentales no cubren todas las necesidades de un organismo, siendo también necesarios servicios de procesamiento central. Algunos programas, como los modelos de predicción económica, son demasiado grandes para poder ejecutarse en un computador pequeño. Ficheros de datos corporativos de gran tamaño, como los correspondientes a contabilidad y nóminas, precisan de un servicio centralizado al tiempo que deberían ser accesibles por parte de distintos usuarios. Además, hay otros tipos de ficheros que, aunque especializados, deben compartirse entre diferentes usuarios. Existen también razones de peso para llevar a cabo la conexión de estaciones de trabajo inteligentes individuales no sólo a un servicio central sino también entre sí. Los miembros del equipo de un proyecto o de un organismo necesitan compartir trabajo e información, siendo digitalmente la forma más eficiente para hacerlo.

Algunos recursos caros, tales como un disco o una impresora láser, pueden ser compartidos por todos los usuarios de una LAN departamental. Además, la red puede servir de nexo entre servicios de red corporativos mayores; por ejemplo, la compañía puede disponer de una LAN a nivel de edificio y de una red privada de área amplia. Un servidor de comunicaciones puede proporcionar acceso controlado a estos recursos.

El uso de redes LAN para dar soporte a computadores personales y estaciones de trabajo se ha convertido en un hecho casi universal en todo tipo de organizaciones. Incluso aquellos lugares en que aún existe una fuerte dependencia de un computador principal, se ha transferido parte de la carga de procesamiento a redes de computadores personales. Quizá el mejor ejemplo de la forma en que se utiliza un computador personal sea la implementación de aplicaciones cliente/servidor.

Un requisito importante en redes de computadores personales es el bajo coste. En particular, el coste de la conexión a la red debe ser significativamente menor que el del dispositivo conectado. Así, para un computador personal típico es deseable que el coste de conexión sea del orden de decenas de miles de pesetas, aceptándose costes de conexión mayores para dispositivos más caros, como estaciones de trabajo de altas prestaciones. En cualquier caso, esto sugiere que la velocidad de la red puede estar limitada, ya que, en general, el coste es superior cuanto mayor sea la velocidad.

REDES DE RESPALDO Y DE ALMACENAMIENTO

Las redes de respaldo («backend») se utilizan para interconectar grandes sistemas tales como computadores centrales, supercomputadores, y dispositivos de almacenamiento masivo. El requisito principal en este caso es la transferencia elevada de datos entre un número limitado de dispositivos en un área redu-

cida, siendo también necesaria generalmente una alta fiabilidad. Entre sus características típicas se encuentran las siguientes:

- **Alta velocidad:** se precisan velocidades de 100 Mbps o más para satisfacer la demanda de alto volumen de tráfico.
- **Interfaz de alta velocidad:** las operaciones de transferencia de datos entre un gran sistema anfitrión y un dispositivo de almacenamiento masivo se realizan generalmente a través de interfaces de entrada/salida paralelo de alta velocidad en lugar de a través de interfaces de comunicaciones más lentas. Por tanto, el enlace físico entre la estación y la red debe ser de alta velocidad.
- **Acceso distribuido:** se necesita una técnica de control distribuido de acceso al medio (MAC) para permitir que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.
- **Distancia limitada:** generalmente las redes de soporte se emplean en salas de computadores o en un número reducido de habitaciones contiguas.
- **Número limitado de dispositivos:** el número de computadores principales y dispositivos de almacenamiento masivo caros existente en una sala de computadores es generalmente del orden de las decenas.

Generalmente, las redes de respaldo se encuentran en grandes compañías o en instalaciones de investigación con alto presupuesto en procesamiento de datos. Dada la escala referida, una pequeña diferencia en la productividad puede significar centenares de millones de pesetas.

Consideremos un lugar donde se hace uso de un computador principal dedicado, lo que implica una aplicación grande o un conjunto de aplicaciones. Si la carga crece el computador principal puede remplazarse por uno más potente, quizá por un sistema multiprocesador. En algunos lugares no basta con colocar un solo sistema dado que el crecimiento de la demanda supera el aumento de las prestaciones del equipamiento, por lo que se precisarán eventualmente varios computadores independientes. De nuevo, existen razones que fuerzan la interconexión de estos sistemas. El coste de la interrupción del sistema es alto, de modo que sería posible, fácil y rápido, trasladar las aplicaciones a sistemas de respaldo. Debe ser posible testar nuevos procedimientos y aplicaciones sin degradar el sistema de producción. Los ficheros de gran tamaño deben ser accesibles por parte de más de un computador. El equilibrado de la carga posibilitaría la maximización de la utilización y de las prestaciones.

Se puede observar que algunos de los requisitos principales para redes de salas de computadores son los contrarios a los de las LAN de computadores personales. Se requieren altas velocidades para poder trabajar adecuadamente, lo que implica generalmente la transferencia de bloques de datos de gran tamaño. Afortunadamente, aunque el coste del equipamiento para conseguir altas velocidades es alto, éste es razonable debido al coste mucho mayor de los dispositivos conectados.

Un concepto relacionado con el de red de respaldo es el de red de almacenamiento (SAN, storage area network). Una SAN es una red independiente para gestionar necesidades de almacenamiento.

La SAN desliga las tareas de almacenamiento de servidores específicos y crea un servicio de almacenamiento compartido a través de una red de alta velocidad. Entre el conjunto de dispositivos de almacenamiento de la red se pueden encontrar discos duros, unidades de cinta y dispositivos CD. La mayor parte de las SAN hace uso del canal de fibra descrito en el Capítulo 14.

REDES OFIMÁTICAS DE ALTA VELOCIDAD

Tradicionalmente, un entorno ofimático ha incluido una gran variedad de dispositivos con requisitos de transferencia de datos de baja-media velocidad. Sin embargo, están apareciendo nuevas aplicaciones en el entorno ofimático para las que resultan inadecuadas las limitadas velocidades (hasta 10 Mbps) de las LAN tradicionales. Así, los procesadores de imágenes de sobremesa han incrementado el flujo de datos de red en una cantidad sin precedentes, siendo ejemplos de estas aplicaciones los dispositivos fax, los procesadores de imágenes de documentos y los programas gráficos en computadores personales y esta-

ciones de trabajo. Considérese que una página típica con una resolución de 200 elementos de dibujo, o pels[2] (puntos blancos o negros), por pulgada (resolución adecuada pero no alta) genera 3.740.000 bits (8,5 pulgadas × 11 pulgadas × 40.000 pels por pulgada cuadrada). Incluso haciendo uso de técnicas de compresión, esto generará una carga tremenda. Además, la tecnología y el precio/prestaciones de los discos han evolucionado de forma que son comunes las capacidades de almacenamiento de sobremesa que superan 1 Gbyte. Estas nuevas demandas necesitan redes LAN de alta velocidad que puedan soportar el amplio número y mayor extensión geográfica de los sistemas ofimáticos en comparación con los sistemas existentes en salas de computadores.

LAN TRONCALES

El uso creciente de aplicaciones de procesamiento distribuido y de computadores personales ha provocado la necesidad de una estrategia LAN flexible. El soporte de comunicaciones de datos entre oficinas precisa de un servicio de red capaz de cubrir las distancias involucradas y de interconectar equipos situados en un mismo edificio (quizás grande) o en un conjunto de ellos. Aunque es posible desarrollar una sola LAN para interconectar todos los equipos de procesamiento de datos de una oficina, no es una alternativa plausible en la mayoría de los casos. Existen varios inconvenientes en una estrategia de una sola LAN:

- **Fiabilidad:** un servicio de interrupción, incluso de corta duración, en una LAN simple podría provocar un trastorno importante para los usuarios.
- **Capacidad:** una sola LAN se podría saturar cuando crezca a lo largo del tiempo el número de dispositivos conectados a la red.
- **Coste:** una tecnología de LAN simple no resulta óptima para los diversos requisitos de interconexión y comunicación. La existencia de un gran número de microcomputadores de bajo coste hace que el soporte de red para estos dispositivos sea también de bajo coste. Las redes LAN que admiten conexiones de muy bajo coste no son adecuadas para satisfacer los requisitos globales.

Una alternativa más atractiva consiste en el empleo de LAN de menor coste y capacidad en edificios o departamentos y llevar a cabo la interconexión de estas redes mediante una LAN de mayor capacidad. Esta última red se denomina LAN troncal o vertebral («backbone»).

13.2. ARQUITECTURA LAN

La arquitectura de una LAN se describe mejor en términos de una jerarquía de protocolos que organizan las funciones básicas de la misma. Esta sección comienza con una descripción de la arquitectura de protocolos estandarizada para redes LAN, que incluye las capas física, de control de acceso al medio y de control de enlace lógico. Cada una de estas capas se trata a continuación.

ARQUITECTURA DE PROTOCOLOS

Los protocolos definidos específicamente para la transmisión en redes LAN y MAN tratan cuestiones relacionadas con la transmisión de bloques de datos a través de la red. Según OSI, los protocolos de capas superiores (capas 3 o 4 y superiores) son independientes de la arquitectura de red y son aplicables a redes LAN, MAN y WAN. Así pues, el estudio de protocolos LAN está relacionado con las capas inferiores del modelo OSI.

---

[2] Un *elemento de dibujo*, o *pel*, es la muestra discreta más pequeña de una línea escaneada de un sistema facsímil, que sólo contiene información blanco-negro (no existe escala de grises). Por el contrario, un pixel es un elemento de dibujo que contiene información de escala de grises.

En la Figura 13.1 se relacionan los protocolos LAN de la arquitectura OSI (Figura 1.10). Esta arquitectura fue desarrollada por el comité IEEE 802 y ha sido adoptada por todas las organizaciones que trabajan en la especificación de los estándares LAN; es la referida como el modelo de referencia IEEE 802[3].

Desde abajo hacia arriba, la capa inferior del modelo de referencia IEEE 802 es la **capa física** del modelo OSI, e incluye funciones tales como:

- Codificación/decodificación de señales.
- Generación/eliminación de preámbulo (para sincronización).
- Transmisión/recepción de bits.

Además, la capa física del modelo 802 incluye una especificación del medio de transmisión y de la topología. Generalmente, esto se considera «debajo» de la capa inferior del modelo OSI; sin embargo, dado que la elección del medio de transmisión y la topología es crítica en el diseño de redes LAN, se incluye una especificación del medio.

Por encima de la capa física se encuentran las funciones asociadas a los servicios ofrecidos a los usuarios LAN. Entre ellas se encuentran las siguientes:

- En transmisión, ensamblado de datos en tramas con campos de dirección y de detección de errores.
- En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
- Control de acceso al medio de transmisión LAN.
- Interfaz con las capas superiores y control de errores y de flujo.

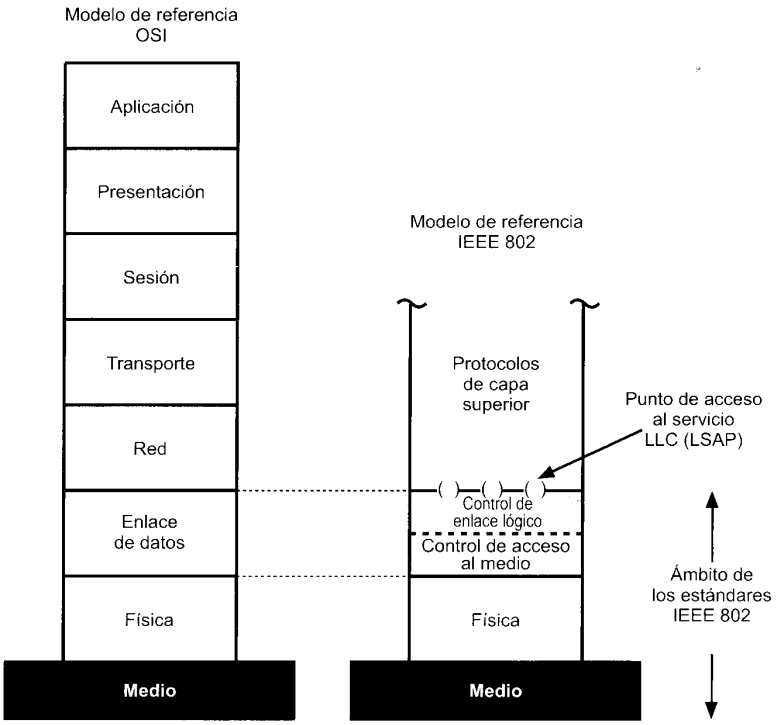


Figura 13.1. Capas del protocolo IEEE 802 en comparación con las del modelo OSI.

[3] Véase Apéndice 13A para una descripción del comité de normalización IEEE 802.

Estas funciones se asocian generalmente a la capa 2 de OSI. El conjunto de funciones del último punto de los cuatro indicados se agrupan en la capa de **control de enlace lógico** (**LLC**, logical link control), mientras que las funciones especificadas en los tres primeros puntos se tratan en una capa separada denominada **control de acceso al medio** (**MAC**, medium access control). Esta separación de funciones se debe a las siguientes razones:

- La lógica necesaria para la gestión de acceso a un medio compartido no se encuentra en la capa 2 de control de enlace de datos tradicional.
- Se pueden ofrecer varias opciones MAC para el mismo LLC.

En la Figura 13.2 se ilustra la relación existente entre los niveles de la arquitectura (comparar con la Figura 10.15). Los datos de nivel superior se pasan hacia abajo al nivel LLC, que añadé una cabecera de información de control dando lugar a una *unidad de datos de protocolo* (*PDU*, Protocol Data Unit) *LLC*. Esta información de control se utiliza para el funcionamiento del protocolo LLC. La PDU LLC se pasa a la capa MAC, que añade información de control al principio y al final del paquete creando una *trama MAC*. Una vez más es necesaria la información de control en la trama para el funcionamiento del protocolo MAC. Para situarnos en contexto, la figura muestra también el uso del protocolo TCP/IP y una capa de aplicación por encima de los protocolos LAN.

TOPOLOGÍAS

A continuación centraremos nuestro estudio en una introducción a las topologías LAN básicas para la capa física. Las topologías usuales en LAN son bus, árbol, anillo y estrella (Figura 13.3). El bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas; usaremos el término *bus* cuando las diferencias no sean importantes.

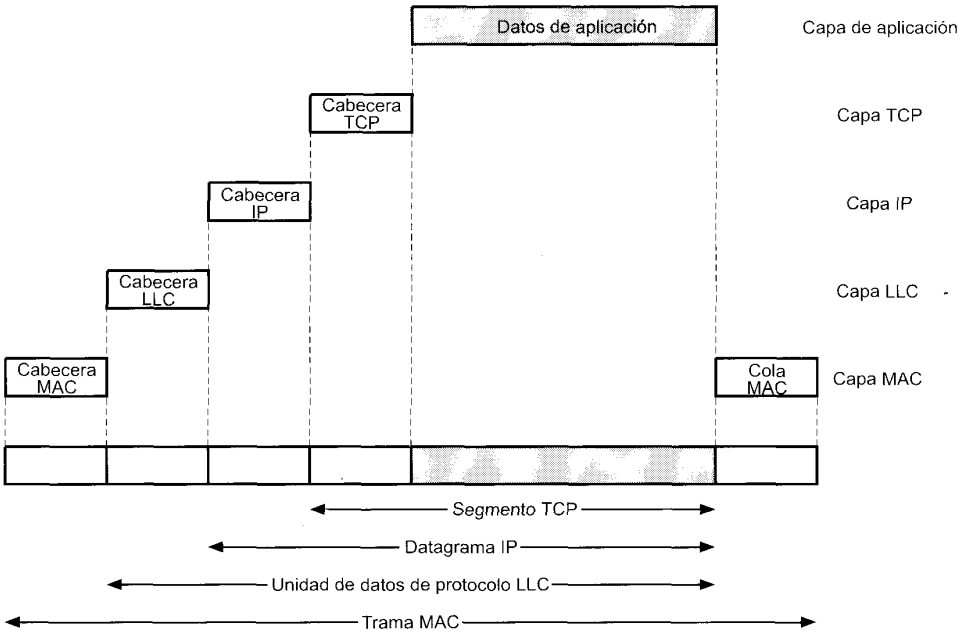


Figura 13.2. Protocolos LAN en contexto.

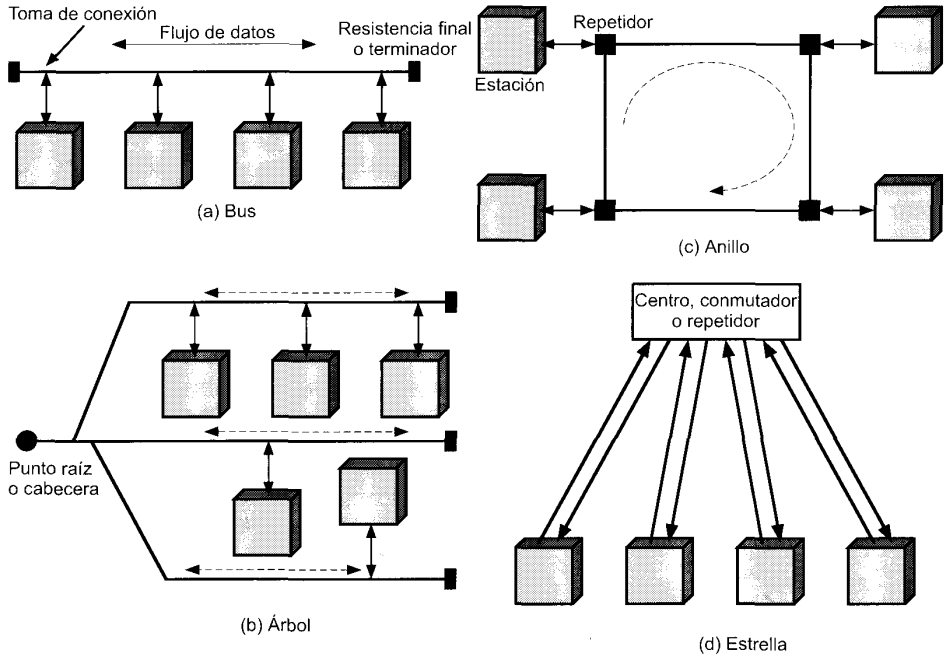


Figura 13.3. Topologías LAN.

Topologías en bus y en árbol

Ambas topologías se caracterizan por el uso de un medio multipunto. En el caso de la topología en bus, todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión («taps»), a un medio de transmisión lineal o bus. El funcionamiento *full-duplex* entre la estación y la toma de conexión permite la transmisión de datos a través del bus y la recepción de éstos desde aquél. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de estaciones. En cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.

La topología en árbol es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados, que comienza en un punto conocido como *raíz* o *cabecera* («headend»). Uno o más cables comienzan en el punto raíz, y cada uno de ellos puede presentar ramificaciones. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos. De nuevo, la transmisión desde una estación se propaga a través del medio y puede alcanzar al resto de estaciones.

Existen dos problemas en esta disposición. En primer lugar, dado que la transmisión desde una estación se puede recibir en las demás estaciones, es necesario algún método para indicar a quién va dirigida la transmisión. En segundo lugar, se precisa un mecanismo para regular la transmisión. Para ver la razón de este hecho hemos de comprender que si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas; también se puede considerar la situación en que una estación decide transmitir continuamente durante un largo periodo de tiempo.

Para solucionar estos problemas las estaciones transmiten datos en bloques pequeños llamados tramas. Cada trama consta de una porción de los datos que una estación desea transmitir además de una cabecera de trama que contiene información de control. A cada estación en el bus se le asigna una dirección, o identificador, única, incluyéndose en la cabecera la dirección destino de la trama.

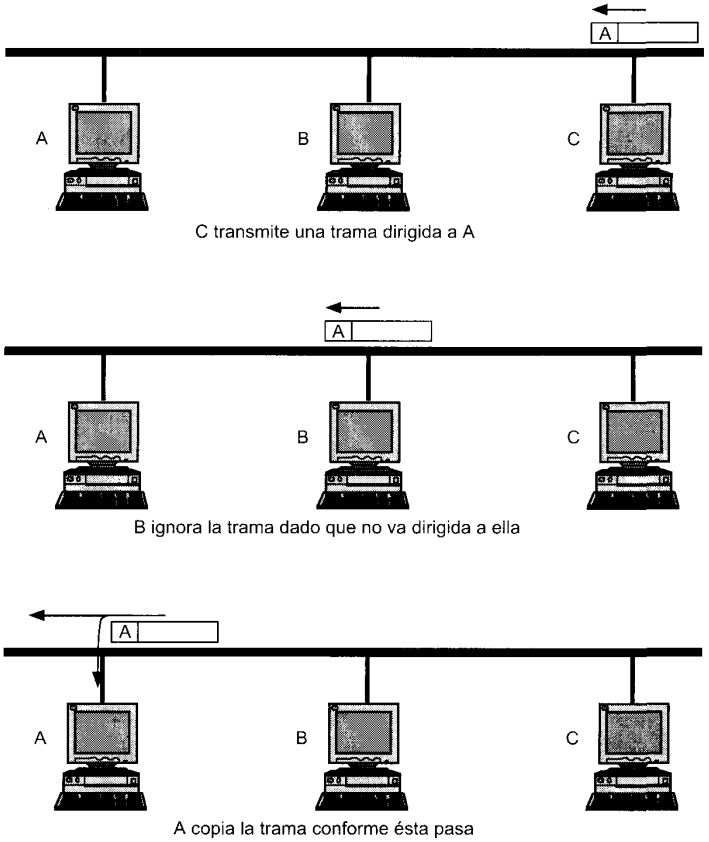


Figura 13.4. Transmisión de tramas en una LAN en bus.

En la Figura 13.4 se ilustra este esquema. En este ejemplo, la estación C desea transmitir una trama de datos a A, de modo que la cabecera de la trama incluirá la dirección de A. En la propagación de la trama a lo largo del bus, ésta atraviesa B, quien observa la dirección de destino e ignora la trama. A, por su parte, observa que la trama va dirigida a ella y copia los datos de ésta mientras que pasa.

La estructura de la trama resuelve el primer problema mencionado anteriormente: proporciona un mecanismo para indicar el receptor de los datos. También proporciona una herramienta básica para resolver el segundo problema, el control de acceso. En particular, las estaciones transmiten por turnos en forma cooperativa, lo que implica, como se verá más adelante, el uso de información de control adicional en la cabecera de las tramas.

En la topología en bus o en árbol no son necesarias acciones especiales para eliminar tramas del medio: cuando una señal alcanza el final de éste, es absorbida por el terminador.

Topología en anillo

En la topología en anillo, la red consta de un conjunto de *repetidores* unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo relativamente simple, capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos.

Los enlaces son unidireccionales; es decir, los datos se transmiten sólo en un sentido, de modo que éstos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario.

Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él.

Como en el caso de las topologías en bus y en árbol, los datos se transmiten en tramas. Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama, mientras ésta la atraviesa, en una memoria temporal local. La trama continúa circulando hasta que alcanza de nuevo la estación origen, donde es eliminada del medio (Figura 13.5).

Dado que el anillo es compartido por varias estaciones, se necesita una técnica de control de acceso al medio para determinar cuándo puede insertar tramas cada estación.

Topología en estrella

En redes LAN con topología en estrella cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción.

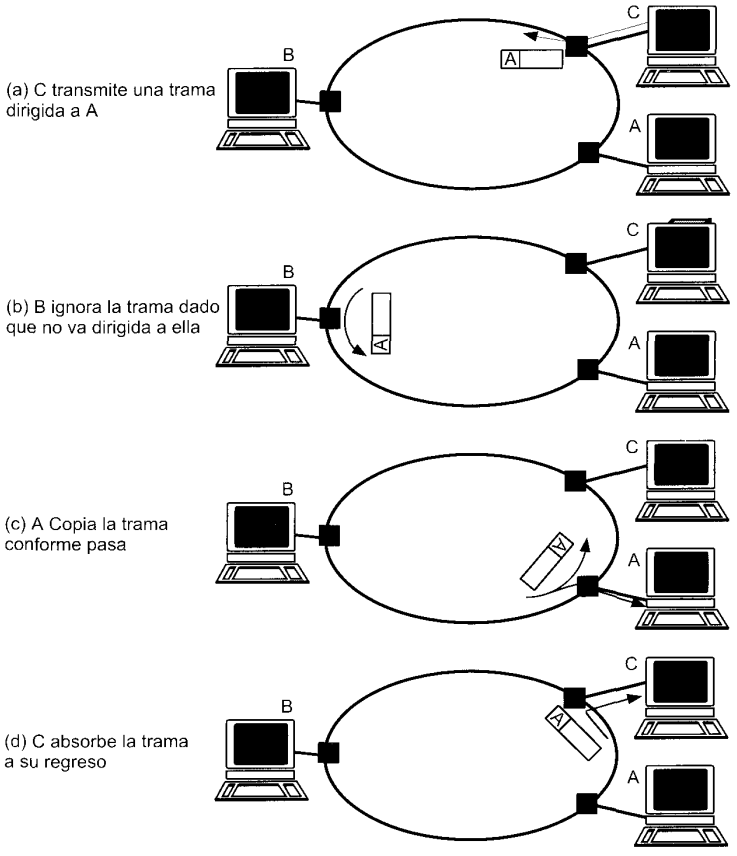


Figura 13.5. Transmisión de tramas en una LAN en anillo.

En general existen dos alternativas para el funcionamiento del nodo central. Una es el funcionamiento en modo de difusión, en el que la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central.

En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus: una transmisión desde cualquier estación es recibida por el resto de estaciones, y sólo puede transmitir una estación en un instante de tiempo dado.

Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

CONTROL DE ACCESO AL MEDIO

Todas las LAN y MAN constan de un conjunto de dispositivos que deben compartir la capacidad de transmisión de la red, de manera que se requiere algún método de control de acceso al medio con objeto de hacer un uso eficiente de esta capacidad. Ésta es la función del protocolo de control de acceso al medio (MAC).

Los parámetros clave en cualquier técnica de control de acceso al medio son dónde y cómo. *Dónde* se refiere a si el control se realiza de forma centralizada o distribuida. En un esquema centralizado se diseña un controlador con autoridad para conceder el acceso a la red, de modo que una estación que desee transmitir debe esperar hasta que se le conceda permiso por parte del controlador. En una red descentralizada, las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán. Un esquema centralizado presenta ciertas ventajas, entre las que se encuentran:

- Puede mejorar el control de acceso proporcionando prioridades, rechazos y capacidad garantizada.
- Permite el uso de una lógica de acceso relativamente sencilla en cada estación.
- Resuelve problemas de coordinación distribuida entre entidades paritarias.

Las principales desventajas de los esquemas centralizados son:

- Genera un punto de falla; es decir, existe un punto en la red tal si se produce un fallo en él, fallará toda la red.
- Puede actuar como un cuello de botella, reduciendo las prestaciones.

Los pros y contras de los esquemas distribuidos son los contrarios de los puntos anteriores.

El segundo parámetro, *cómo*, viene impuesto por la topología y es un compromiso entre factores tales como el coste, las prestaciones y la complejidad. En general, podemos clasificar las técnicas de control de acceso como síncronas o asíncronas. Con las técnicas síncronas se dedica una capacidad dada a la conexión. Ésta es la misma aproximación usada en conmutación de circuitos, multiplexación por división en frecuencias (FDM) y multiplexación por división en el tiempo síncrona (TDM). Estas técnicas no son óptimas en redes LAN y MAN dado que las necesidades de las estaciones son impredecibles. Es preferible, por tanto, tener la posibilidad de reservar capacidad de forma asíncrona (dinámica) más o menos en respuesta a solicitudes inmediatas. La aproximación asíncrona se puede subdividir en tres categorías: rotación circular, reserva y competición.

Rotación circular

Con la técnica de rotación circular a cada estación se le da la oportunidad de transmitir, ante lo que la estación puede declinar la proposición o puede transmitir sujeta a un límite superior, especificado generalmente en términos de cantidad de datos a transmitir o tiempo para ello. En cualquier caso, cuando la estación termina debe ceder el turno de transmisión a la siguiente estación en la secuencia lógica. El

control de secuencia puede ser centralizado o distribuido, siendo el método de sondeo un ejemplo de técnica centralizada.

Cuando varias estaciones disponen de datos a transmitir durante un largo periodo de tiempo, las técnicas de rotación circular pueden resultar muy eficientes. En cambio, si sólo unas pocas estaciones disponen de datos a transmitir durante un extenso periodo de tiempo existirá un coste considerable en el paso del turno entre estaciones, ya que la mayoría de ellas no transmiten datos sino que solamente ceden el turno. En estas circunstancias pueden ser preferibles otras técnicas dependientes de si el tráfico de datos es a ráfagas o continuo. El tráfico continuo se caracteriza por transmisiones largas y razonablemente continuas; algunos ejemplos son comunicación de voz, telemetría y transferencia de ficheros grandes. Por su parte, el tráfico a ráfagas se caracteriza por transmisiones cortas y esporádicas como en el caso de tráfico interactivo terminal-estación.

Reserva

Las técnicas de reserva son adecuadas para tráfico continuo. Generalmente en estas técnicas se divide el tiempo en ranuras, como en el caso de la técnica TDM síncrona. Una estación que desea transmitir reserva futuras ranuras para un largo, incluso indefinido, periodo de tiempo. Una vez más, las reservas se pueden llevar a cabo de forma centralizada o distribuida.

Contención

Usualmente, las técnicas de contención son apropiadas para tráfico a ráfagas. Con estas técnicas no se realiza control para determinar de quién es el turno, sino que todas las estaciones compiten en una forma que puede ser, como veremos, bastante dura y caótica. Estas técnicas son necesariamente de naturaleza distribuida, radicando su principal ventaja en el hecho de que son sencillas de implementar y eficientes en condiciones de baja o moderada carga; sin embargo, para algunas de estas técnicas, las prestaciones tienden a deteriorarse bajo condiciones de alta carga.

Aunque tanto las técnicas de reserva centralizadas como las distribuidas se implementan algunos productos LAN, las más comunes son las técnicas de rotación circular y de competición.

La discusión anterior resulta un poco abstracta, clarificándose cuando se presenten técnicas específicas en el Capítulo 14. Para referencias futuras, en la Tabla 13.1 se listan los protocolos MAC que se definen en las normas LAN y MAN.

Formato de trama MAC

La capa MAC recibe un bloque de datos de la capa LLC y debe realizar funciones relacionadas con el acceso al medio y la transmisión de datos. Como en otras capas de la arquitectura de protocolos, MAC

Tabla 13.1. Técnicas de control de acceso al medio normalizadas.

	Topología en bus	**Topología en anillo**	**Topología conmutada**
Rotación circular	Bus con paso de testigo (IEEE 802.4) Sondeo (IEEE 802.11)	Anillo con paso de testigo (IEEE 802.5; FDDI)	Petición/prioridad (IEEE 802.12)
Reserva	DQDB (IEEE 802.6)		
Contención	CSMA/CD (IEEE 802.3) CSMA (IEEE 802.11)		CSMA/CD (IEEE 802.3)

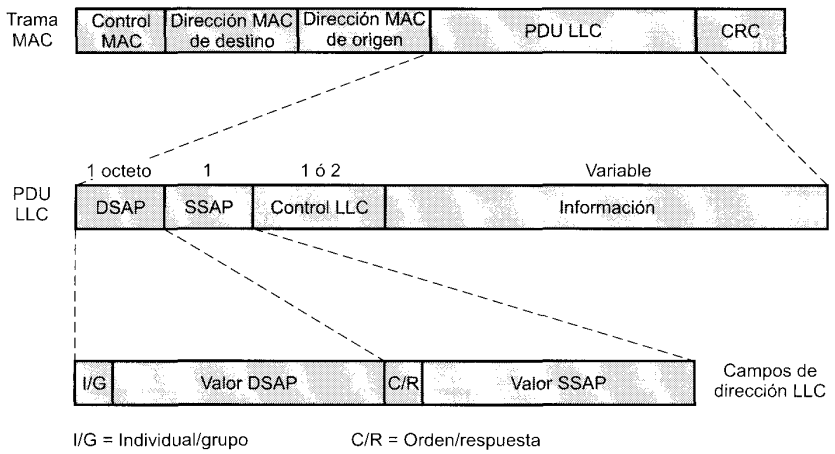


Figura 13.6. PDU LLC con formato genérico de trama MAC.

implementa estas funciones haciendo uso de una unidad de datos de protocolo (PDU) a la que se denomina trama MAC.

El formato exacto de la trama MAC difiere ligeramente para los distintos protocolos MAC en uso. En general, todas las tramas MAC tienen un formato similar al de la Figura 13.6. Los campos de esta trama son:

- **Control MAC:** este campo contiene información de control de protocolo necesaria para el funcionamiento del protocolo MAC. Por ejemplo, aquí se podría indicar un nivel de prioridad.
- **Dirección MAC de destino:** punto de conexión física MAC en la LAN del destino de la trama.
- **Dirección MAC de origen:** punto de conexión física MAC en la LAN del origen de la trama.
- **LLC:** datos LLC de la capa inmediatamente superior.
- **CRC:** campo de comprobación de redundancia cíclica (también conocido como campo de secuencia de comprobación de trama, FCS). Como se vio en HDLC y en otros protocolos de control de enlace de datos (Capítulo 7), este campo es un código de detección de errores.

En la mayor parte de los protocolos de control de enlace de datos, la entidad de protocolo es responsable no sólo de la detección de errores haciendo uso del campo CRC, sino también de la recuperación de éstos mediante la retransmisión de las tramas erróneas. En la arquitectura de protocolos LAN, estas dos funciones se dividen entre las capas MAC y LLC. La capa MAC es responsable de la detección de errores y del rechazo de tramas erróneas. Opcionalmente, la capa LLC controla qué tramas han sido recibidas correctamente y retransmite las erróneas.

CONTROL DE ENLACE LÓGICO

La capa LLC en redes LAN es similar en varios aspectos a otras capas de enlace de uso común. Como todas las capas de enlace, LLC está relacionado con la transmisión de una unidad de datos de protocolo del nivel de enlace (PDU) entre dos estaciones, sin necesitar un nodo de conmutación intermedio. LLC presenta dos características no compartidas por la mayor parte de otros protocolos de control de enlace:

1. Debe admitir acceso múltiple, consecuencia de la naturaleza de medio compartido del enlace (esto difiere de una línea multipunto en que ahora no existe ningún nodo primario).
2. La capa MAC lo descarga de algunos detalles del acceso al enlace.

El direccionamiento en LLC implica la especificación de los usuarios LLC origen y destino. Usualmente, un usuario es un protocolo de una capa superior o una función de gestión de red en la estación. Manteniendo la terminología OSI para el usuario de una capa de la arquitectura de protocolos, estas direcciones de usuario LLC se denominan puntos de acceso al servicio (SAP).

En primer lugar se estudiarán los servicios que ofrece LLC a un usuario de una capa superior, discutiendo posteriormente el protocolo LLC.

Servicios LLC

LLC especifica los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios. El funcionamiento y formato de este estándar están basados en HDLC. Existen tres posibles servicios para dispositivos conectados que usan LLC:

- **Servicio no orientado a conexión sin confirmación:** este servicio es de tipo datagrama. Es muy sencillo ya que no incluye mecanismos de control de flujo ni de errores, por lo que no está garantizada la recepción de los datos. Sin embargo, en la mayoría de los dispositivos existe alguna capa superior o software encargado de cuestiones de fiabilidad.
- **Servicio en modo conexión:** este servicio es similar al ofrecido por HDLC. Se establece una conexión lógica entre dos usuarios que intercambian datos, existiendo control de flujo y de errores.
- **Servicio no orientado a conexión con confirmación:** es una mezcla de los dos anteriores. Los datagramas son confirmados, pero no se establece conexión lógica previa.

Generalmente, un vendedor ofrece estos servicios como opciones que el consumidor puede elegir cuando adquiere el equipo. Otra posibilidad es que el consumidor compre un equipo que presente dos o los tres servicios, seleccionando cada uno de ellos de acuerdo con la aplicación.

El **servicio no orientado a conexión sin confirmación** requiere una lógica mínima y es útil en dos situaciones. En primer lugar, en aquellas en las que capas superiores o software ofrecen la seguridad y los mecanismos de control de flujo necesarios, evitándose la duplicidad. Por ejemplo, TCP podría ofrecer los mecanismos necesarios para asegurar una recepción de datos segura. En segundo lugar, existen situaciones en las que el coste de establecimiento y mantenimiento de la conexión resulta injustificado e incluso contraproducente (por ejemplo, las actividades de adquisición de datos que implican el muestreo periódico de fuentes de datos tales como sensores e informes automáticos de autotest de seguridad de equipos o componentes de red). En una aplicación de supervisión, la pérdida ocasional de datos puede no provocar problemas siempre que el siguiente informe llegue pronto. Así, en la mayoría de los casos, son preferibles los servicios no orientados a conexión sin confirmación.

El **servicio en modo conexión** se puede utilizar en dispositivos muy simples, como controladores de terminal, que disponen de poco software por encima de este nivel. En estos casos, el servicio proporciona mecanismos de control de flujo y de fiabilidad, usualmente implementados en capas superiores del software de comunicaciones.

El **servicio no orientado a conexión confirmado** resulta útil en varias situaciones. Con el servicio en modo conexión, el software de control de enlace lógico debe mantener algún tipo de tabla conteniendo el estado de cada conexión activa. Si el usuario necesita garantizar la recepción, pero existe un gran número de destinos para los datos, el servicio en modo conexión no resulta práctico dado el gran número de tablas necesarias. Un ejemplo es un proceso de control o una empresa automatizada donde es necesario un dispositivo central para comunicar con un gran número de procesadores y controladores programables. Otra posible utilización de este servicio es la gestión de alarmas o señales de control de emergencia de una empresa: dada su importancia, es necesaria una confirmación de modo que el emisor pueda estar seguro de que se produjo la señal; por otro lado, dada la urgencia de la señal, el usuario podría no desear perder tiempo en establecer una conexión lógica como paso previo al envío de los datos.

Protocolo LLC

El protocolo LLC básico se diseñó después de HDLC y presenta funciones y formatos similares a él. Las diferencias entre los dos protocolos se pueden resumir en las siguientes:

- LLC hace uso del modo de operación balanceado asíncrono de HDLC para dar soporte al servicio LLC en modo conexión. Éste se denomina operación de tipo 2, no empleándose los otros modos de HDLC.
- LLC presta un servicio no orientado a conexión sin confirmación usando la PDU de información no numerada, lo que se conoce como operación de tipo 1.
- LLC ofrece un servicio no orientado a conexión confirmado haciendo uso de dos PDU no numeradas nuevas, lo que se denomina operación de tipo 3.
- LLC permite multiplexación mediante el empleo de puntos de acceso al servicio LLC (LSAP).

Los tres protocolos LLC emplean el mismo formato de PDU (Figura 13.6), consistente en cuatro campos. Cada uno de los campos DSAP y SSAP contiene una dirección de 7 bits que especifica los usuarios LLC destino y origen. Un bit del campo DSAP indica si la dirección es individual o de grupo, mientras que un bit de SSAP indica si la PDU es una orden o una respuesta. El formato del campo de control LLC es idéntico al de HDLC (Figura 7.10), haciendo uso de números de secuencia ampliados (7 bits).

Para la **operación de tipo 1**, que ofrece el servicio no orientado a conexión no confirmado, se utiliza la PDU de información no numerada (UI) para transmitir datos de usuario. No existe confirmación, control de flujo ni control de errores, aunque existe detección de errores y rechazo a nivel MAC.

Otras dos PDU son utilizadas para dar soporte a las funciones de gestión asociadas a los tres tipos de operación. Ambas PDU se usan de la siguiente forma. Una entidad LLC puede emitir una orden (bit C/R = 0) XID o TEST, enviando en respuesta la entidad LLC receptora el correspondiente XID o TEST. La PDU XID se usa para intercambiar dos tipos de información: tipos de operación admitidos y tamaño de ventana. Por su parte, la PDU TEST se emplea para llevar a cabo un test en bucle cerrado del camino de transmisión entre dos entidades LLC. Tras recibir una PDU de orden TEST, la entidad LLC de destino envía, tan pronto como le es posible, una PDU de respuesta TEST.

En la **operación de tipo 2** se establece una conexión de enlace de datos entre dos SAP LLC previamente al intercambio de éstos. El establecimiento de la conexión se intenta por parte del protocolo de tipo 2 en respuesta a una solicitud de un usuario. La entidad LLC envía una PDU SABME[4] para solicitar una conexión lógica con la otra entidad LLC. Si el usuario LLC especificado en el campo DSAP acepta la conexión, la entidad de destino LLC devuelve una PDU de confirmación no numerada (UA). La conexión queda identificada unívocamente por el par de SAP de usuario. Si el usuario LLC destino rechaza la solicitud de conexión, su entidad LLC devuelve una PDU de modo de desconexión (DM).

Una vez que la conexión está establecida, los datos se intercambian, como en HDLC, haciendo uso de PDU de información. Las PDU de información contienen los números de secuencia enviado y recibido para la gestión del orden secuencial y el control de flujo. Como en HDLC, las PDU de tipo supervisor se utilizan para el control de errores y de flujo. Cualquiera de las dos entidades LLC puede terminar una conexión LLC lógica mediante el envío de una PDU de desconexión (DISC).

En la **operación de tipo 3** se confirma cada PDU transmitida. Se define una nueva PDU no numerada (no existente en HDLC), la de información no orientada a conexión con confirmación (AC). Los datos de usuario se envían en sucesivas PDU de orden AC, y deben ser confirmadas usando una PDU de respuesta AC. Para prevenir las pérdidas de PDU se utiliza un número de secuencia de 1 bit, de forma que el emisor alterna el uso de 0 y 1 en sus PDU de orden AC y el receptor responde con una PDU AC con el número opuesto al de la orden correspondiente. Sólo se puede enviar una PDU en cada sentido en un instante de tiempo dado.

---

[4] SABME significa Establecer el Modo Balanceado Ampliado Asíncrono («Set Asynchronous Balanced Mode Extended»). Se usa en HDLC para elegir ABM y seleccionar números de secuencia ampliados de 7 bits. Tanto ABM como los números de secuencia de 7 bits son obligatorios en la operación de tipo 2.

13.3 REDES LAN EN BUS

Esta sección presenta algunos detalles técnicos de las redes LAN con topología en bus. Comenzaremos describiendo las características generales de esta topología, dedicando el resto de la sección al estudio del uso de cable coaxial y fibra óptica para implementarla.

CARACTERÍSTICAS DE LA TOPOLOGÍA EN BUS

La topología en bus es una configuración multipunto; es decir, existen más de dos dispositivos conectados al medio y con capacidad de transmisión a través del mismo. Esto da lugar a varias cuestiones de diseño. La primera es la necesidad de una técnica de control de acceso al medio, discutida más adelante.

Otra cuestión importante en el diseño está relacionada con el equilibrado de las señales. Cuando dos estaciones intercambian datos a través de un enlace, la potencia de señal del emisor debe estar comprendida entre unos límites. La señal debe ser suficientemente fuerte para que, después de la atenuación sufrida en el medio, llegue al receptor con una potencia mínima. También debe ser lo suficientemente potente como para presentar una relación señal-ruido adecuada. En cambio, la señal no debe ser tan potente como para saturar el circuito del emisor, lo que distorsionaría la señal. A diferencia del equilibrado en líneas punto a punto, éste no resulta sencillo para líneas multipunto. Si una estación desea transmitir hacia otra, el equilibrado de la señal se debe realizar para todas las permutaciones de estaciones tomadas de dos en dos: para n estaciones, el número de permutaciones es $n \times (n - 1)$. Así, para una red con 200 estaciones (sistema no demasiado grande) se deben satisfacer simultáneamente 39.800 condiciones de potencia de señal. Para distancias entre dispositivos comprendidas entre decenas y miles de metros, esto resulta ser una tarea extremadamente complicada para cualquier red con un número elevado de dispositivos. En sistemas que hagan uso de señales de radiofrecuencia (RF), el problema es más complejo debido a la posibilidad de interferencias de señales RF. Una solución usual consiste en dividir el medio en segmentos más pequeños, en los que es posible el equilibrado entre pares, haciendo uso de amplificadores o repetidores entre ellos.

MEDIOS DE TRANSMISIÓN PARA REDES LAN EN BUS

Existen cuatro medios alternativos para su uso en redes LAN en bus:

- **Par trenzado:** en los primeros desarrollos de redes LAN se usaba par trenzado de voz para proporcionar instalaciones LAN fáciles y económicas, implementándose así varios sistemas operando a 1 Mbps (por ejemplo, [BOSE81]). Sin embargo, el uso de par trenzado no resulta práctico para velocidades superiores en un bus compartido, de forma que esta aproximación se descartó hace mucho tiempo.
- **Cable coaxial de banda base:** un cable coaxial de banda base es aquel que hace uso de señales digitales. El esquema Ethernet original utilizaba este tipo de medio.
- **Cable coaxial de banda ancha:** este cable es el utilizado en los sistemas de televisión por cable, donde se hace uso de señales analógicas a las frecuencias de radio y televisión.
- Este sistema es más caro y más difícil de instalar y mantener que el de cable coaxial de banda base. Aunque las especificaciones IEEE 802.3 incluyen una alternativa de banda ancha, esta aproximación no alcanzó nunca popularidad y no se ha vuelto a considerar.
- **Fibra óptica**: a lo largo de los años ha existido bastante investigación en torno a esta alternativa, pero el coste de las tomas de conexión de fibra óptica y la disponibilidad de alternativas mejores ha provocado que no se utilice esta opción.

Así, para la topología en bus, sólo el cable coaxial de banda base ha conseguido un amplio uso, especialmente en los sistemas Ethernet e IEEE 802.3. En cambio, en comparación con la instalación de fibra óptica o par trenzado en estrella, la topología en bus haciendo uso de cable coaxial de banda base

presenta varias limitaciones. Incluso la realización de cambios simples puede implicar el acceso al cable coaxial, el desplazamiento de tomas de conexión y el reencaminamiento de los segmentos de cable. En consecuencia, se han llevado a cabo pocas o ninguna nuevas instalaciones de LAN en bus con cable coaxial. A pesar de sus limitaciones, existe ya instalada una cantidad considerable de este tipo de redes, por lo que merece la pena resumir sus características.

CABLE COAXIAL DE BANDA BASE

Una LAN en banda base se define como una red que hace uso de señales digitales; es decir, los datos binarios a transmitir se insertan en el cable como una secuencia de pulsos de tensión, usando generalmente codificación Manchester o Manchester Diferencial (véase Figura 5.2). La naturaleza de las señales digitales es tal que el espectro en frecuencias del cable se ocupa completamente, por lo que no es posible disponer de varios canales en el cable (multiplexación por división en frecuencias). La transmisión es bidireccional; es decir, una señal insertada en un punto cualquiera del medio se propaga en ambos sentidos hacia los extremos, donde es absorbida. Los sistemas en bus en banda base sólo pueden tener como mucho una extensión de unos pocos kilómetros. Esto se debe a que la atenuación de la señal, más pronunciada a altas frecuencias, provoca la superposición de los pulsos y un debilitamiento de la señal, siendo prácticamente inviable la comunicación a largas distancias.

El uso original del cable coaxial de banda base para una LAN en bus fue el sistema Ethernet, que opera a 10 Mbps y es la base del estándar IEEE 802.3.

La mayor parte de los sistemas de cable coaxial de banda base utilizan un cable especial de 50 ohmios en lugar del cable estándar de 75 ohmios usado en CATV. Estos valores se refieren a la impedancia del cable, la cual se puede decir, de forma coloquial, que es una medida de cómo debe ser aplicada la tensión al cable para conseguir una potencia de señal dada. Para señales digitales, el cable de 50 ohmios sufre reflexiones menos intensas debido a la inserción de las capacidades inherentes a las tomas de conexión, y ofrece mejor inmunidad al ruido electromagnético de baja frecuencia en comparación con el cable de 75 ohmios.

Como en cualquier sistema de transmisión, existe un compromiso entre velocidad, longitud del cable, número de tomas de conexión y características eléctricas del cable y de los componentes de transmisión/recepción. Por ejemplo, a medida que la velocidad es menor la longitud del cable puede ser mayor. Esta afirmación es cierta debido a que cuando la señal se propaga a lo largo del medio de transmisión, la integridad de la señal sufre atenuación, ruido y otros problemas. Cuanto mayor es la longitud de propagación mayor es el efecto, incrementándose así la probabilidad de error. Sin embargo, a menor velocidad de transmisión los pulsos individuales de una señal digital perduran más y pueden ser recuperados en presencia de problemas más fácilmente que para velocidades superiores, donde los pulsos son más cortos.

He aquí un ejemplo que ilustra algunos compromisos. La especificación Ethernet y el estándar IEEE 802.3 original hacen uso de un cable de 50 ohmios de 0,4 pulgadas de diámetro y una velocidad de transmisión de 10 Mbps. Con estos parámetros, la longitud máxima del cable es de 500 metros. Las estaciones se conectan al cable mediante tomas de conexión, siendo la distancia entre cualesquiera dos tomas múltiplo de 2,5 metros para asegurar que las reflexiones en tomas de conexión adyacentes no se sumen en fase [YEN83]. Se permite un número máximo de 100 tomas de conexión. En la jerga de IEEE, este sistema se denomina 10BASE5 (10 Mbps, banda base, 500 metros de cable).

Posteriormente, para conseguir un sistema LAN de computadores personales de menor coste, IEEE 802.3 incluyó la especificación 10BASE2. En la Tabla 13.2 se compara este esquema, denominado Cheapernet, con 10BASE5. La principal diferencia es el uso de un cable más fino (0,5 cm), del tipo empleado en productos como los sistemas de telefonía pública. El cable más delgado es más flexible y, por tanto, más sencillo de doblar en las esquinas y de conectar en una estación, frente al cable coaxial que necesita ser instalado en la pared y requiere otro cable de conexión entre el principal y la estación de trabajo. El cable fino resulta más fácil de instalar y hace uso de una electrónica más sencilla que el

Tabla 13.2. Especificaciones IEEE 802.3 para redes LAN en bus de cable coaxial de banda base a 10 Mbps.

	10BASE5	**10BASE2**
Velocidad de datos	10 Mbps	10 Mbps
Longitud máxima de segmento	500 m	185 m
Extensión de la red	2.500 m	1.000 m
Nodos por segmento	100	30
Espaciado de los nodos	2,5 m	0,5 m
Diámetro del cable	1 cm	0,5 cm

cable grueso. Por otro lado, en cambio, el cable fino sufre una mayor atenuación y presenta una menor inmunidad al ruido que el cable grueso, lo que hace que admita un número menor de tomas de conexión en distancias menores.

Para aumentar la longitud de la red se pueden usar repetidores. Éstos funcionan de forma ligeramente diferente a los repetidores de redes en anillo. El repetidor en bus no se usa como un punto de conexión de dispositivo, y es capaz de transmitir en ambos sentidos. Un repetidor une dos segmentos de cable y transmite señales digitales en ambos sentidos entre los dos segmentos. Un repetidor es transparente al resto del sistema; dado que no lleva a cabo almacenamientos temporales, no aísla lógicamente un segmento del otro. Así, por ejemplo, si dos estaciones en segmentos diferentes intentan transmitir al mismo tiempo, sus paquetes interferirán (se produce colisión). Para evitar interferencias multitrayectoria sólo se permite un camino de segmentos y repetidores entre cualesquiera dos estaciones. En la Figura 13.7 se ilustra una LAN en bus de banda base con múltiples segmentos.

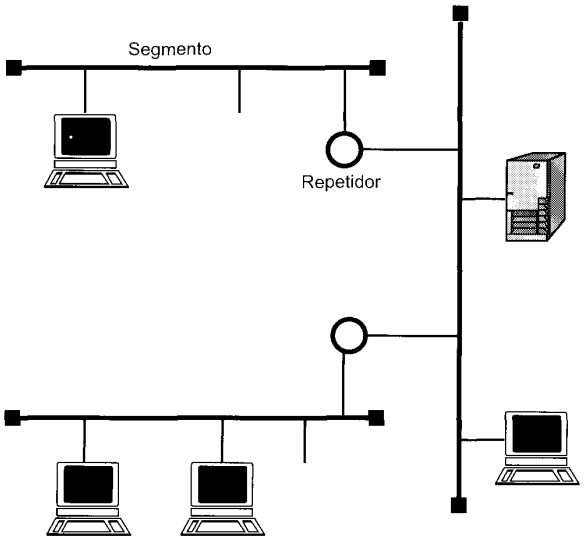


Figura 13.7. Configuración en banda base.

13.4. LAN EN ANILLO

CARACTERÍSTICAS DE LAS LAN EN ANILLO

Un anillo consta de varios repetidores, cada uno de ellos conectado a otros dos por líneas de transmisión unidireccionales formando un único camino cerrado. Los datos se transmiten secuencialmente, bit a bit, alrededor del anillo desde un repetidor hacia el siguiente. Cada repetidor regenera y retransmite cada bit.

Para que un anillo funcione como una red de comunicaciones son necesarias tres funciones: inserción de datos, recepción de datos y eliminación de datos, que son realizadas por los repetidores. Cada repetidor, además de servir como un elemento activo en el anillo, sirve como punto de conexión de dispositivo. Los datos se transmiten en paquetes, cada uno de ellos conteniendo un campo de dirección de destino. El campo de dirección de un paquete, al circular por el anillo y atravesar un repetidor, es copiado por éste; si la dirección coincide con la de la estación, se copia el resto del paquete.

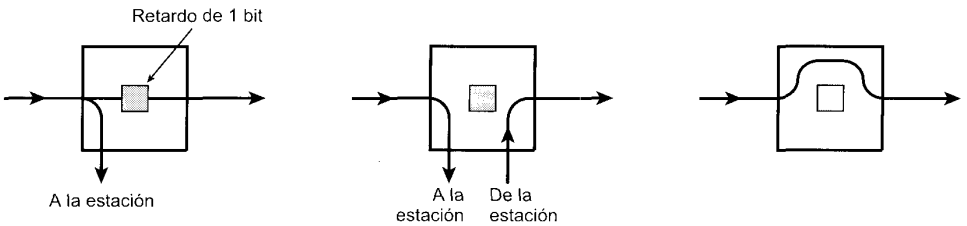
Los repetidores realizan las funciones de inserción y recepción de datos de forma diferente a las tomas que sirven como puntos de conexión de dispositivos en un bus o en un árbol. La eliminación de datos es, sin embargo, más complicada en el caso de un anillo. Las señales en un bus o en un árbol se insertan en la línea, se propagan hacia los extremos y son absorbidas por los terminadores; así, el bus o el árbol están libres de datos poco después de haber cesado la comunicación. Sin embargo, dado que el anillo es un bucle cerrado, el paquete circulará indefinidamente a menos que sea eliminado. Un paquete puede ser eliminado por el repetidor destino. Otra alternativa consiste en que cada paquete sea eliminado por el repetidor que lo emitió después de que haya dado una vuelta completa en el anillo.

Esta última aproximación es mejor debido a que (1) permite confirmaciones automáticas y (2) permite direccionamiento múltiple: un paquete puede ser enviado simultáneamente a varias estaciones.

Se puede hacer uso de una gran diversidad de estrategias para determinar cómo y cuándo insertar los paquetes en el anillo. Estas estrategias son, de hecho, protocolos de control de acceso al medio, discutiéndose el más usual de ellos, anillo con paso de testigo, en el Capítulo 14.

El repetidor puede tener dos objetivos principales: (1) contribuir al funcionamiento adecuado del anillo dejando pasar todos los datos que lo atraviesan, y (2) ofrecer un punto de acceso a las estaciones conectadas para transmitir y recibir datos. Existen dos estados correspondientes a estos dos cometidos (Figura 13.8): estado de escucha y estado de transmisión.

En el estado de escucha cada bit recibido se retransmite con un pequeño retardo, necesario para permitir al repetidor realizar las funciones básicas. Idealmente, el retardo debe ser del orden del intervalo de duración de un bit (el tiempo que tarda el repetidor en transmitir un bit completo por la línea de salida). Las funciones son:



(a) Estado de escucha (b) Estado de transmisión (c) Estado de cortocircuito

Figura 13.8. Estados del repetidor de un anillo.

- Búsqueda de secuencias patrones de bits. Entre ellas está la dirección o direcciones de las estaciones conectadas. Otro patrón, usado en la estrategia de control con paso de testigo explicada más adelante, indica permiso para transmitir. Obsérvese que el repetidor debe tener conocimiento del formato de los paquetes para realizar la función de búsqueda.
- Captación de cada bit entrante y su envío a la estación conectada mientras se continúa con la retransmisión de cada bit. Esto se realizará para cada bit de cada paquete dirigido a la estación.
- Modificación de un bit mientras circula. Los bits se pueden modificar en determinadas estrategias de control para, por ejemplo, indicar que el paquete ha sido copiado. Esto sirve como confirmación.

Cuando la estación dispone de datos a transmitir y el repetidor al que se encuentra conectada, de acuerdo con la estrategia de control, tiene permiso para hacerlo, este último entra en estado de transmisión. En este estado el repetidor recibe bits de la estación y los retransmite por la línea de salida. Durante el período de transmisión pueden aparecer bits por la línea de entrada del anillo. Existen dos posibles situaciones, tratadas de forma diferente:

- Los bits pueden proceder del mismo paquete que el repetidor está transmitiendo, lo cual sucederá si la «longitud de bit» del anillo es menor que el tamaño de paquete. En este caso, el repetidor pasa los bits hacia la estación, que puede comprobarlos como método de confirmación.
- En algunas estrategias de control se permite la existencia simultánea de más de un paquete en el anillo. Si el repetidor recibe bits de un paquete distinto al que está transmitiendo, puede almacenarlos temporalmente para retransmitirlos con posterioridad.

Estos dos estados, escucha y transmisión, son suficientes para un funcionamiento adecuado del anillo. Un tercer estado, estado de cortocircuito («bypass»), resulta también útil. En este estado se puede activar un relé de cortocircuito, de manera que las señales propagadas atraviesan el repetidor sin más retardo que el de propagación en el medio. El relé de cortocircuito presenta dos ventajas: (1) proporciona una solución parcial al problema de fiabilidad discutido más adelante, y (2) mejora las prestaciones al eliminar los retardos de repetidor para aquellas estaciones del medio que no se encuentren activas.

En enlaces repetidor-repetidor se puede usar par trenzado, cable coaxial de banda base y fibra óptica. El cable coaxial de banda ancha, en cambio, no resulta fácil de utilizar. Cada repetidor puede estar capacitado para recibir y transmitir datos de forma asíncrona sobre varios canales.

FLUCTUACIÓN EN LA TEMPORIZACIÓN

En un medio de transmisión en anillo la señal incluye alguna forma de sincronización, como, por ejemplo, el uso de codificación Manchester Diferencial (Figura 5.2). Mientras los datos circulan por el anillo son recibidos en cada repetidor, obteniéndose el sincronismo con dos fines: primero, saber cuándo hacer un muestreo de la señal de entrada para obtener los bits de datos, y segundo, usar esta información en la retransmisión de la señal hacia el siguiente repetidor. La obtención del sincronismo se puede realizar de forma aleatoria a partir de las transiciones en mitad del intervalo de los datos recibidos por varias razones, entre las que se encuentra la aparición de ruido durante la transmisión e imperfecciones en la circuitería de recepción. La razón principal, sin embargo, es la distorsión de retardo (descrita en la Sección 3.3). La desviación en la obtención del sincronismo se conoce como fluctuación en la temporización («timing jitter»).

A medida que cada repetidor recibe datos de entrada, emite una señal limpia sin distorsión. Sin embargo, no desaparece el error de temporización. De esta forma, la anchura de los pulsos digitales crece y se contrae de forma aleatoria a medida que las señales viajan a través el anillo, acumulándose la fluctuación en la temporización. El efecto acumulativo de la fluctuación provoca la variación de la «longitud de bit» o latencia de bit en el anillo. Sin embargo, a menos que la latencia del anillo permanezca constante, los bits se desechan (no se retransmiten) si ésta decrece, o se insertan si ésta crece.

La fluctuación en la temporización impone una limitación sobre el número de repetidores en el anillo. Aunque esta limitación no se puede solucionar completamente, se pueden adoptar varias medidas para mejorarla. Esencialmente, se usan conjuntamente dos aproximaciones. En primer lugar, cada repetidor puede incluir un bucle cerrado en fase (PLL), dispositivo que usa realimentación para minimizar la desviación entre un tiempo de bit y el siguiente. En segundo lugar, se puede usar una memoria temporal en uno o más repetidores. Esta memoria se inicia para gestionar un determinado número de bits, y se amplía y reduce para mantener constante la longitud de bit en el anillo. La combinación de circuitos PLL y memoria temporal incrementa de forma significativa el tamaño máximo de anillo permitido.

PROBLEMAS POTENCIALES EN EL ANILLO

Existen varios problemas potenciales en la topología en anillo. La rotura de un enlace o el fallo en un repetidor hace que la red entera deje de funcionar. La instalación de un nuevo repetidor para poder conectar nuevos dispositivos a la red necesita la identificación de dos repetidores cercanos, topológicamente adyacentes. La fluctuación en la temporización debe ser solucionada. Por último, dado que el anillo es cerrado, se necesita algún método para eliminar los paquetes que circulan, con técnicas de apoyo para reaccionar ante la ocurrencia de errores.

El último problema mencionado es una cuestión de protocolo que se discutirá más adelante. El resto de problemas se pueden gestionar mejorando la topología del anillo, tema que pasamos a discutir a continuación.

ARQUITECTURA EN ESTRELLA-ANILLO

Se pueden hacer dos observaciones respecto de la arquitectura en anillo básica descrita anteriormente. Primero, existe una limitación práctica respecto del número de repetidores en el anillo. Este límite viene impuesto por la fluctuación, la fiabilidad y los problemas de mantenimiento citados y por el retardo acumulado en un gran número de repetidores. Un límite de unos pocos cientos de repetidores parece razonable. Segundo, el funcionamiento del anillo no depende del encaminamiento real de los cables que unen los repetidores.

Estas observaciones han dado lugar al desarrollo de una arquitectura en anillo mejorada, la de estrella-anillo, que soluciona algunos de los problemas del anillo y permite la construcción de redes locales mayores.

En primer lugar consideremos la fusión de un anillo con una estrella. Esto se consigue haciendo pasar los enlaces entre repetidores por un único lugar. Este concentrador del cableado del anillo presenta varias ventajas. Dado que el acceso a la señal en cualquier enlace es centralizado, resulta sencillo aislar un fallo. Se puede enviar un mensaje sobre el anillo y seguir su evolución a fin de ver hasta dónde llega sin que se produzcan problemas. Un segmento con problemas puede ser desconectado y reparado más tarde. La incorporación de nuevos repetidores a anillo es sencilla: se colocan dos cables desde el nuevo repetidor al lugar de concentración de cables del anillo y se conecta a éste.

El relé de cortocircuito asociado a cada repetidor se puede desplazar al concentrador del cableado del anillo. Ante cualquier fallo, el relé puede eludir automáticamente su repetidor y dos enlaces. Una característica interesante de este hecho es que el camino de transmisión desde un repetidor al siguiente es aproximadamente constante, de modo que el rango de niveles de señal al que debe adaptarse automáticamente el sistema es mucho menor.

El concentrador del cableado del anillo permite una rápida recuperación ante un fallo en un cable o en un repetidor. A pesar de ello, un simple fallo podría, al menos temporalmente, deshabilitar toda la red. Además, el rendimiento y las fluctuaciones siguen imponiendo una limitación práctica al número máximo de estaciones en el anillo, ya que cada repetidor implica un incremento en el retardo. Finalmente, el uso de un único concentrador del cableado en una red extensa conlleva una gran cantidad de cable.

Para tratar de solucionar estos problemas se puede construir una LAN consistente en varios anillos conectados por puentes. El uso de puentes se estudiará en la Sección 13.7.

13.5. LAN EN ESTRELLA

LAN EN ESTRELLA CON PAR TRENZADO Y FIBRA ÓPTICA

En los últimos años ha crecido el interés por el uso del par trenzado como medio de transmisión para redes LAN, alcanzando una gran popularidad las LAN en bus con este tipo de cable. Sin embargo, estas LAN presentan algunos inconvenientes con respecto a las LAN de cable coaxial. Lo primero es que el menor coste aparente del par trenzado no lo es tanto como se podría pensar cuando se usa un bus lineal. Es cierto que el cable de par trenzado es más barato que el cable coaxial, pero, por otro lado, la mayor parte del coste del cableado de una LAN es la instalación del mismo, y ésta no es mayor para un cable coaxial que para un par trenzado. En segundo lugar, el cable coaxial proporciona una mayor calidad de señal y, por tanto, permite más dispositivos en distancias mayores para velocidades de datos superiores que el par trenzado.

El renovado interés por el par trenzado, al menos en el contexto de redes LAN de tipo bus, radica en el uso de pares no apantallados para el cableado de redes LAN en estrella. La razón de este interés es que el par trenzado no apantallado es sencillamente cable telefónico, y prácticamente todos los edificios de oficinas están equipados con pares trenzados que van desde armarios de interconexión a cada despacho. Este hecho presenta varias ventajas en el desarrollo de una LAN:

- No existe prácticamente coste en la instalación de par trenzado no apantallado, puesto que el cable está ya ahí. El cable coaxial, en cambio, se debe colocar expresamente, lo que puede resultar difícil en edificios viejos dado que los conductos existentes pueden resultar insuficientes.
- En la mayoría de los edificios de oficinas es imposible prever los lugares donde será necesario el acceso a la red. Dado que es extremadamente caro instalar un cable coaxial para cada despacho, una LAN basada en cable coaxial cubrirá generalmente sólo una parte del edificio. Si posteriormente se cambian equipos de una oficina a otra fuera del dominio de la LAN, la ampliación en la cobertura de ésta resulta muy cara. Con el uso del cable de teléfono no se presenta este problema puesto que todos los despachos están equipados con él.

Así pues, la solución más popular del uso de un par trenzado en una LAN es un cableado en estrella. Los productos comerciales usan un esquema tal que el elemento central de la estrella es un elemento activo, al que se denomina **centro** («hub»). Cada estación se conecta al centro mediante dos enlaces (transmitir y recibir). El centro actúa como un repetidor: cuando transmite una única estación, el centro replica la señal en la línea de salida hacia cada estación. Usualmente, el enlace consiste en dos pares trenzados no apantallados. Dada la alta velocidad y la baja calidad de transmisión del par trenzado no apantallado, la longitud de un enlace está limitada en torno a 100 m. Como alternativa, se puede usar un enlace de fibra óptica, en cuyo caso la longitud máxima es del orden de 500 m.
Obsérvese que aunque este esquema es físicamente una estrella, funciona lógicamente como un bus: una transmisión por parte de una estación se recibe en el resto de estaciones, y se produce colisión si dos estaciones transmiten al mismo tiempo.

Varios niveles de centros se pueden poner en cascada formando una configuración jerárquica. En la Figura 13.9 se muestra una configuración en dos niveles. Existe un **centro raíz** (HHUB) y uno o más **centros intermedios** (IHUB). Cada centro puede ser una mezcla de estaciones y otros centros conectados a él por debajo. Esta estructura se adecua bien a edificios cableados, donde, generalmente, existe un armario de interconexiones en cada planta del edificio, pudiendo colocarse un centro en cada una de ellas. Cada centro podría dar servicio a las estaciones situadas en su misma planta.

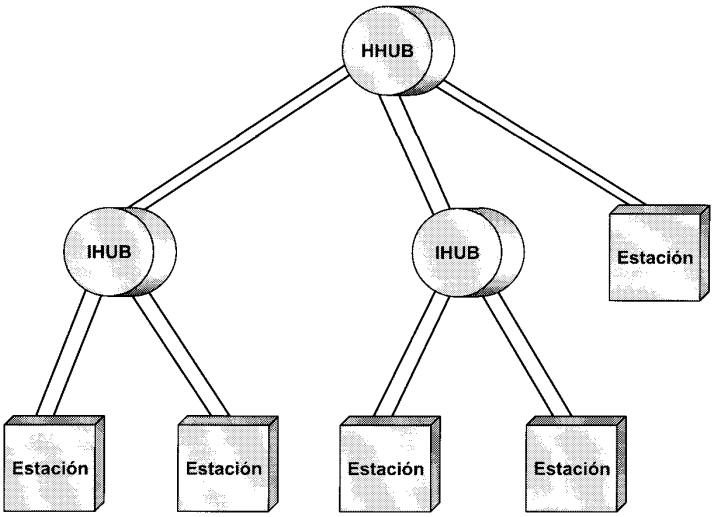


Figura 13.9. Topología en estrella en dos niveles.

CENTROS Y CONMUTADORES

En la discusión previa se ha usado el término *centro*, utilizándose dicho término para referirnos a distintos tipos de dispositivos. La distinción más importante es entre un centro compartido y un centro de LAN conmutada.

Para aclarar la distinción entre distintos tipos de centros, en la Figura 13.10a se muestra un bus típico correspondiente a una LAN convencional a 10 Mbps. Un bus se instala de forma que todos los dispositivos a conectar se encuentran próximos a él. En la figura la estación B está transmitiendo, de forma que esta transmisión sale de B hacia el bus, a lo largo de éste en los dos sentidos y sobre las líneas de acceso de cada una de las otras estaciones conectadas. En esta configuración todas las estaciones deben compartir la capacidad total del bus, que es de 10 Mbps.

Un centro compartido tiene un centro raíz, a veces situado en un armario de cableado en un edificio. El cableado en estrella se emplea para conectar las estaciones con el centro, de forma que la transmisión por parte una estación se recibe en el centro y se retransmite sobre todas las líneas de salida. Por tanto, para evitar la ocurrencia de colisión, sólo una estación puede transmitir en un momento dado. De nuevo, la capacidad total de la LAN es de 10 Mbps. El uso de un centro compartido presenta varias ventajas frente a la configuración en bus: aprovecha el cableado de los edificios además del hecho de que el centro se puede configurar para determinar el mal funcionamiento de una estación que congestiona la red, de modo que se podría eliminar dicha estación de la red. En la parte (b) de la figura se ilustra el funcionamiento de un centro compartido. De nuevo se encuentra transmitiendo la estación B. Esta transmisión sale de B a lo largo de la línea de transmisión entre esta estación y el centro, y desde él al resto de estaciones conectadas a lo largo de las líneas de recepción correspondientes.

Se pueden mejorar las prestaciones mediante el uso de un centro de conmutación. En este caso, el centro raíz actúa como un conmutador, distinto de un conmutador de paquetes o de circuitos. Una trama procedente de una estación dada es conmutada hacia la correspondiente línea de salida para su envío hacia la estación destino. Al mismo tiempo, algunas otras líneas desocupadas se pueden usar para conmutar otro tráfico. En la Figura 13.10c se muestra un ejemplo en el que la estación B está transmitiendo una trama a A y, al mismo tiempo, C transmite una trama hacia D. Así, en este ejemplo, el rendimiento actual de la LAN es 20 Mbps, aunque cada dispositivo individual esté limitado a 10 Mbps El centro de conmutación presenta varias características interesantes:

1. No se necesita cambiar el software o el hardware de los dispositivos conectados para convertir una LAN en bus o una LAN con centro compartido en una LAN con centro de conmutación. En el caso de una LAN CSMA/CD, cada dispositivo conectado continúa usando el protocolo CSMA/CD para acceder a la LAN. Desde el punto de vista de los dispositivos conectados nada ha cambiado en el acceso lógico.
2. Suponiendo que el centro tiene suficiente capacidad para atender a todos los dispositivos conectados, cada uno de ellos tiene una capacidad dedicada igual a la de la LAN completa. Por ejemplo, en la Figura 13.10c, si el centro puede dar un rendimiento de 20 Mbps, parece como si cada dispositivo conectado tuviese una capacidad dedicada de entrada o salida de 10 Mbps.

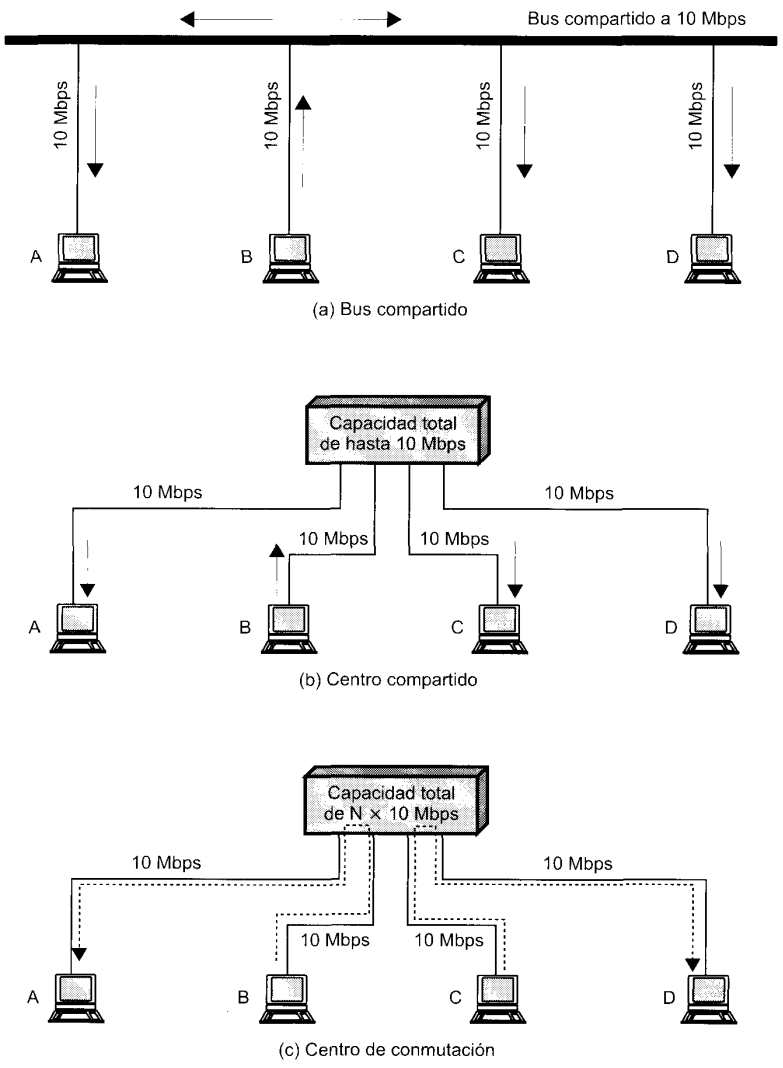


Figura 13.10. Centros y conmutadores en una LAN.

3. El centro conmutado permite el escalado de forma sencilla, pudiéndose conectar dispositivos adicionales a él mediante el incremento correspondiente de su capacidad.

Comercialmente existen dos tipos de centros conmutados:

- **Conmutador de almacenamiento y envío:** el centro acepta una trama sobre una línea de entrada, la almacena temporalmente y después la encamina hacia la línea de salida correspondiente.
- **Conmutador rápido:** el centro aprovecha que la dirección de destino se encuentra al comienzo de la trama MAC (control de acceso al medio) para retransmitir la trama entrante sobre la línea de salida correspondiente tan pronto como sabe la dirección de destino.

El conmutador de tipo rápido permite el mayor rendimiento posible, aunque a riesgo de propagar tramas erróneas dado que no es capaz de comprobar el CRC antes de efectuar la retransmisión. Por su parte, el conmutador de almacenamiento y envío implica un retardo entre la emisión y la recepción pero mantiene la integridad completa de la red.

13.6. REDES LAN INALÁMBRICAS

En los últimos años las LAN inalámbricas han ocupado un lugar importante en el mercado de las redes de área local. Cada vez más, las organizaciones se han dado cuenta de que las LAN inalámbricas son un complemento indispensable a las redes cableadas a fin de satisfacer necesidades de movilidad, traslado, trabajo en red *ad hoc* y cobertura de lugares difíciles de cablear. Hasta hace relativamente poco tiempo, las redes LAN inalámbricas eran poco usadas debido al alto precio, baja velocidad de transmisión, cuestiones de seguridad y necesidades de licencia. A medida que estos problemas se han ido solucionando, la popularidad de las LAN inalámbricas ha crecido rápidamente.

En esta sección se verán los requisitos y ventajas de las redes LAN inalámbricas, así como las aproximaciones más importantes para su implementación.

APLICACIONES DE LAN INALÁMBRICAS

[PAHL95] indica cuatro áreas de aplicación para las redes LAN inalámbricas: ampliación de redes LAN, interconexión de edificios, acceso nómada y redes *ad hoc*. A continuación se analizan todas ellas.

Ampliación de redes LAN

Los primeros productos de LAN inalámbricas, aparecidos a finales de los 80, eran ofrecidos como sustitutos de las LAN cableadas tradicionales. Una red LAN inalámbrica evita el coste de la instalación del cableado y facilita la tarea de traslado y otras modificaciones en la estructura de la red. Sin embargo, esta motivación de las LAN inalámbricas fue superada por los acontecimientos. Primero, debido al aumento en la necesidad de redes LAN, los arquitectos incluyeron en el diseño de sus nuevos edificios costosos precableados para aplicaciones de datos. Segundo, con los avances en la tecnología de transmisión de datos se incrementó la seguridad en los pares trenzados para redes LAN. Así, dado que la mayor parte de los edificios viejos estaban ya cableados con par trenzado de Clase 3, y muchos de los edificios de nueva construcción lo están con par trenzado de Clase 5, resulta escaso el uso de LAN inalámbricas frente a LAN cableadas.

Sin embargo, el papel de una LAN inalámbrica como alternativa a las LAN cableadas es importante en un gran número de entornos. Algunos ejemplos son edificios de gran superficie, como plantas de fabricación, plantas comerciales y almacenes; edificios históricos con insuficiente cable de par trenzado donde está prohibido hacer más agujeros para nuevo cableado; y pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan económicos. En todos estos casos, una LAN inalámbrica ofrece una alternativa más efectiva y atractiva. En la mayor parte de estas situaciones, un organismo dispondrá también de una LAN cableada con servidores y algunas estaciones de trabajo estacio-

narias. Por ejemplo, una planta de manufacturación dispone generalmente de una oficina independiente de la propia planta pero que debe estar interconectada a ella con propósitos de trabajo en red. Por tanto, una LAN inalámbrica está conectada en muchas ocasiones con una LAN cableada en el mismo recinto, denominándose este campo de aplicación ampliación o extensión de redes LAN.

En la Figura 13.11 se muestra una configuración sencilla de una LAN inalámbrica típica en muchos entornos. Existe una LAN troncal cableada, como una Ethernet, que conecta varios servidores, estaciones de trabajo y uno o más puentes o dispositivos de encaminamiento para comunicar con otras redes. Adicionalmente, existe un módulo de control (CM) que funciona como interfaz con la LAN inalámbrica. El módulo de control incluye funciones de los puentes o de los dispositivos de encaminamiento para conectar la LAN inalámbrica con la troncal. Además se incluye algún tipo de lógica de control de acceso, como, por ejemplo, un esquema de sondeo o uno de paso de testigo, para regular el acceso de los sistemas finales. Hemos de destacar que algunos de los sistemas finales son dispositivos independientes, como estaciones de trabajo y servidores; además, los centros («hub») u otros módulos de usuario (UM) que controlan varias estaciones fuera de una LAN cableada pueden también formar parte de la LAN inalámbrica.

La configuración de la Figura 13.11 se denomina LAN inalámbrica de celda única, ya que todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control. Otra configuración común, sugerida en la Figura 13.12, es una LAN inalámbrica de celdas múltiples. En este caso existen varios módulos de control interconectados por una LAN cableada. Cada módulo de control da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión; por ejemplo, con una LAN de infrarrojos la transmisión está limitada a una sola habitación, por lo que se necesita una celda en cada habitación de un edificio de oficinas con soporte inalámbrico.

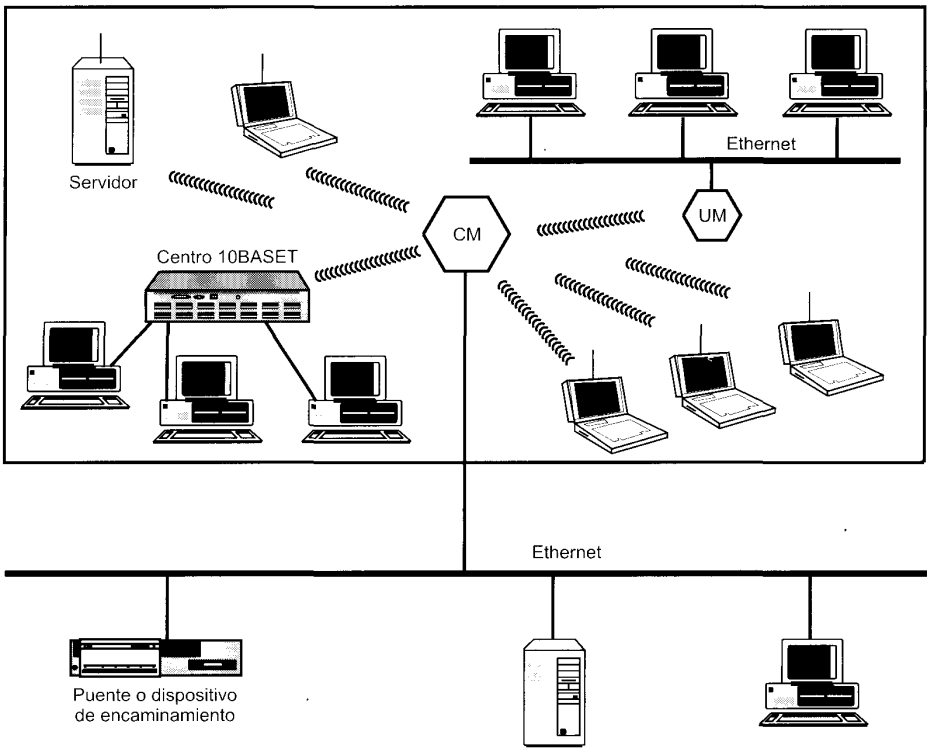


Figura 13.11. Ejemplo de configuración de una LAN inalámbrica de celda única.

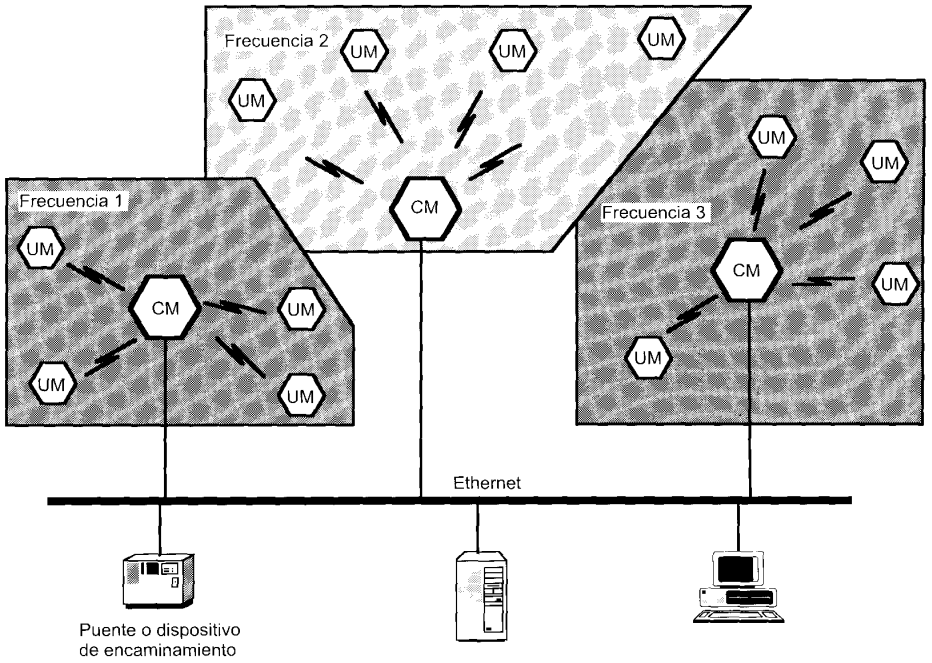


Figura 13.12. Ejemplo de configuración de una LAN inalámbrica de celdas múltiples.

Interconexión de edificios

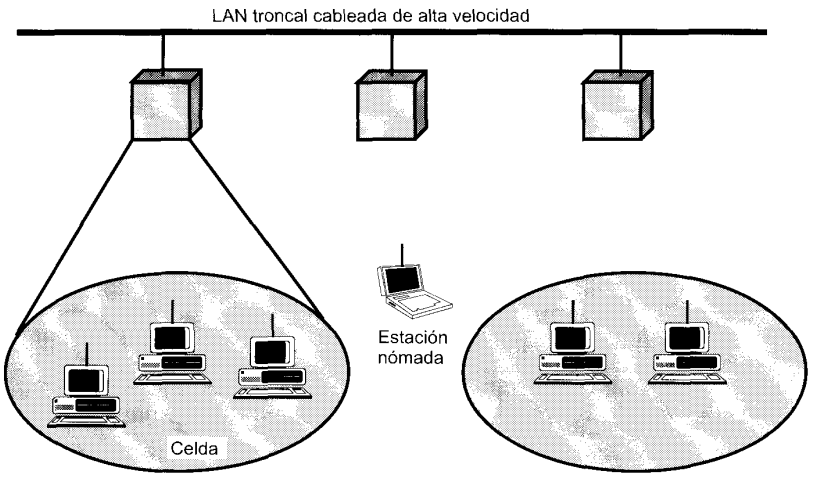
Otro uso de las LAN de tecnología inalámbrica es la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o inalámbricas. En este caso se usa un enlace no guiado entre dos edificios. Los dispositivos así conectados son generalmente puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de redes LAN inalámbricas.

Acceso nómada

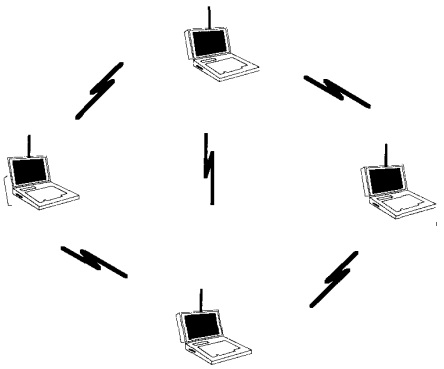
El acceso nómada permite un enlace no guiado entre un centro de LAN y un terminal de datos móvil con antena, como un computador portátil. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de viaje la transferencia de datos desde un computador personal portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio como es un campus o un centro financiero situado lejos de un grupo de edificios. En ambos casos los usuarios se pueden desplazar con sus computadores portátiles y pueden desear conectarse con los servidores de una LAN inalámbrica desde distintos lugares.

Trabajo en red *ad hoc*

Una red *ad hoc* es una red igual a igual (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computador, puede reunirse para una reunión de negocios o para una conferencia, conectando sus computadores a una red temporal sólo durante la reunión.



(a) LAN inalámbrica con infraestructura



(b) LAN *ad hoc*

Figura 13.13. Configuraciones de redes LAN inalámbricas.

En la Figura 13.13 se sugieren las diferencias entre una LAN inalámbrica *ad hoc* y una LAN inalámbrica que admite ampliaciones de LAN y acceso nómada. En el primer caso, la LAN inalámbrica presenta una infraestructura estacionaria consistente en una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra. Por el contrario, en una red LAN *ad hoc* no existe infraestructura; más aún, un conjunto de estaciones localizadas en el mismo dominio se puede autoconfigurar dinámicamente para formar una red temporal.

REQUISITOS DE LAS LAN INALÁMBRICAS

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total de las estaciones conectadas y capacidad de difusión. Además, existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- **Rendimiento:** el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio no guiado para maximizar la capacidad.
- **Número de nodos:** las LAN inalámbricas pueden necesitar dar soporte a cientos de nodos mediante el uso de varias celdas.
- **Conexión a la LAN troncal:** en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que conectan con ambos tipos de LAN. Puede ser también necesario dar soporte a usuarios móviles y redes inalámbricas *ad hoc*.
- **Área de servicio:** una superficie de cobertura para una red LAN inalámbrica tiene un diámetro típico de entre 100 y 300 metros.
- **Consumo de batería:** los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable. Esto sugiere que resulta inapropiado un protocolo MAC que necesita nodos móviles para supervisar constantemente los puntos de acceso o realizar comunicaciones frecuentes con una estación base.
- **Robustez en la transmisión y seguridad:** a menos que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- **Funcionamiento de red ordenada:** a medida que las LAN inalámbricas se están haciendo más populares, es probable que dos o más de estas redes operen en la misma o en alguna zona en que sea posible la interferencia entre ellas. Estas interferencias pueden frustrar el normal funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- **Funcionamiento sin licencia:** los usuarios podrían preferir adquirir y trabajar sobre LAN inalámbricas que no precisan de una licencia para la banda de frecuencia usada por la red.
- **Sin intervención/nómada:** el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.
- **Configuración dinámica:** los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

TECNOLOGÍAS DE LAN INALÁMBRICAS

Las LAN inalámbricas se clasifican generalmente de acuerdo con la técnica de transmisión usada. Todas las LAN actuales se encuentran dentro de una de las siguientes categorías:

- **LAN de infrarrojos (IR):** una celda individual en una LAN IR está limitada a una sola habitación dado que la luz infrarroja no es capaz de atravesar muros opacos.
- **LAN de espectro expandido:** este tipo de LAN hace uso de tecnologías de transmisión de espectro expandido. En la mayoría de los casos estas LAN operan en las bandas ISM (industria, ciencia y medicina), de modo que no se necesita licencia FCC para su utilización en los Estados Unidos.
- **Microondas de banda estrecha:** estas LAN operan en el rango de las microondas pero no hacen uso de espectro ensanchado. Algunos de estos productos operan a frecuencias para las que es necesario licencia FCC, mientras que otras lo hacen en alguna de las bandas ISM.

En la Tabla 13.3 se resumen algunas de las características principales de estas tres tecnologías.

Tabla 13.3. Comparación de las tecnologías de redes LAN inalámbricas.

	Infrarrojos		Espectro expandido		Radio
	Infrarrojos difusos	**Infrarrojos de haz directo**	**Salto de frecuencia**	**Secuencia directa**	**Microondas de banda estrecha**
Velocidad (Mbps)	1-4	1-10	1-3	2-20	10-20
Movilidad	Estacionario/móvil	Estacionario con LOS	Móvil	Estacionario/móvil	
Rango (m)	20-70	30	35-100	35-300	15-40
Detectabilidad	Despreciable		Pequeña		Alguna
Longitud de onda/frecuencia	λ: 800-900 nm		902-928 MHz 2,4-2,4835 GHz 5,725-5,85 GHz		902-928 MHz 5,2-5,775 GHz 18,825-19,205 GHz
Técnica de modulación	ASK		FSK	QPSK	FS/QPSK
Potencia radiada	—		< 1W		25 mW
Método de acceso	CSMA	Anillo con paso de testigo, CSMA	CSMA		Reserva, ALOHA, CSMA
Necesidad de licencia	No		No		Sí a menos que sea ISM

13.7. PUENTES

Casi siempre existe necesidad de llevar a cabo la expansión más allá de los confines de una LAN para proporcionar interconexión con otras LAN y con redes de área amplia. Dos aproximaciones generales se utilizan con este fin: puentes y dispositivos de encaminamiento. El uso de puentes es la aproximación más sencilla y permite la interconexión de LAN similares, mientras que los dispositivos de encaminamiento son de propósito más general y posibilitan la interconexión de una gran variedad de redes LAN y WAN. En esta sección se lleva a cabo el estudio de los puentes, dejándose el de los dispositivos de encaminamiento para la Parte V del texto.

Los puentes se han diseñado para su uso entre redes de área local (LAN) que utilizan protocolos idénticos en las capas física y de acceso al medio (por ejemplo, todas siguiendo la norma IEEE 802.3). Dado que todos los dispositivos usan los mismos protocolos, el volumen de procesamiento necesario en el puente es mínimo. Los puentes más sofisticados permiten la conversión entre formatos MAC diferentes (por ejemplo, la interconexión de una LAN Ethernet con una en anillo con paso de testigo).

Dado que los puentes se utilizan en situaciones en las que todas las LAN tienen las mismas características, el lector puede preguntarse por qué no utilizar simplemente una gran LAN. Dependiendo de ciertas circunstancias, existen varias razones para el empleo de varias LAN interconectadas mediante puentes:

- **Fiabilidad:** el peligro en la conexión de todos los dispositivos de procesamiento de datos de un organismo en una sola red es que un fallo en ella puede imposibilitar la comunicación para todos los dispositivos. En cambio, haciendo uso de puentes, la red puede dividirse en unidades autocontenidas.

- **Prestaciones:** en general, las prestaciones de una LAN decrecen cuando aumenta el número de dispositivos o la longitud del medio. A veces, varias LAN pequeñas pueden ofrecer mejores prestaciones si se pueden agrupar los dispositivos de manera tal que el tráfico interno de cada red supere significativamente el tráfico entre ellas.
- **Seguridad:** la disposición de varias LAN puede mejorar la seguridad en las comunicaciones. Es deseable mantener diferentes tipos de tráfico (por ejemplo, contabilidad, personal, planificación estratégica) con diferentes necesidades de seguridad y en medios separados físicamente. Simultáneamente a este hecho, los diferentes tipos de usuarios con diferentes niveles de seguridad necesitan comunicarse mediante mecanismos controlados y supervisados.
- **Geografía:** es evidente que se necesitan dos LAN separadas para dar soporte a dispositivos agrupados en dos lugares geográficamente distantes. Incluso en el caso de dos edificios separados por una carretera, resulta más fácil usar como puente un enlace de microondas que intentar disponer un cable coaxial entre los dos edificios.

FUNCIONES DE LOS PUENTES

En la Figura 13.14 se ilustra el funcionamiento de un puente que conecta dos redes LAN, A y B, que utilizan el mismo protocolo MAC. En este ejemplo el puente se conecta a ambas redes, si bien, usualmente, la función de puente se lleva a cabo mediante dos «semipuentes», uno conectado a cada LAN. Las funciones del puente son pocas y sencillas:

- Lectura de todas las tramas transmitidas en A y aceptación de aquellas dirigidas a estaciones en B.
- Retransmisión hacia B de cada una de las tramas, haciendo uso del protocolo de control de acceso al medio de esta LAN.
- El mismo proceso para el tráfico de B a A.

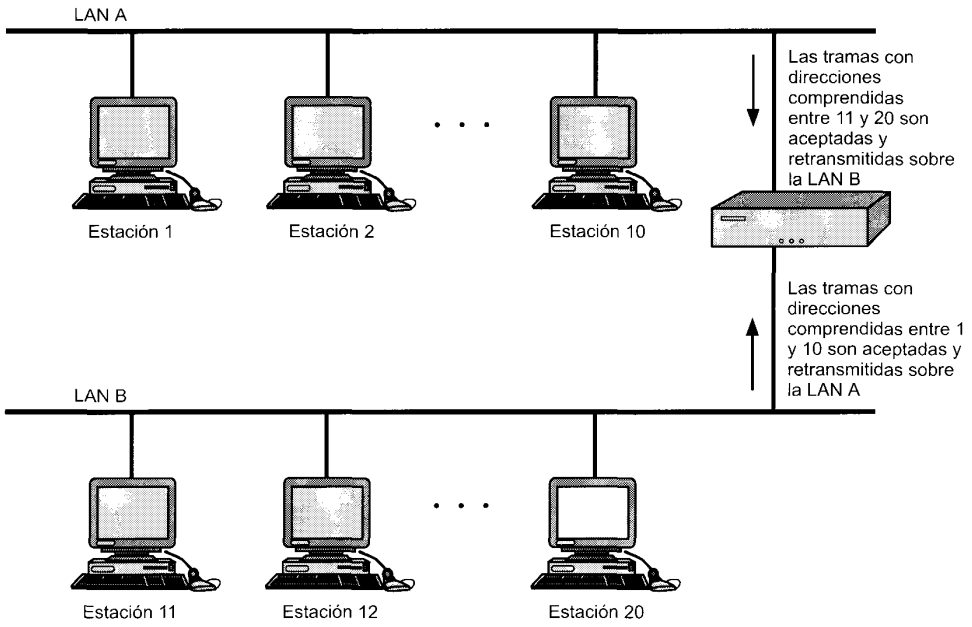


Figura 13.14. Funcionamiento de los puentes.

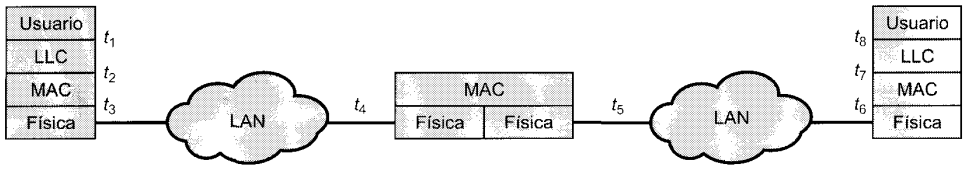
Merece la pena resaltar varios aspectos del diseño de los puentes:

- El puente no modifica el contenido o formato de las tramas que recibe ni las encapsula con una cabecera adicional. Cada trama a transmitir es simplemente copiada desde una LAN y repetida con, exactamente, el mismo patrón de bits de la otra LAN. Esto se puede hacer así dado que las dos LAN usan los mismos protocolos.
- El puente debe disponer de suficiente memoria temporal para aceptar demandas de pico. Para un periodo de tiempo pequeño las tramas se pueden recibir más rápidamente de lo que se pueden retransmitir.
- El puente debe presentar capacidad de direccionamiento y de encaminamiento. Como mínimo, debe conocer las direcciones de cada red para determinar qué tramas debe dejar pasar. Además, pueden existir más de dos redes LAN interconectadas por varios puentes, en cuyo caso puede ser necesario encaminar una trama a través de varios puentes a lo largo de su trayecto desde el origen hasta el destino.
- Un puente puede conectar más de dos LAN.

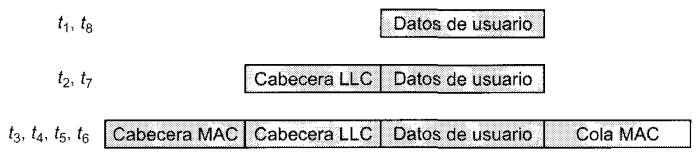
En resumen, el puente permite una ampliación de las LAN de tal manera que no se precisa modificar el software de comunicaciones de las estaciones conectadas a ellas. Desde el punto de vista de cada una de las estaciones en las dos (o más) LAN, parece como si sólo existiese una única red LAN en la que cada estación tiene una única dirección. Las estaciones utilizan esa dirección única y no necesitan discriminar explícitamente entre estaciones en la misma o en diferentes LAN; el puente se encarga de ello.

ARQUITECTURA DE PROTOCOLOS DE PUENTES

La especificación IEEE 802.1D define la arquitectura de protocolos para puentes MAC. En la arquitectura 802 la dirección final o de estación se establece en el nivel MAC, de modo que es a este nivel al que puede funcionar un puente. En la Figura 13.15 se muestra el caso más simple, consistente en dos LAN con los mismos protocolos MAC y LLC conectadas por un único puente. El puente funciona como se ha descrito anteriormente: captura las tramas MAC cuyo destino no se encuentra en la LAN de origen, las almacena temporalmente y las transmite sobre la otra LAN. Por lo que se refiere a la capa LLC,



(a) Arquitectura



(b) Operación

Figura 13.15. Conexión de dos redes LAN mediante un puente.

existe un diálogo entre las entidades LLC paritarias en las dos estaciones finales, no conteniendo el puente esta capa dado que su única función es la retransmisión de las tramas MAC.

En la Figura 13.15b se indica la forma en que se encapsulan los datos en un puente. Éstos se ofrecen al protocolo LLC por parte de algún usuario. La entidad LLC añade una cabecera y pasa la unidad de datos resultante a la entidad MAC, que añade una cabecera y una cola para dar lugar a una trama MAC. El puente captura la trama de acuerdo con la dirección MAC de destino especificada en ella, y, dado que su función es retransmitirla intacta a la LAN destino, no elimina los campos MAC. De esta forma, la trama se deposita en la LAN destino y es capturada por la estación destino.

El concepto de puente de retransmisión MAC no está limitado al uso de un único puente para conectar dos LAN adyacentes. Si las LAN están distanciadas, se pueden conectar a través de dos puentes intercomunicados. La comunicación entre los dos puentes puede consistir en una red, de conmutación de paquetes de área amplia por ejemplo, o en un enlace punto a punto. En estos casos, cuando un puente captura una trama MAC, debe encapsularla apropiadamente y transmitirla sobre la conexión hacia el otro puente, el cual eliminará los campos extra y transmitirá la trama MAC en su forma original a la estación de destino.

ENCAMINAMIENTO ESTÁTICO

Existe una tendencia en muchas organizaciones acerca del aumento del número de redes LAN interconectadas mediante puentes. Cuanto mayor es este número más importante resulta proporcionar rutas alternativas entre LAN a través de puentes para cuestiones de equilibrado de carga y reconfiguración en caso de aparición de fallos. De este modo, muchas organizaciones encuentran que las tablas de encaminamiento estáticas predefinidas resultan inadecuadas, siendo necesario algún tipo de encaminamiento dinámico.

Considérese la configuración dada en la Figura 13.16. Supongamos que la estación 1 transmite una trama sobre la LAN A con destino a la estación 6. La trama se recibirá en los puentes 101, 102 y 107, de forma que todos ellos determinarán que la estación de destino no se encuentra en una de las LAN a las que están conectados. Por tanto, cada puente tomará una decisión acerca de si retransmitir o no la trama sobre sus otras LAN con objeto de dirigirla hacia el destino deseado. En este caso, el puente 102 repetiría la trama sobre la LAN C, mientras que los puentes 101 y 107 decidirán no llevar a cabo la retransmisión de la trama. Una vez que la trama se ha enviado sobre la LAN C, se recibirá en los puentes 105 y 106, los cuales, como antes, deben decidir si retransmitirla o no. En caso de su retransmisión, el puente 105 puede hacerlo sobre la LAN F, donde la trama será finalmente recibida por la estación de destino 6.

Se observa que, en el caso general, el puente debe disponer de capacidad de encaminamiento, de modo que cuando un puente recibe una trama debe decidir si llevar a cabo o no su retransmisión. Si el puente se encuentra conectado a dos o más redes, debe decidir si retransmitir la trama o no y, en su caso, sobre qué LAN hacerlo.

La decisión de encaminamiento puede no resultar siempre tan sencilla. En la Figura 13.16 se muestra la existencia de dos rutas entre las LAN A y E. Esta redundancia proporciona una disponibilidad superior en la interconexión de las redes, posibilitando el equilibrado de la carga. En este caso, si la estación 1 transmite una trama a través de la LAN A dirigida a la estación 5 de la LAN E, los puentes 101 o 107 pueden retransmitir la trama. Parece más adecuado que sea el 107 quien lo haga dado que sólo necesita un salto, mientras que si lo hiciera el puente 101 se requerirían dos saltos. Una consideración adicional es que pueden producirse cambios en la configuración, de manera que, por ejemplo, el puente 107 puede fallar, en cuyo caso las tramas siguientes desde la estación 1 hacia la 5 deberían ir a través del puente 101. Por tanto, se puede decir que la capacidad de encaminamiento debe tener en consideración la topología de la configuración de interconexión entre redes y puede requerir ser alterada dinámicamente.

En los últimos años se han propuesto e implementado varias técnicas de encaminamiento. La más sencilla y comúnmente usada es la de **encaminamiento estático**. Esta estrategia resulta adecuada para

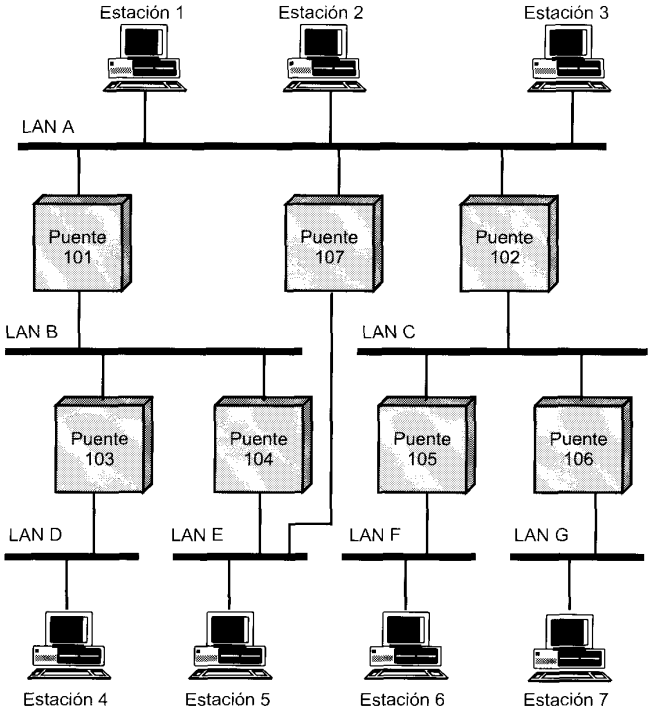


Figura 13.16. Configuración de puentes y redes LAN con rutas alternativas.

un número pequeño de redes LAN y para interconexiones relativamente estables. Adicionalmente, dos grupos del comité IEEE 802 han desarrollado especificaciones para estrategias de encaminamiento. El grupo IEEE 802.1 ha propuesto una normalización de encaminamiento basada en el uso del algoritmo del **árbol de expansión,** mientras que el comité de anillo con paso de testigo («token ring»), IEEE 802.5, ha propuesto su propia especificación, denominada **encaminamiento del origen**. En el resto de la sección se presentan las estrategias de encaminamiento estático y del árbol de expansión, que es el algoritmo de encaminamiento para puentes más usado.

En el encaminamiento estático se selecciona una ruta para cada pareja de LAN origen-destino en la configuración. Si se dispone de rutas alternativas entre dos LAN, generalmente se selecciona aquélla con menor número de saltos. Las rutas son fijas, o al menos sólo cambian cuando se produce un cambio en la topología de la interconexión.

La estrategia para llevar cabo una configuración de encaminamiento fija para puentes es similar a la empleada en una red de conmutación de paquetes (Figura 10.7). Se crea una matriz de encaminamiento central, almacenada quizá en un centro de control de red, que indica, para cada pareja de LAN origen-destino, la identidad del primer puente en la ruta. Así, por ejemplo, la ruta desde la LAN E a la LAN F comienza yendo a la LAN A a través del puente 107. Consultando de nuevo la matriz, la ruta desde la LAN A a la F pasa por el puente 102 para alcanzar la LAN C. Finalmente, la ruta desde la LAN C a la LAN F es directa a través del puente 105. Por tanto, la ruta completa desde la LAN E hasta la LAN F es puente 107, LAN A, puente 102, LAN C, puente 105.

Las tablas de encaminamiento se pueden obtener a partir de esta matriz y se guardan en cada puente. Cada puente precisa una tabla para cada una de las LAN a la que está conectado. La información de cada tabla se obtiene a partir de una sola entrada de la matriz; por ejemplo, el puente 105 tiene dos

tablas, una para las tramas recibidas de la LAN C y otra para las de la LAN F. La tabla muestra, para cada dirección MAC destino posible, la identidad de la LAN a la que el puente debería enviar la trama.

Una vez establecidas las tablas, el encaminamiento es una tarea sencilla. Un puente copia las tramas procedentes de cada una de sus LAN. Si la dirección MAC de destino corresponde con una entrada de su tabla de encaminamiento, la trama se retransmite a través de la LAN apropiada.

La estrategia de encaminamiento estático se usa ampliamente en los productos comerciales existentes, siendo necesaria la carga manual de las tablas de encaminamiento por parte de un administrador de red. Las principales ventajas de esta estrategia son su sencillez y sus mínimas necesidades de procesamiento. Sin embargo, en una interconexión compleja, en la que los puentes se pueden incorporar dinámicamente y pueden existir fallos, esta estrategia resulta demasiado limitada.

TÉCNICA DEL ÁRBOL DE EXPANSIÓN

El método del árbol de expansión es un mecanismo en el que los puentes desarrollan automáticamente una tabla de encaminamiento y la actualizan en respuesta a cambios en la topología. El algoritmo consta de tres mecanismos: retransmisión de tramas, aprendizaje de direcciones y mecanismo para evitar bucles.

Retransmisión de tramas

En este esquema, un puente mantiene una **base de datos de retransmisión** para cada puerto de conexión a una LAN. La base de datos indica las direcciones de estación para las que las tramas deben transmitirse sobre un puerto dado. Esto se puede interpretar de la siguiente forma: para cada puerto se mantiene una lista de estaciones situadas en el «mismo lado» del puente que el puerto. Por ejemplo, para el puente 102 de la Figura 13.16, las estaciones de las LAN C, F y G se encuentran en el mismo lado del puente que el puerto de la LAN C, y las estaciones de las LAN A, B, D y E están en el mismo lado del puente que el puerto de la LAN A. Cuando se recibe una trama por uno de los puertos, el puente debe decidir si la trama se enviará a través suyo y sobre cuál de los otros puertos se realizará la retransmisión. Suponiendo que un puente recibe una trama MAC a través del puerto x, se aplican las siguientes reglas:

1. Búsqueda en la base de datos de retransmisión para determinar si la dirección MAC se asocia a un puerto distinto de x.
2. Si no se encuentra la dirección MAC de destino, la trama se envía a través de todos los puertos excepto por el que llegó. Esto es parte de la técnica de aprendizaje que se describe más adelante.
3. Si la dirección de destino se encuentra en la base de datos para algún puerto y, se determina si ese puerto se encuentra en estado de bloqueo o de envío. Por razones que se explicarán más adelante, un puerto puede estar a veces bloqueado, lo que le impide emitir o recibir tramas.
4. Si el puerto y no está bloqueado, se transmite la trama a través de ese puerto sobre la LAN a la que se encuentra conectado.

Aprendizaje de direcciones

El esquema anterior se basa en la existencia en los puentes de una base de datos de transmisión que indica la dirección de cada estación destino desde el puente en cuestión. Como en el caso del encaminamiento estático, esta información puede cargarse a priori en el puente. Sin embargo, sería deseable un mecanismo automático efectivo para aprender las direcciones de cada estación. Un esquema sencillo para conseguir esta información se basa en el empleo del campo de dirección origen presente en las tramas MAC.

La estrategia es como sigue. Cuando se recibe una trama por un puerto dado, es claro que viene desde la dirección de la LAN entrante. El campo de dirección origen de la trama indica la estación emisora, de modo que un puente puede actualizar su base de datos de retransmisión a partir de esa dirección MAC. Con el fin de permitir cambios en la topología, cada entrada en la base de datos dispone de un temporizador. Cuando se añade una nueva entrada a la base de datos, se activa el temporizador asociado. Si éste expira, se elimina la entrada de la base de datos dado que la información de dirección correspondiente puede no ser válida por más tiempo. Cada vez que se recibe una trama se comprueba su dirección origen en la base de datos. Si se encuentra como entrada ya en ésta, se actualiza (la dirección puede haber cambiado) y se reinicia el temporizador. Si la entrada, por el contrario, no está en la base de datos, se crea una nueva con su propio temporizador.

Algoritmo del árbol de expansión

El mecanismo de aprendizaje de direcciones descrito anteriormente es efectivo si la topología de la interconexión de redes en un árbol; es decir, si no existen rutas alternativas en la red. La existencia de rutas alternativas implica la aparición de bucles cerrados. Por ejemplo, la siguiente ruta en la Figura 13.16 es un bucle cerrado: LAN A, puente 101, LAN B, puente 104, LAN E, puente 107, LAN A.

Para analizar el problema creado por la existencia de un bucle cerrado consideremos la Figura 13.17. La estación A transmite una trama destinada a la estación B en el instante de tiempo t_0. Ambos puentes capturan esta trama y actualizan sus bases de datos para indicar que la estación A se encuentra en la dirección de la LAN X, y retransmiten la trama a través de la LAN Y. Supongamos que el puente α la retransmite en el instante de tiempo t_1 y el puente β un poco después, en t_2. Así, B recibirá dos copias de la trama. Además, cada puente recibirá las transmisiones de los otros a través de la LAN Y. Obsérvese que cada transmisión es una trama MAC con la dirección origen de A y la dirección destino de B, con lo que cada puente actualizará su base de datos para indicar que la estación A se encuentra en la dirección de la LAN Y. Ningún puente es capaz ahora de retransmitir una trama dirigida a la estación A.

Para solucionar este problema se utiliza un sencillo resultado de la teoría de grafos: para cualquier grafo conectado, compuesto de nodos y de terminales que conectan cada par de nodos, existe un árbol de expansión de terminales que mantiene la conectividad del grafo pero no contiene bucles cerrados. En

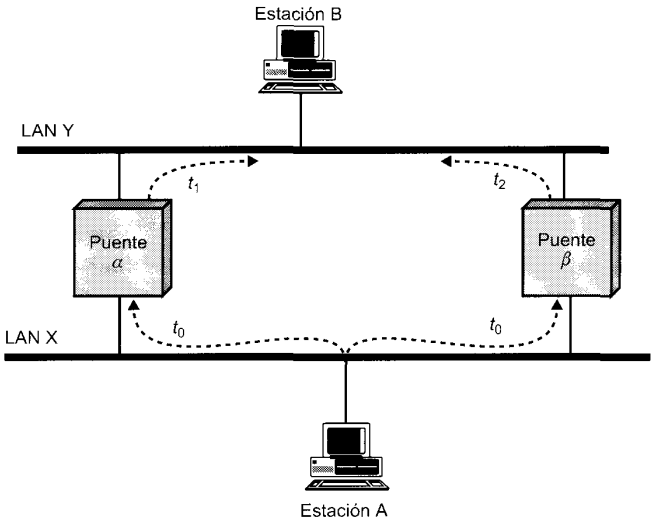


Figura 13.17. Bucle de puentes.

términos de interconexión, cada red LAN se corresponde con un nodo del grafo y cada puente con un terminal. Así, en la Figura 13.16, la eliminación de uno (y sólo uno) de los puentes 107, 101 y 104 da lugar a un árbol de expansión. Resulta deseable el desarrollo de un algoritmo sencillo mediante el que los puentes de la interconexión puedan intercambiar información suficiente (sin intervención de los usuarios) para obtener el árbol de expansión. El algoritmo debe ser dinámico; es decir, los puentes deben ser capaces de percatarse ante un cambio en la topología y obtener automáticamente un nuevo árbol de expansión.

El algoritmo del árbol de expansión desarrollado por IEEE 802.1, como su propio nombre sugiere, puede desarrollar dicho árbol de expansión. Todo lo que se precisa es que cada uno de los puentes tenga asignado un identificador único y se asocien costes a cada uno de los puertos de los puentes. Aparte de cualquier consideración especial, todos los costos podrían ser iguales, lo que produciría un árbol de menor número de saltos. El algoritmo implica el intercambio de un número reducido de mensajes entre todos los puentes para obtener el árbol de expansión de mínimo coste. Cuando se produzca un cambio en la topología los puentes recalcularán automáticamente el árbol de expansión.

13.8 LECTURAS Y SITIOS WEB RECOMENDADOS

La bibliografía acerca de redes LAN y MAN es extensa. Los temas tratados en este capítulo se desarrollan en mayor profundidad en [STAL00]. [NAUG96] ofrece una revisión interesante del cableado de redes LAN, proporcionando [TRUL97] un estudio más detallado del mismo.

[PAHL95] y [BANT94] son artículos excelentes sobre LAN inalámbricas. Por su parte, [KAHN97] presenta un buen estudio de LAN de infrarrojos. Finalmente, [GEIR99] es un excelente libro donde se realiza una amplia cobertura de la tecnología inalámbrica, los estándares IEEE 802.11 y numerosos casos prácticos.

BANT94 Bantz, D., y Bauchot, F. «Wireless LAN Design Alternatives.» *IEEE Network*, March/April, 1994.

GEIE99 Geier, J. *Wireless LANs*. New York: Macmillan Technical Publishing, 1999.

KAHN97 Kahn, J., y Barry, J. «Wireless Infrared Communications.» *Proceedings of the IEEE*, February 1997.

NAUG96 Naugle, M. *Local Area Networking*. New York: McGraw-Hill, 1996.

PAHL95 Pahlavan, K.; Probert, T.; y Chase, M. «Trends in Local Wireless Networks.» *IEEE Communications Magazine*, March 1995.

STAL00 Stallings, W. *Local and Metropolitan Area Networks, 6th edition*. Upper Saddle River, NJ: Prentice Hall, 2000

TRUL97 Trulove, J. *LAN Wiring*. New York: McGraw-Hill, 1997.

SITIOS WEB RECOMENDADOS

- **Alianza de LAN inalámbricas:** presenta la tecnología LAN inalámbrica, incluyendo una discusión acerca de consideraciones de implementación, y casos prácticos de usuarios. Dispone también de enlaces a sitios relacionados.
- **Comité de normalización LAN/MAN IEEE 802:** estado y documentos de todos los grupos de trabajo.

13.9. PROBLEMAS

13.1. ¿Se podría usar HDLC como protocolo de control de enlace de datos en una LAN? ¿Por qué?

13.2. Un dispositivo asíncrono, como, por ejemplo, un teletipo, transmite caracteres uno a uno con retardos impredecibles entre ellos. ¿Qué problemas pueden aparecer, si es que hay alguno, si un dispositivo así se conecta a una red local y se le permite transmitir a voluntad (sujeto a conseguir el acceso al medio)? ¿Cómo se podrían solucionar estos problemas?

13.3. Considérese la transferencia de un fichero que contiene un millón de caracteres de 8 bits desde una estación a otra. Indique el tiempo consumido y el rendimiento efectivo para los siguientes casos:

a) Una topología en estrella con conmutación de circuitos. Suponga que el tiempo de establecimiento de llamada es despreciable y que la velocidad de transmisión del medio es 64 kbps.

b) Una topología en bus con dos estaciones distanciadas D, una velocidad de transmisión de B bps y un tamaño de paquete P con 80 bits suplementarios. Cada paquete se confirma mediante un paquete de 88 bits antes de que se envíe el siguiente. La velocidad de propagación en el bus es de 200 m/μs. Resuelva para:

(1) D = 1 km, B = 1 Mbps, P = 256 bits
(2) D = 1 km, B = 10 Mbps, P = 256 bits
(3) D = 10 km, B = 1 Mbps, P = 256 bits
(4) D = 1 km, B = 50 Mbps, P = 10.000 bits

c) Una topología en anillo con una longitud circular total de $2D$, con una distancia D entre las dos estaciones. La confirmación se realiza permitiendo a la estación destino dejar pasar los paquetes hacia la estación origen. Existen N repetidores en el anillo, cada uno de los cuales introduce un retardo igual al tiempo de duración de un bit. Repita el cálculo para cada una de las situaciones (1) a (4) del apartado anterior para N = 10, 100 y 1.000.

13.4. Considere un bus de banda base con varias estaciones equidistantes con una velocidad de transmisión de 10 Mbps y una longitud del bus de 1 km.

a) ¿Cuál es el tiempo medio para enviar una trama de 1.000 bits a otra estación, medido desde el comienzo de la transmisión hasta el final de la recepción? Suponga una velocidad de propagación de 200 m/μs.

b) Si dos estaciones comienzan a transmitir exactamente al mismo tiempo, sus paquetes interferirán entre sí. Si cada estación transmisora monitoriza el bus durante la transmisión, ¿cuánto tiempo antes, en segundos, se percata de la ocurrencia de una interferencia? ¿Y en intervalos de duración de un bit?

13.5. Repita el Problema 13.4 para una velocidad de transmisión de 100 Mbps.

13.6. Para una velocidad de propagación de 200 m/μs, ¿cuál es la longitud efectiva añadida a un anillo para un retardo de bit en cada repetidor de:

a) 1 Mbps?
b) 40 Mbps?

13.7. Para unir dos edificios se utiliza una topología en árbol. Si se puede conseguir el permiso para colocar el cable entre los dos edificios, se utiliza un esquema de árbol continuo. En caso contrario, cada edificio tendrá una red de topología en árbol independiente y un enlace punto a punto conectará una estación de comunicaciones especial en una red con una estación de comunica-

ciones en la otra red. ¿Qué funciones deben realizar las estaciones de comunicaciones? Repita el proceso para un anillo y una estrella.

13.8. Un sistema A consiste en un anillo simple con 300 estaciones, una por repetidor. Un sistema B consta de tres anillos con 100 estaciones cada uno unidos por un puente. Si la probabilidad de fallo en un enlace es P_l, en un repetidor es P_r y en un puente es P_b, obtenga una expresión para:

a) Probabilidad de fallo del sistema A.

b) Probabilidad de fallo completo del sistema B.

c) Probabilidad de que una estación particular no encuentre disponible la red, para los sistemas A y B.

d) Probabilidad de que cualesquiera dos estaciones, elegidas aleatoriamente, no puedan comunicarse, para los sistemas A y B.

e) Calcule los valores para los apartados (a) a (d) con $P_l = P_b = P_r = 10^{-2}$.

13.9. Dibuje una figura similar a la Figura 13.15 para una configuración en la que

a) Se conectan dos redes LAN a través de dos puentes conectados mediante un enlace punto a punto.

b) Se conectan dos LAN a través de dos puentes conectados mediante una red de conmutación de paquetes X.25.

13.10. Especifique la matriz de encaminamiento central y las tablas de encaminamiento de cada uno de los puentes de la configuración dada en la Figura 13.16.

13.11. El protocolo MAC en redes en anillo con paso de testigo especifica que los bits A y C pueden ser activados por una estación en el anillo para indicar, respectivamente, reconocimiento de la dirección y copia de la trama. Esta información se encuentra así disponible para la estación origen cuando la trama vuelve a ésta tras haber circulado alrededor del anillo. Si un puente captura una trama y la retransmite, ¿debería activar los bits A y C? Ponga un ejemplo de ambos criterios.

APÉNDICE 13A. ESTÁNDARES IEEE 802

La clave para el desarrollo del mercado de redes LAN es la disponibilidad de una interfaz de bajo coste. El coste de conectar un equipo a una LAN debe ser mucho menor que el del equipo en sí. Este requisito, adicionalmente a la complejidad de la lógica de la LAN, establece una solución basada en el empleo de circuitos integrados y de técnicas de integración a muy alta escala (VLSI). Sin embargo, los fabricantes de circuitos integrados son reacios a invertir los recursos necesarios a menos que exista un gran mercado. Un estándar LAN ampliamente aceptado asegura este volumen de demanda al tiempo que posibilita la intercomunicación de equipos de distintos fabricantes. Éste es el objetivo del comité IEEE 802.

El comité ha definido varias normalizaciones, adoptadas en 1985 por el Instituto de Estandarización Nacional Americano (ANSI) como Estándares Nacionales Americanos. Estos estándares han sido sucesivamente revisados y redefinidos como estándares internacionales por la Organismo Internacional de Estandarización (ISO) en 1987, bajo la denominación ISO 8802. Desde entonces, el comité IEEE 802 ha continuado con la revisión y ampliación de los estándares, adoptados últimamente por ISO.

El comité llegó a dos conclusiones. La primera es que la tarea de comunicaciones a través de una red local es suficientemente compleja como para ser descompuesta en subtareas más manejables. El resultado de esto fue el modelo de referencia IEEE 802 presentado al principio de este capítulo (Figura 13.1).

La segunda conclusión es que ninguna aproximación técnica cumplirá todos los requisitos. A esta conclusión se llegó cuando se hizo patente que un solo estándar no satisfaría a todos los participantes del comité, previéndose soporte así para varias topologías, métodos de acceso y medios de transmisión. La respuesta del comité fue la normalización de todas las propuestas serias en lugar de intentar establecer sólo una. El estado actual de la normalización se refleja en la existencia de numerosos subcomités en IEEE 802 y el trabajo realizado por cada uno de ellos. Son los siguientes:

- **Grupo de trabajo en protocolos LAN de capas superiores 802.1:** generalidades y arquitectura, interconexión con puentes, LAN puenteadas virtualmente (VLAN).
- **Grupo de trabajo en control de enlace lógico 802.2:** inactivo.
- **Grupo de trabajo en Ethernet 802.3:** método de acceso y señalización física.
- **Grupo de trabajo en redes en bus con paso de testigo («token bus») 802.4:** método de acceso y señalización física (inactivo).
- **Grupo de trabajo en redes en anillo con paso de testigo («token ring») 802.5:** método de acceso y señalización física.
- **Grupo de trabajo en redes de área metropolitana 802.6:** método de acceso y señalización física (inactivo).
- **TAG de banda ancha 802.7:** grupo asesor en tecnologías de banda ancha (inactivo).
- **TAG de fibra óptica 802.8:** grupo asesor en tecnologías de fibra óptica.
- **Grupo de trabajo en LAN isócronas 802.9:** método de acceso y señalización física.
- **Grupo de trabajo en seguridad 802.10:** diversos niveles de seguridad para todos los estándares IEEE 802.
- **Grupo de trabajo en LAN inalámbricas 802.11:** método de acceso y señalización física.
- **Grupo de trabajo en demanda de prioridad 802.12:** método de acceso y señalización física
- **802.13:** no usado.
- **Grupo de trabajo en cable modem 802.14.**
- **Grupo de trabajo en redes inalámbricas de área personal 802.15:** estándares para redes inalámbricas para cubrir distancias cortas.
- **Grupo de estudio de acceso inalámbrico de banda ancha 802.16.**
- **Grupo de estudio QoS/control de flujo.**

CAPÍTULO 14

Sistemas LAN

- El IEEE 802 ha desarrollado una serie de estándares. En cada estándar se especifica la técnica de acceso al medio (MAC, Medium Access Control), además de diversas opciones de medios de transmisión con distintas velocidades.
- El protocolo LAN 802 más utilizado es el 802.3, basado en las especificaciones iniciales de Ethernet.
- Una aproximación potente y flexible es la utilizada en las LAN ATM. Este tipo de LAN generaliza la tecnología y protocolos ATM, desarrolladas para entornos de área amplia, al contexto de las redes corporativas. Estas LAN son interesantes debido a la posibilidad que ofrece ATM para integrar flujos de datos, voz, imágenes, y vídeo, además de que esta tecnología está íntimamente relacionada con las WAN ATM.
- Otra aproximación para la implementación de LAN es el Canal de Fibra Óptica, utilizado en las redes de almacenamiento (SAN, Storage Area Network). Esta tecnología está desarrollada para estaciones de trabajo de altas prestaciones o servidores, así como para la conexión directa de dispositivos de E/S de alta velocidad.
- El IEEE 802 ha desarrollado además un estándar para LAN inalámbricas, utilizando tecnologías de infrarrojos y de espectro expandido.

A continuación se consideran específicamente los sistemas LAN. Como se mencionó en el Capítulo 13, tanto la topología como las técnicas de control de acceso al medio son características fundamentales para la clasificación de las redes LAN y para el desarrollo de normalizaciones. En este capítulo se estudian los siguientes sistemas:

- Ethernet (CSMA/CD).
- Anillo con paso de testigo/FDDI.
- Redes LAN ATM.
- Canales de fibra óptica.
- Redes LAN inalámbricas.

14.1. ETHERNET (CSMA/CD)

La técnica de control de acceso al medio más ampliamente usada en las topologías en bus y en estrella es la de acceso múltiple sensible a la portadora con detección de colisiones (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). La versión original en banda base de esta técnica fue desarrollada por Xerox para redes LAN Ethernet, este desarrollo fue la base para la posterior especificación del estándar IEEE 802.3.

En esta sección nos centraremos en el estándar IEE 802.3. Como en el caso de otras normalizaciones LAN, existe tanto una capa de control de acceso al medio como una capa física, ambas estudiadas a continuación.

CONTROL DE ACCESO AL MEDIO EN IEE 802.3

El funcionamiento de la técnica CSMA/CD se puede entender más fácilmente si primero se estudian los esquemas a partir de los que evolucionó.

Precursores

La técnica CSMA/CD y sus precursoras pueden ser denominadas de acceso aleatorio o de contención. Se denominan de acceso aleatorio en el sentido de que no existe un tiempo preestablecido o predecible para que las estaciones transmitan; la transmisión se realiza aleatoriamente. Son de contención en el sentido de las estaciones compiten para conseguir el acceso al medio.

La primera de estas técnicas, conocida como ALOHA, se desarrolló para redes de paquetes de radio, siendo, a pesar de ello, aplicable a cualquier medio de transmisión compartido. En ALOHA cuando una estación tiene que transmitir una trama lo hace, pasando después a escuchar el medio durante un tiempo igual al máximo retardo de propagación posible de ida y vuelta a través de la red (igual a dos veces el tiempo de propagación de una trama entre las dos estaciones más separas) más un pequeño incremento fijo de tiempo. Si durante este intervalo de escucha la estación oye una confirmación, perfecto; si no, retransmitirá la trama. Si la estación no recibe una confirmación después de varias retransmisiones, desistirá. La estación receptora determina si una trama recibida es correcta examinando el campo de la secuencia de comprobación de la trama, al igual que se hace en HDLC. Si la trama es válida y la dirección de destino en la cabecera de la trama coincide con la de la receptora, la estación devuelve inmediatamente una confirmación. La trama puede ser incorrecta debido a la presencia de ruido en el canal o debido a que otra estación transmitió una trama casi al mismo tiempo. En el último caso, las dos tramas pueden interferir entre sí en el receptor de modo que no se acepte ninguna; esto se conoce como *colisión*. Si se decide que la trama recibida no es válida, la estación receptora simplemente ignorará la trama.

ALOHA es extremadamente sencilla, y debido a esta sencillez presenta algunos puntos débiles. Dado que el número de colisiones crece rápidamente cuando aumenta la carga, la utilización máxima del canal es sólo del orden del 18 por ciento (véase [STAL00]).

Para mejorar la eficiencia se desarrolló una modificación sobre ALOHA, conocida como ALOHA ranurado. En este esquema el tiempo del canal se hace discreto, considerando ranuras uniformes de duración igual al tiempo de transmisión de una trama, para este fin es necesario el uso de un reloj central u otra técnica que permita sincronizar todas las estaciones. La transmisión sólo se permite en los instantes de tiempo que coincidan con el comienzo de una ranura. Así, las tramas que se solapen lo harán completamente, lo que incrementa la utilización máxima del sistema hasta el 37 por ciento aproximadamente.

Tanto ALOHA como ALOHA ranurado presentan una utilización baja del canal. Ninguna de las dos técnicas aprovecha una de las propiedades más importante en las redes de paquetes de radio y redes LAN, consistente en que el retardo de propagación entre las estaciones es generalmente muy pequeño en comparación con el tiempo de transmisión de las tramas[1]. Consideremos las siguientes observaciones. Si el tiempo de propagación entre estaciones fuese grande en comparación con el tiempo de transmisión, entonces, tras la transmisión de una trama deberá transcurrir mucho tiempo antes de que otras estaciones constaten este hecho. Una de las otras estaciones puede transmitir una trama durante este intervalo de tiempo, de modo que las dos tramas pueden interferir entre sí y no se aceptará ninguna de ellas. De hecho, si las distancias son suficientemente grandes, pueden comenzar a transmitir varias estaciones, una tras otra, y ninguna de sus tramas resultará ilesa. Supongamos, sin embargo, que el tiempo de propagación es pequeño comparado con el de transmisión. En este caso, cuando una estación transmita una trama, el resto de estaciones lo sabrán casi inmediatamente. De esta manera, si pueden constatar esta circunstancia de algún modo, no intentarán transmitir hasta que lo haya hecho la primera. Las colisiones no serán habituales ya que sólo ocurrirán cuando dos estaciones comiencen a transmitir casi simultáneamente. Otra forma de verlo es que un tiempo de retardo pequeño proporciona a las estaciones una mejor realimentación sobre el estado de la red; esta información se puede usar para mejorar la eficiencia.

[1] Esta afirmación es cierta para Ethernet a 10-Mbps, pero no lo es para 100-Mbps o Ethernet a 1-Gbps. En estos casos, es preferible utilizar una aproximación conmutada (Figura 13.12c) en lugar de CSMA/CD.

Estas observaciones condujeron al desarrollo de la técnica de acceso múltiple sensible a la portadora (CSMA). Con CSMA, una estación que desee transmitir, primero escuchará el medio para determinar si existe alguna otra transmisión en curso (sensible a la portadora). Si el medio se está usando, la estación deberá esperar. En cambio, si éste se encuentra libre, la estación podrá transmitir. Puede suceder que dos o más estaciones intenten transmitir aproximadamente al mismo tiempo, en cuyo caso se producirá colisión: los datos de ambas transmisiones interferirán y no se recibirán con éxito. Para solucionar esto, las estaciones aguardan una cantidad de tiempo razonable después de transmitir en espera de una confirmación, teniendo en consideración el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión y retransmite.

Podemos ver cómo esta estrategia resulta efectiva para redes en las que el tiempo de transmisión de trama es mucho mayor que el de propagación. Las colisiones sólo se producirán en el caso de que más de un usuario comience a transmitir dentro del mismo intervalo de tiempo (igual al período de propagación). Si una estación comienza a transmitir una trama y no existen colisiones durante el tiempo de propagación que transcurre desde el inicio de la transmisión del paquete hasta que alcanza a la estación más lejana, no se producirá colisión para esta trama dado que ahora todas las estaciones están enteradas de la transmisión.

La utilización máxima que se puede conseguir haciendo uso de CSMA puede superar con mucho la del ALOHA ranurado. La utilización máxima depende de la longitud de la trama y del tiempo de propagación; cuanto mayor sea la longitud de las tramas o cuanto menor sea el tiempo de propagación, mayor será la utilización. Esta cuestión se trata en el Apéndice 14B.

En CSMA se necesita un algoritmo que determine qué debe hacer una estación si encuentra el medio ocupado. La técnica denominada 1-*persistente* es la aproximación más usual, y es la utilizada en IEE 802.3. Una estación que desee transmitir escuchará el medio y actuará de acuerdo con las siguientes reglas:

1. Si el medio se encuentra libre, transmite; si no se aplica la regla 2.
2. Si el medio está ocupado, continúa escuchando hasta que el canal se detecta libre, entonces transmite inmediatamente.

Se producirá colisión, siempre que dos o más estaciones estén en espera de transmitir. Esta técnica sólo toma medidas tras la colisión.

Descripción de CSMA/CD

CSMA, aunque más eficiente que ALOHA y ALOHA ranurado, es también claramente ineficiente. Cuando colisionan dos tramas, el medio estará inutilizado mientras dure la transmisión de ambas. La capacidad desaprovechada, en comparación con el tiempo de propagación puede ser considerable para tramas largas. Este desaprovechamiento puede reducirse si una estación continúa escuchando el medio mientras dura la transmisión, lo que conduce a las siguientes reglas para la técnica CSMA/CD:

1. La estación transmite si el medio está libre, si no se aplica la regla 2.
2. Si el medio se encuentra ocupado, la estación continúa escuchando hasta que encuentra libre el canal, en cuyo caso transmite inmediatamente.
3. Si se detecta una colisión durante la transmisión, las estaciones transmiten una señal corta de alerta para asegurarse de que todas las estaciones constatan la colisión y cesan de transmitir.
4. Después de transmitir la señal de alerta se espera un intervalo de tiempo de duración aleatoria, tras el cual se intenta transmitir de nuevo (volviendo al paso 1).

La Figura 14.1 ilustra la técnica para el caso de un bus en banda base. La estación A comienza a transmitir un paquete con destino D en el instante de tiempo t_0. Tanto B como C están dispuestas para transmitir en t_1. B detecta una transmisión y aplaza la suya. Sin embargo, C aún no se ha percatado de la

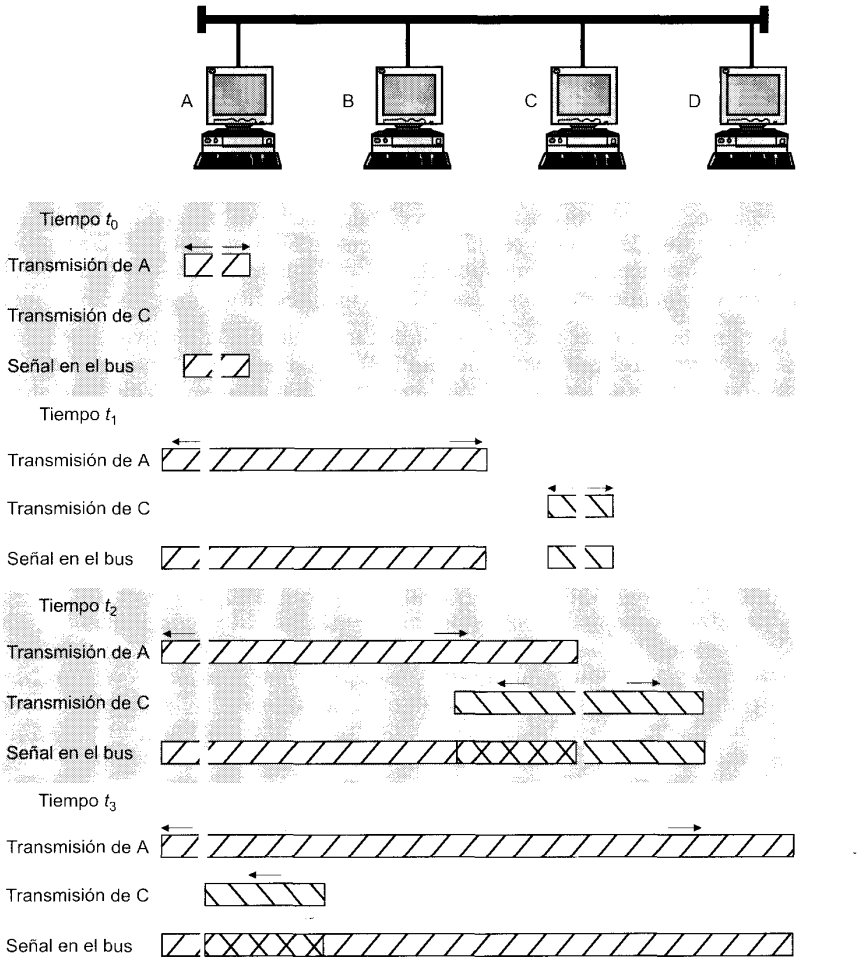


Figura 14.1. Funcionamiento de CSMA/CD.

transmisión de A (debido a que el primer bit de la transmisión de A todavía no ha alcanzado a C) y comienza a transmitir. Cuando la transmisión de A llega a C, en t_2, ésta detecta la colisión y cesa de transmitir. El efecto de la colisión se propaga hacia A, donde se detecta en un instante posterior, t_3, siendo en este momento cuando A deja de transmitir.

La capacidad desaprovechada en CSMA/CD se reduce al tiempo que se tarda en detectar la colisión. Pregunta: ¿qué tiempo es éste? Considérese primero el caso de un bus en banda base y dos estaciones tan distantes como sea posible. Por ejemplo, en la Figura 14.1 supóngase que la estación A comienza a transmitir y que justo antes de que esta transmisión alcance a D, ésta está dispuesta a transmitir. D empezará a transmitir debido a que todavía no es consciente de la transmisión de A. Casi inmediatamente se producirá colisión, siendo detectada por D. Sin embargo, la colisión debe propagarse a lo largo del camino hacia A, para que ésta constate la ocurrencia del suceso. De acuerdo con este razonamiento, se concluye que el tiempo involucrado en detectar la colisión no es mayor que dos veces el retardo de propagación extremo a extremo.

Una regla importante aplicada en la mayor parte de los sistemas CSMA/CD, incluyendo a las normalizaciones IEEE, consiste en que la trama debe ser lo suficientemente larga como para permitir la detección de la colisión antes de que finalice la transmisión. Si se usan tramas más cortas, no se produce la detección de la colisión, presentando la técnica CSMA/CD las mismas prestaciones que el protocolo CSMA menos eficiente.

Para mantener la estabilidad del sistema, la cantidad de retardo en el paso 4 se obtiene mediante la técnica denominada espera exponencial binaria. En esta técnica, la estación intentará transmitir por cada vez que colisione, si bien, tras cada colisión el valor medio del tiempo de espera se hace doble. Tras 16 intentos infructuosos, la estación cejará en su intento e informará sobre el error acontecido. De esta manera, cuando se incremente la congestión en el sistema, las estaciones tendrán que esperar más, para así reducir la probabilidad de colisión.

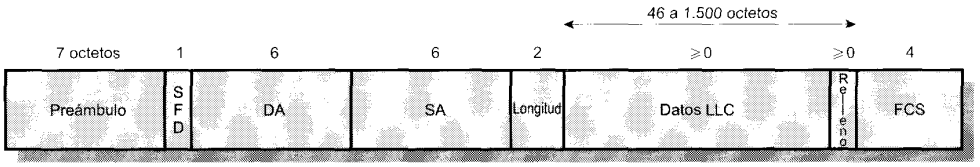
En buses en banda base, una colisión implicará la aparición de niveles de tensión superiores a los que cabría esperar en el caso de una transmisión sin colisiones. Consecuentemente, el estándar IEEE dicta que el transmisor detectará una colisión si la señal presente en el cable en el punto de conexión es mayor que el máximo nivel que se podría producir si se tratara de una única transmisión. Debido a que la señal se atenúa con la distancia aparece un problema potencial: si dos estaciones muy distantes están transmitiendo, la señal que reciban la una de la otra estará muy atenuada. La energía de la señal recibida podría ser tan pequeña que una vez sumada a la señal transmitida en el punto de conexión, pudiera ocurrir que la señal combinada no superara el umbral de continua (DC) preestablecido. Esta razón, además de otras, es la que ha justificado que el estándar de IEEE restrinja la longitud máxima del cable coaxial a 500 m en el 10BASE5, y a 200 m en el 10BASE2.

En la topología en estrella con pares trenzados (Figura 13.9) es posible utilizar un esquema para la detección de colisiones mucho más sencillo. En este caso la detección de colisiones se basa en magnitudes lógicas, en lugar de utilizar niveles de tensión. En cualquiera de los concentradores («hubs») si hay actividad (señal) en más de una entrada se concluye que hay colisión, generándose en este caso una señal especial denominada señal presencia de colisión. Esta señal se genera y se envía mientras se detecte actividad en cualquiera de las líneas de entrada, y es interpretada por todos los nodos como la producción de una colisión.

Trama MAC

La Figura 14.2 muestra el formato de la trama del protocolo 802.3. Ésta consta de los siguientes campos:

- **Preámbulo:** el receptor usa un octeto patrón de 7 bits ceros y unos alternados para establecer la sincronización entre el emisor y el receptor.
- **Delimitador del comienzo de la trama (SFD, start frame delimiter):** consiste en la secuencia de bits 10101011, e indica el comienzo real de la trama y posibilita al receptor localizar el primer bit del resto de la trama.



SFD = (Delimitación de comienzo de trama, "stard of frame delimiter")
DA = (Dirección destino, "destination address")
SA = (Dirección origen, "source address")
FCS = (Secuencia de comprobación de trama, "frame check sequence")

Figura 14.2. Formato de la trama IEEE 802.3.

- **Dirección de destino (DA, destination address):** especifica la estación o estaciones a las que va dirigida la trama. Esta estación puede ser una única dirección física, una dirección de grupo o una dirección global.
- **Dirección de origen (SA, source address):** especifica la estación que envió la trama.
- **Longitud/tipo:** contendrá la longitud del campo de datos LLC expresado en octetos, o el campo Tipo de Ethernet, dependiendo de que la trama siga la norma IEEE 802.3 o la especificación primitiva de Ethernet. En cualquier caso, el tamaño máximo de la trama, excluyendo el preámbulo y el SFD, es 1.518 octetos.
- **Datos LLC:** unidad de datos proporcionada por el LLC.
- **Relleno:** octetos añadidos para asegurar que la trama sea lo suficientemente larga tal que la técnica de detección de colisiones (CD) funcione correctamente.
- **Secuencia de comprobación de trama (FCS, frame check sequence):** comprobación redundante cíclica de 32 bits, calculada teniendo en cuenta todos los campos excepto el de preámbulo, el SFD y el FCS.

ESPECIFICACIONES IEEE 802.3 A 10 MBPS (ETHERNET)

El comité IEEE 802.3 ha sido el más activo en la definición de configuraciones físicas alternativas. Esta actividad tiene sus ventajas e inconvenientes. Lo positivo es que la normalización responde a la evolución de la tecnología, mientras que el aspecto negativo es que el consumidor, y no digamos el potencial proveedor, se encuentra con una gran variedad de opciones. Sin embargo, el comité ha trabajado mucho para asegurar que las distintas opciones puedan ser integradas fácilmente en una configuración que satisfaga un gran número de necesidades. Así, el usuario que tiene un conjunto complejo de requisitos puede encontrar una ventaja en la flexibilidad y en la variedad del estándar 802.3.

El comité ha desarrollado una notación concisa con el fin de distinguir las diferentes implementaciones disponibles:

⟨velocidad de transmisión en Mbps⟩⟨método de señalización⟩
⟨longitud máxima del segmento en centenas de metros⟩

Las alternativas definidas son[2]:

- 10BASE5
- 10BASE2
- 10BASE-T
- 10BASE-F

Obsérvese que 10BASE-T y 10BASE-F no siguen la notación: «T» se usa para par trenzado, y «F» para fibra óptica. La Tabla 14.1 resume estas opciones. Todas las alternativas enumeradas en la tabla especifican una velocidad de datos de 10 Mbps. Además de estas alternativas, existen varias versiones que funcionan a 100 Mbps y un 1Gbps, que se estudian en la última parte de esta sección.

Especificación del medio 10BASE5

10BASE5 es la especificación del medio original en 802.3, y se basa directamente en Ethernet. 10BASE5 especifica el uso de cable coaxial de 50 ohmios y señalización digital Manchester[3]. La longitud

[2] Existe también la opción 1BASE-T, que define un sistema de par trenzado a 1-Mbps usando una topología en estrella. Esta opción está obsoleta. Está también la opción 10BROAD36, que corresponde a un bus en banda ancha, esta opción se usa muy poco.
[3] Véase Sección 5.1.

Tabla 14.1. Alternativas para el medio de transmisión en la capa física IEEE 802.3 a 10 Mbps.

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Medio de transmisión	Cable coaxial (50 ohm)	Cable coaxial (50 ohm)	Par trenzado no apantallado	Par de fibra óptica a 850 nm
Técnica de señalización	Banda base (Manchester)	Banda base (Manchester)	Banda base (Manchester)	Manchester/ on-off
Topología	Bus	Bus	Estrella	Estrella
Longitud máxima del segmento (m)	500	185	100	500
Nodos por segmento	100	30	—	33
Diámetro del cable (mm)	10	5	0,4-0,6	62,5/125 μm

máxima del segmento de cable se fija a 500 metros. Esta longitud se puede extender mediante la utilización de repetidores. Un repetidor es transparente al nivel MAC; y dado que no gestiona memoria temporal, no aísla un segmento de otro. Así, por ejemplo, si dos estaciones en diferentes segmentos intentan transmitir al mismo tiempo, sus transmisiones colisionarán. Para evitar la aparición de bucles sólo se permite un único camino formado por segmentos y repetidores entre cualesquiera dos estaciones. La normalización permite un máximo de cuatro repetidores en el camino entre cualesquiera dos estaciones, ampliándose así la longitud efectiva del medio hasta 2,5 kilómetros.

Especificación del medio 10BASE2

10BASE2 se introdujo con el fin de proporcionar un sistema menos costoso que 10BASE5 para redes LAN de computadores personales. Al igual que en 10BASE5, esta especificación utiliza cable coaxial de 50 ohmios y señalización Manchester. La principal diferencia es que 10BASE2 emplea un cable más fino, que admite tomas de conexión para distancias más cortas que el cable de 10BASE5.

Dado que 10BASE2 y 10BASE5 usan la misma velocidad de transmisión, es posible mezclar en la misma red segmentos de ambas especificaciones. Para ello se usa un repetidor adaptado a 10BASE5 por una parte y a 10BASE2 por la otra. La única restricción consiste en que el segmento 10BASE2 no se debería usar para conectar dos segmentos 10BASE5, ya que el segmento troncal («backbone») debería ser tan inmune al ruido como lo son los segmentos que conecta.

Especificación del medio 10BASE-T

Si se sacrifica algo la separación máxima entre cualesquiera dos estaciones, se puede desarrollar una LAN a 10 Mbps haciendo uso de par trenzado no apantallado. Este tipo de cable está instalado en edificios corporativos y de negocios como cable para uso telefónico, por lo que puede usarse para redes LAN. Esta aproximación se establece en la especificación 10BASE-T, en la que se define una topología en estrella. Una configuración simple puede consistir en varias estaciones conectadas a un punto central, denominado repetidor multipuerto, mediante pares trenzados. El punto central acepta la entrada a través de una línea, y la repite en todas las otras líneas.

Las estaciones se conectan al repetidor multipuerto mediante un enlace punto a punto, que consta generalmente de dos pares trenzados no apantallados. Debido a la alta velocidad y pobre calidad de la transmisión en el par trenzado no apantallado, la longitud máxima de un enlace está limitada a 100 metros. Como alternativa, se puede usar un enlace de fibra óptica, en cuyo caso la longitud máxima es de 500 m.

Especificación del medio 10BASE-F

La especificación 10BASE-F permite al usuario aprovechar las excelentes propiedades de distancia y de transmisión que exhibe la fibra óptica. El estándar contiene realmente tres especificaciones:

- **10-BASE-FP (pasiva):** topología en estrella pasiva para interconectar estaciones y repetidores con 1 km por segmento como máximo.
- **10-BASE-FL (enlace):** define un enlace punto a punto que se puede usar para conectar estaciones o repetidores a una distancia máxima de 2 km.
- **10-BASE-FB (troncal):** define un enlace punto a punto que puede usarse para conectar repetidores a 2 km como máximo.

Las tres especificaciones utilizan un par de fibras para cada enlace de transmisión, cada una de ellas se emplea para transmitir en un sentido. En todos los casos, el esquema de señalización hace uso de la codificación Manchester. Cada elemento de señal Manchester se transforma en un elemento de señal óptica, interpretándose la presencia de luz como estado en alto y la ausencia de ésta como estado en bajo. Así, una secuencia de bits Manchester a 10 Mbps necesita realmente 20 Mbps de la fibra.

10-BASE-FP define un sistema en estrella pasiva que puede admitir un máximo de 33 estaciones conectadas a una estrella pasiva central, que consiste en un dispositivo de fibra óptica que toma la señal de una de las líneas de entrada y la transmite por todas las líneas de salida sin retardo; esencialmente, una estrella pasiva es un divisor de señales. 10-BASE-FL y 10-BASE-FP definen conexiones punto a punto que pueden emplearse para ampliar la longitud de la red. La principal diferencia entre ellas es que 10-BASE- FP hace uso de transmisión síncrona. En la señalización síncrona, una señal óptica llega a un repetidor, se sincroniza con un reloj local y se retransmite. En la señalización asíncrona convencional, usada en 10-BASE-FL, no se realiza la sincronización anterior, de manera que cualquier variación en la temporización se propaga a través de varios repetidores. Debido al efecto no acumulativo de la transmisión síncrona, para conseguir longitudes mayores en 10- BASE-FB se pueden apilar hasta 15 en cascada.

ESPECIFICACIONES IEEE 802.3 a 100 MBPS (FAST ETHERNET)

Ethernet a alta velocidad (Fast Ethernet) es un conjunto de especificaciones desarrolladas por el comité IEEE 802.3 con el fin de proporcionar una red LAN de bajo coste compatible con Ethernet que funcione a 100 Mbps. La designación genérica para estos estándares es 10BASE-T. El comité definió varias alternativas para diferentes medios de transmisión.

La Figura 14.3 muestra la terminología utilizada en las distintas especificaciones e indica así mismo el medio usado. Todas las opciones 100BASE-T usan el protocolo MAC y el formato de la trama IEEE 802.3. 100BASE-X identifica al conjunto de opciones que usan las especificaciones del medio físico definidas originalmente para FDDI (Fiber Distributed Data Interface). Todos los esquemas 100BASE-X emplean dos enlaces físicos entre los nodos; uno para transmisión y otro para recepción. 100BASE-X hace uso de pares trenzados apantallados (STP) o cables de pares trenzados no apantallados (UTP) de alta calidad (clase 5). 100BASE-FX hace uso de fibra óptica.

En muchos edificios, cualquiera de las opciones 100BASE-X requiere la instalación de nuevo cableado. En estos casos, 100BASE-T4 define una alternativa menos costosa que puede utilizar UTP de voz de clase 3 además de UTP de clase 5 de alta calidad[4]. Para alcanzar los 100 Mbps en cables de baja calidad, 100BASE-T4 especifica el uso de 4 líneas de par trenzado entre los nodos, de los cuales tres se usan simultáneamente para la transmisión de datos en una dirección.

[4] Véase el Capítulo 4 para un estudio del cable de clase 3 y clase 5.

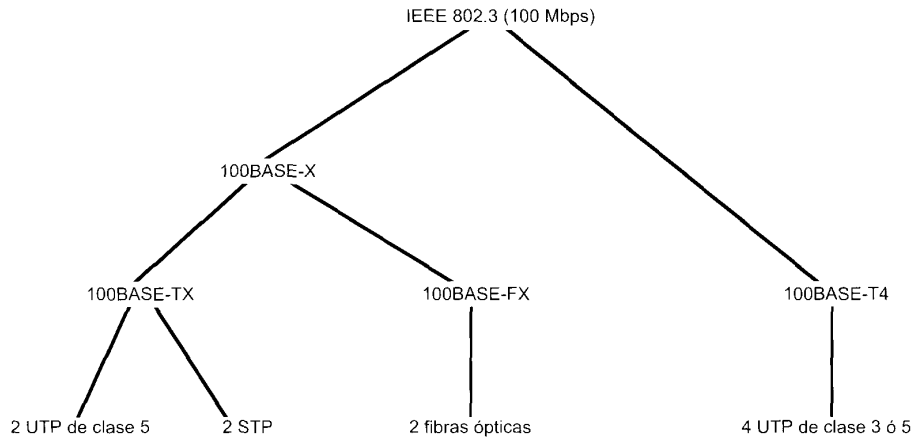


Figura 14.3. Opciones 10BASE-T en IEEE 802.3.

La topología de todas las opciones 100BASE-T es similar a la de 10BASE-T, que corresponde a una estrella.

La Tabla 14.2 resume las características más importantes de las opciones 100BASE-T.

100BASE-X

En todos los medios de transmisión especificados en 100BASE-X, los 100 Mbps se consiguen en un solo sentido utilizando un único enlace (par trenzado individual, fibra óptica individual). Para tal fin, en todos los medios, se necesita un esquema de codificación de señal que sea efectivo y eficiente. El esquema elegido se definió originalmente para FDDI, y se denomina 4B/5B-NRZI. Este esquema se modifica y particulariza en cada opción. Véase el Apéndice 14A para un estudio del mismo.

El esquema 100BASE-X incluye dos especificaciones para el medio físico, una para par trenzado, conocida como 100BASE-TX, y otra para fibra óptica, denominada 100BASE-FX.

Tabla 14.2. Alternativas para el medio de transmisión en la capa física IEEE 802.3 100BASE-T.

	100BASE-TX		**100BASE-FX**	**100BASE-T4**
Medio de transmisión	2 pares	2 pares, UTP clase 5	2 fibras ópticas	4 pares, clase 3, 4 o UTP 5
Técnica de señalización	MLT-3	MLT-3	4B5B, NRZI	8B6T, NRZ
Velocidad de transmisión	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Longitud máxima del segmento	100 m	100 m	100 m	100 m
Cobertura de la red	200 m	200 m	400 m	200 m

100BASE-TX utiliza dos pares de cable de par trenzado, uno para transmisión y otro para recepción. Se permiten tanto STP como UTP de clase 5, y se usa el esquema de señalización MLT-3 (descrito en el Apéndice 14A).

100BASE-FX utiliza dos fibras ópticas, una para transmitir y otra para recibir. En 100BASE-FX es necesario el uso de algún método para convertir la secuencia de grupos de código 4B/5B-NRZI en señales ópticas; esta conversión se denomina modulación en intensidad. Un uno binario se representa por un haz o pulso de luz, mientras que un cero binario se representa por la ausencia de pulso de luz o por uno de muy baja intensidad.

100BASE-T4

100BASE-T4 está pensado para ofrecer una velocidad de transmisión de datos de 100 Mbps a través de cable de clase 3 de baja calidad; la idea es poder reutilizar las instalaciones existentes de este tipo de cable en edificios de oficinas. La especificación también permite el uso opcional de cable de clase 5. 100BASE-T4 no transmite una señal continua entre paquetes, lo que lo hace útil para sistemas alimentados por baterías.

En 100BASE-T4, al utilizar cable de clase 3 para voz, no es de esperar que los 100 Mbps se obtengan utilizando un único par trenzado. Por el contrario, 100BASE-T4 especifica que la secuencia de datos a transmitir se divida en tres secuencias distintas, cada una de las cuales se transmitirá a una velocidad de transmisión efectiva de 33,3 Mbps. Se usan cuatro pares trenzados, de modo que los datos se transmite haciendo uso de tres pares y se reciben a través de otros tres. Por tanto, dos de los pares deben configurarse para una transmisión bidireccional.

Como en el caso de 100BASE-X, en 100BASE-T4 no se emplea un esquema de codificación NRZ. Esto requeriría una velocidad de transmisión de datos de 33 Mbps a través de cada par trenzado y no proporcionaría sincronización. En cambio, se usa un esquema de señalización ternario conocido como 8B6T (descrito en el Apéndice 14A).

GIGABIT ETHERNET

A finales del año 1995, el comité IEEE 802.3 formó el grupo de trabajo de alta velocidad con el fin de investigar estrategias para transmitir paquetes con formato Ethernet a velocidades del orden de Gigabits por segundo. Desde entonces se han especificado un conjunto de estándares a 1.000 Mbps.

La solución en Gigabit Ethernet es la misma que la adoptada en Fast Ethernet, en Gigabit se sigue adoptando tanto el protocolo CSMA/CD, como el formato de sus predecesores Ethernet a 10 Mbps y 100 Mbps. Es compatible con 100BASE-T y 10BASE-T, facilitando la migración. La demanda de tecnología Gigabit Ethernet ha crecido debido a que cada vez más, las organizaciones están adoptando 100BASE-T lo que implica cantidades enormes de tráfico en las líneas troncales.

En la Figura 14.4 se muestra una aplicación típica de Gigabit Ethernet. Un conmutador a 1 Gbps proporciona la conectividad entre los servidores centrales y entre concentradores de alta velocidad. Cada concentrador se conecta a la línea troncal mediante un enlace a 1 Gbps y conecta además a los servidores de cada concentrador, a la vez que ofrece enlaces a 100 Mbps para conectar a estaciones de trabajo, servidores y otros concentradores a 100 Mbps.

Capa de acceso al medio

La especificación a 1.000 Mbps utiliza el mismo formato para las tramas y protocolo que el CSMA/CD usado en las versiones de IEEE 802.3 a 10 Mbps y 100 Mbps. Se han introducido dos mejoras respecto al esquema CSMA/CD básico en lo que se refiere al funcionamiento de los concentradores (Figura 13.10b):

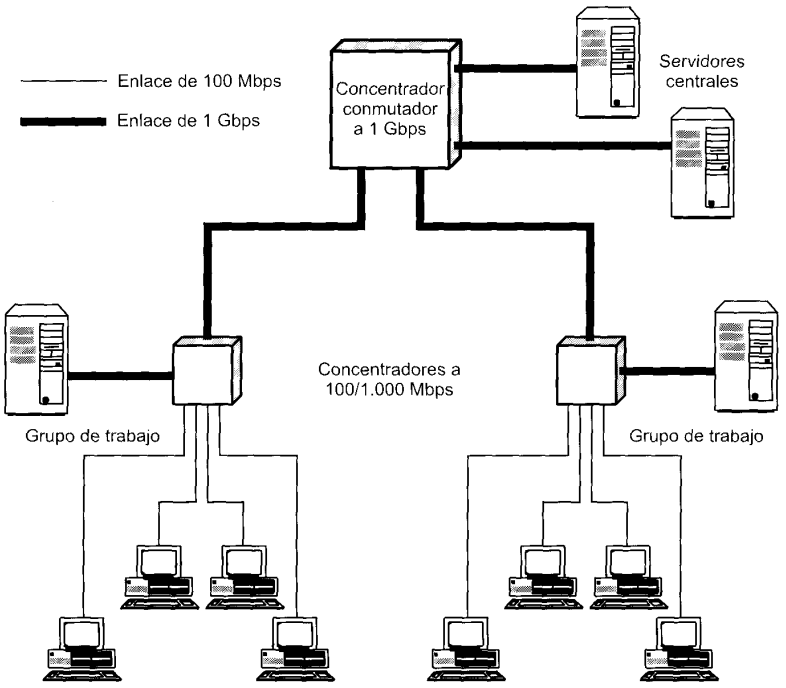


Figura 14.4. Ejemplo de configuración para Gigabit Ethernet.

- **Extensión de la portadora:** esta mejora consiste en añadir una serie de símbolos al final de la trama MAC de tal manera que el bloque resultante tenga una duración equivalente a 4.096 bits, mucho mayor que los 512 bits exigidos en el estándar a 10 y 100 Mbps. El objetivo es que la longitud de la trama, es decir el tiempo de transmisión sea mayor que el tiempo de propagación a 1 Gbps.
- **Ráfagas de tramas:** esta funcionalidad permite que se transmitan de forma consecutiva varias tramas cortas (sin superar un límite) sin necesidad de dejar el control del CSMA/CD. Las ráfagas de tramas evitan la redundancia y gasto que conlleva la técnica de la extensión de la portadora, en el caso de que una estación tenga preparadas para transmitir varias tramas pequeñas.

En el conmutador (Figura 13.10c), que facilita un acceso al medio dedicado, no son necesarias las técnicas de extensión de la portadora ni la de ráfagas de tramas. Esto se debe a que una estación puede transmitir y recibir simultáneamente sin interferencias y sin necesidad de luchar para acceder al medio compartido.

Capa física

La especificación actual del IEEE 802.3 a 1 Gbps define las siguientes alternativas:

- **1000BASE-SX:** esta opción en la que se usan longitudes de onda pequeñas, proporciona enlaces duplex de 275 m usando fibras multimodo de 62,5 μm o hasta 550 m con fibras multimodo de 50 μm. Las longitudes de onda están en el intervalo comprendido entre 770 y 860 nm.

- **1000BASE-LX:** esta alternativa en la que se utilizan longitudes de onda mayores, proporciona enlaces duplex de 550 m con fibras multimodo de 62,5 μm o 50 μm, o de 5 km con fibras monomodo de 10 μm. Las longitudes de onda están entre los 1.270 y los 1.355 nm.
- **1000BASE-CX:** esta opción proporciona enlaces de 1 Gbps entre dispositivos localizados dentro de una habitación (o armario de conexiones) utilizando latiguillos de cobre (cables de pares trenzados de menos de 25 m con un apantallamiento especial). Cada enlace consiste en un dos pares trenzados apantallados, cada uno de los cuales se usa en un sentido.
- **1000BASE-T:** esta opción utiliza cuatro pares no apantallados tipo 5 para conectar dispositivos separados hasta 1.000 m.

La técnica de codificación de la señal que se usa en Gigabit Ethernet es 8B/10B, descrita en el Apéndice 14A.

14.2. ANILLO CON PASO DE TESTIGO Y FDDI

El protocolo MAC más usual en redes LAN con topología en anillo es el de paso de testigo. En esta sección examinaremos dos normalizaciones que utilizan anillo con paso de testigo: IEEE 802.5 y FDDI.

CONTROL DE ACCESO AL MEDIO EN IEEE 802.5

Protocolo MAC

La técnica de anillo con paso de testigo se basa en el uso de una trama pequeña, denominada testigo («token»), que circula cuando todas las estaciones están libres. Cuando una estación desea transmitir debe esperar a que le llegue el testigo. En este caso, toma el testigo cambiando uno de sus bits, lo que lo convierte en la secuencia de comienzo en las tramas de datos. Posteriormente, la estación añade y transmite el resto de campos requeridos en la construcción de la trama.

Cuando una estación toma el testigo y comienza a transmitir, en el anillo deja de estar presente el testigo, de manera que el resto de estaciones que deseen transmitir deben esperar. La trama en el anillo realiza una vuelta completa y se absorbe o drena en la estación transmisora, que insertará un nuevo testigo en el anillo cuando se cumplan una de las dos condiciones siguientes:

- La estación haya terminado la transmisión de su trama.
- Los bits iniciales de la trama transmitida hayan vuelto a la estación (después de una vuelta completa al anillo).

Si la longitud del anillo es menor que la longitud de la trama, la primera condición implica la segunda. En caso contrario, una estación debería liberar el testigo después de que haya terminado de transmitir, pero antes de que comience a recibir su propia transmisión; la segunda condición no es estrictamente necesaria, relajándose en ciertas circunstancias. La ventaja que implica la suposición de la segunda condición es que asegura que, en un instante de tiempo dado, sólo puede haber una trama de datos en el medio y sólo pueda estar transmitiendo una estación, simplificándose los procedimientos de recuperación de errores.

Una vez que se ha insertado un nuevo testigo en el anillo, la siguiente estación en la secuencia que disponga de datos a transmitir podrá tomar el testigo y llevar a cabo la transmisión. La Figura 14.5 ilustra la técnica. En el ejemplo, A envía un paquete a C, quien lo recibe y envía sus propios paquetes a A y D.

Obsérvese que en condiciones de baja carga, el anillo con pase de testigo presenta cierta ineficacia debido a que una estación debe esperar a recibir el testigo antes de transmitir. Sin embargo, en condiciones de alta carga, que es la situación más preocupante, el anillo funciona como un sistema de turno rotatorio («round-robin»), que es eficiente además de equitativo. Para ver esto consideremos la configu-

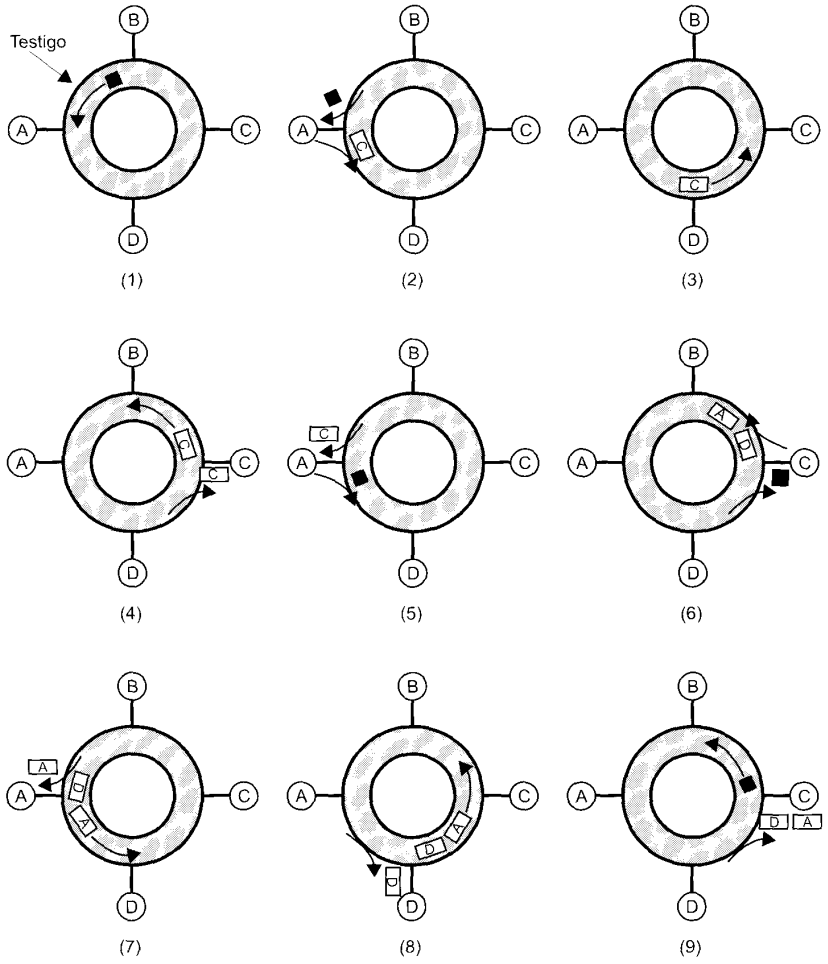


Figura 14.5. Funcionamiento del anillo con paso de testigo.

ración de la Figura 14.5. Después de que la estación A transmita, libera un testigo. La primera estación con opción de transmitir es D. Si lo hace, libera después un testigo y C es la siguiente que puede transmitir; y así sucesivamente.

La principal ventaja del anillo con paso de testigo es el control de acceso flexible que ofrece. En el esquema sencillo que se acaba de describir el acceso es equitativo. Como se verá más adelante, se pueden utilizar distintos esquemas para regular el acceso con el fin de proporcionar prioridad y servicios de concesión y reserva de ancho de banda.

La principal desventaja del anillo con paso de testigo está en la necesidad de procedimientos para realizar el mantenimiento del anillo. La pérdida del testigo impide posteriores utilizaciones del anillo. La duplicidad del testigo puede interrumpir también el funcionamiento del anillo. Se puede seleccionar una estación monitora para asegurar que sólo hay un testigo en el anillo y para reinsertar un testigo libre en caso necesario.

Trama MAC

En la Figura 14.6 se muestra el formato de la trama del protocolo 802.5. Consta de los siguientes campos:

- **Delimitador de comienzo (SD, Starting Delimiter):** indica el comienzo de la trama, SD consta de patrones de delimitación distintos a los datos. Se codifican como sigue: JK0JK000, donde J y K son símbolos de no datos (violación de código). La forma de un símbolo de no datos depende de la codificación de la señal en el medio.
- **Control de acceso (AC, Access Control):** tiene el formato PPPTMRRR, donde PPP y RRR son las variables de prioridad y reserva de 3 bits, y M es el bit monitor; su uso se explica más adelante. T indica si es una trama de testigo o de datos. En el caso de una trama de testigo, el único campo posterior es ED.
- **Control de trama (FC, Frame Control):** indica si la trama es de datos LLC. Si no, los bits de este campo controlan el funcionamiento del protocolo MAC en el anillo con paso de testigo.
- **Dirección destino (DA, Destination Address):** como en 802.3
- **Dirección origen (SA, Source Address):** como en 802.3.
- **Unidad de datos:** contiene datos LLC.
- **Secuencia de comprobación de trama (FCS, Frame Check Sequence):** como en 802.3.
- **Delimitador de fin (ED, End Delimiter):** contiene el bit de detección de error (E), que se activa si cualquier repetidor detecta un error, y el bit intermedio (I), usado para identificar que esta trama no es la final de una transmisión de múltiples tramas.

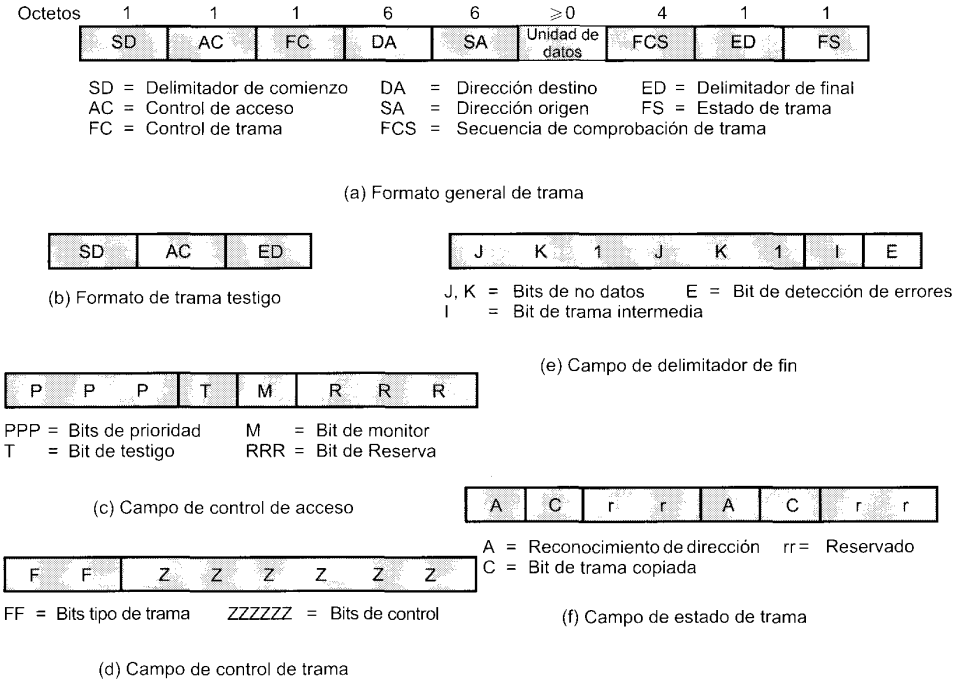


Figura 14.6. Formato de la trama IEEE 802.5.

- **Estado de trama (FS, Frame Status):** contiene los bits de dirección reconocida (A) y de trama copiada (C), cuyo uso se explica más adelante. Dado que los bits A y C no están cubiertos por el campo FCS, se encuentran duplicados con el fin de ofrecer una comprobación de redundancia para detectar valores erróneos.

Ahora podemos enunciar de nuevo el algoritmo de anillo con paso de testigo para el caso de que se use una única prioridad. En este caso, los bits de prioridad y de reserva están desactivados. Una estación que desee transmitir espera hasta que le llegue el testigo, indicado por la desactivación del bit de testigo en el campo AC. La estación toma el testigo activando el bit de testigo. Los campos SD y AC del testigo recibido funcionan ahora como dos campos de la trama transmitida. La estación transmite una o más tramas hasta que termine la transmisión o hasta que expire el contador de posesión de testigo. Cuando el campo AC de la última trama transmitida vuelva, la estación desactiva el bit de testigo y añade un campo ED, lo que da lugar a la inserción de un nuevo testigo en el anillo.

Las estaciones en modo de recepción escuchan el anillo. Cada estación puede comprobar las tramas que pasan y activar el bit E en caso de que se detecte un error. Si una estación detecta su propia dirección MAC, activa el bit A; también puede copiar la trama mediante la activación del bit C. Esto permite a la estación que la originó distinguir entre resultados de transmisión de una trama:

- Estación de destino no existente o no activa (A = 0, C = 0).
- Estación de destino existe pero la trama no se copió (A = 1, C = 0).
- Trama recibida (A = 1, C = 1).

Prioridad en redes en anillo con paso de testigo

La normalización 802.5 incluye una especificación para un mecanismo opcional de prioridad. Se admiten ocho niveles de prioridad mediante el uso de dos campos de 3 bits en cada trama de datos y de testigo: un campo de prioridad y un campo de reserva. Para explicar el algoritmo, definamos las siguientes variables:

P_f = prioridad de trama para la transmisión de una estación.

P_s = prioridad de servicio: prioridad del testigo actual.

P_r = valor de P_s contenido en el último testigo recibido de una estación.

R_s = valor de reserva en el testigo actual.

R_r = mayor valor de reserva en las tramas recibidas en esta estación durante la rotación del último testigo.

El esquema funciona como sigue:

1. Una estación que desee transmitir debe esperar un testigo con $P_s \leqslant P_f$.
2. Mientras espera, una estación puede reservar un futuro testigo con su nivel de prioridad (P_f). Si detecta una trama de datos y el campo de reserva es menor que su prioridad ($R_s < P_f$), la estación puede poner su prioridad en el campo de reserva de la trama ($R_s \leftarrow P_f$). Si detecta una trama de testigo y ($R_s < P_f$ y $P_f < P_s$), la estación pone su prioridad en el campo de reserva de la trama ($R_s \leftarrow P_f$). Esto provoca el borrado de cualquier reserva con menor prioridad.
3. Cuando una estación coge un testigo, activa el bit de testigo para transmitir una trama de datos, pone el campo de reserva de la trama a 0 y no altera el campo de prioridad (el mismo que el de la trama entrante).
4. Tras la transmisión de una o más tramas de datos, la estación enviará un testigo nuevo con los campos apropiados de reserva y prioridad.

El efecto de los pasos anteriores es la ordenación de las demandas que compiten, y permitir a las transmisiones en espera con prioridad superior captar el testigo tan pronto como sea posible. Si reflexionamos podemos percatarnos de que, como se estableció, el algoritmo presenta un efecto de trinquete sobre la prioridad, llevándolo al nivel de prioridad superior utilizado y manteniéndolo a este valor. Para evitar este hecho, una estación que aumente la prioridad (emite un testigo con prioridad mayor que el que recibió) tiene responsabilidad de bajarla después al nivel anterior. Por tanto, una estación que sube la prioridad debe recordar tanto la vieja como la nueva prioridad y bajar la del testigo en el momento apropiado. Esencialmente, cada estación es responsable de asegurar que el testigo no circule indefinidamente debido a que la prioridad sea demasiado elevada. Recordando la prioridad de transmisiones anteriores, una estación puede detectar esta condición y bajar la prioridad a un valor de reserva anterior menor.

En cada estación se usan dos pilas para implementar el mecanismo de decremento de prioridad, una para reservas y otras para prioridades:

S_x = pila para almacenar nuevos valores de prioridad de testigo

S_r = pila donde se almacenan valores anteriores de prioridad de testigo

La razón de la necesidad de usar pilas en lugar de variables escalares es que la prioridad pude aumentarse varias veces por una o más estaciones. Los sucesivos aumentos deben deshacerse en orden inverso.

En resumen: una estación que tiene que transmitir una trama con prioridad superior a la de la trama actual puede reservar el siguiente testigo con su nivel de prioridad mientras pasa la trama. Cuando se emite el siguiente testigo, éste debe tener el nivel de prioridad reservado. Las estaciones con prioridad inferior no pueden coger el testigo, de manera que éste pasa a la estación que lo reservó o a una estación intermedia con datos a transmitir de prioridad igual o superior que el nivel de prioridad reservado. La estación que actualiza el nivel de prioridad es responsable de volverlo a decrementar a su antiguo valor cuando han terminado todas las estaciones de prioridad superior. Cuando esta estación observa un testigo de prioridad superior después de haber transmitido, puede suponer que no hay en espera más tráfico de prioridad superior y decrementa el testigo antes de que pase.

La Figura 14.7 es un ejemplo. Tiene lugar los siguientes sucesos:

1. A transmite una trama de datos a B con prioridad 0. Cuando la trama completa una vuelta en el anillo y vuelve a A, ésta emite una trama de testigo. Sin embargo, mientras la trama de datos atraviesa D, D hace una reserva con prioridad 3 poniendo el campo de reserva a este valor.
2. A emite un testigo con prioridad igual a 3.
3. Si ni B ni C tienen datos que transmitir con prioridad 3 o superior, no pueden coger el testigo. Éste circula hasta D, que lo coge y emite una trama de datos.
4. Después de que la trama de datos de D vuelve a ella, D emite un nuevo testigo con la misma prioridad que el testigo que recibió: prioridad 3.
5. A detecta un testigo con el mismo nivel de prioridad que usó en su última emisión de testigo, de manera que lo coge, aunque no tenga datos que transmitir.
6. A envía un testigo con el nivel de prioridad anterior: prioridad 0.

Observemos que después de que A haya emitido un testigo de prioridad 3, cualquier estación con datos pendientes de transmisión de prioridad 3 o superior puede coger el testigo. Supongamos que este punto C tiene ahora datos que transmitir con prioridad 4. C toma el testigo, transmite su trama de datos y reenvía un testigo con prioridad 3, que es cogido por D. En el momento en que un testigo con prioridad 3 llegue a A, todas las estaciones que intervienen con datos a enviar de prioridad 3 o supe-

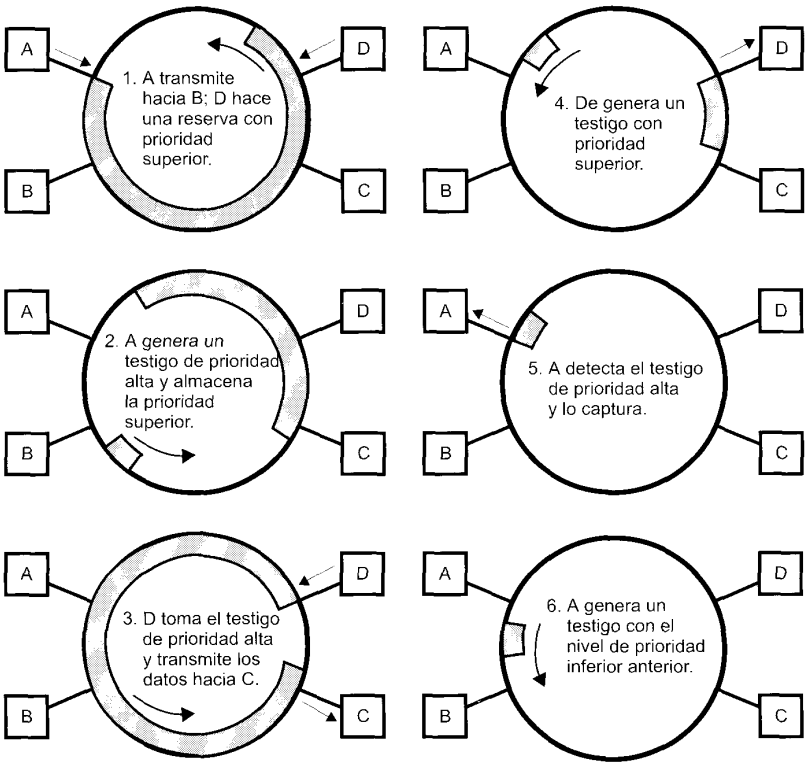


Figura 14.7. Esquema de prioridades en redes en anillo con paso de testigo.

rior habrán tenido la oportunidad, por lo que es el momento apropiado para que A decremente la prioridad del testigo.

Liberación rápida de testigo

Si la longitud del anillo expresada en bits es menor que la trama, cuando una estación emite una trama la cabecera de ésta retornará a la estación emisora antes de que se haya completado la transmisión. En este caso, la estación puede emitir un testigo en cuanto haya finalizado la transmisión de la trama. Si la trama es más corta que la longitud del anillo, antes de que una estación haya terminado la transmisión de una trama debe esperar hasta que la cabeza de la misma vuelva antes de emitir un testigo. En este último caso no se usa parte de la capacidad teórica del anillo.

Se ha incluido una opción de liberación rápida del testigo (ETR) en la norma 802.5 con el fin de permitir una utilización más eficaz del medio. ETR permite a la estación transmisora liberar un testigo en cuanto haya terminado la transmisión de la trama, independientemente de que la cabecera de la rama haya retornado o no a la estación. La prioridad usada en la liberación del testigo previa a la recepción de la cabecera de la trama anterior es la prioridad de la trama más reciente recibida.

Un efecto de la técnica ETR es que puede aumentar el retardo de acceso para tráfico prioritario cuando el anillo se encuentre ocupado por tramas cortas. Dado que una estación debe emitir un testigo antes de que pueda leer los bits de reserva de la trama en circulación, la estación no responderá a reservas. Por tanto, el mecanismo de prioridad queda incapacitado al menos parcialmente.

Las estaciones que implementan ETR son compatibles y se pueden interconectar con aquellas que no dispongan de él.

Anillo con paso de testigo dedicado

La actualización del IEEE 802.5 de 1997 introdujo una nueva técnica de control del acceso al medio denominada anillo con paso de testigo dedicado (DTR, Dedicated Token Ring). Recuérdese de la Sección 13.4 que el anillo puede adoptar una topología en estrella mediante el uso de un concentrador («hub»). El algoritmo de paso de testigo se puede utilizar en esa topología de manera que la capacidad del anillo siga siendo compartida, ya que el acceso al medio está determinado por el testigo. Si embargo, es igualmente posible que el concentrador central funcione como un conmutador (Figura 13.10c), de tal manera que la conexión entre cada estación y el conmutador funciona como un enlace punto a punto en full-duplex. La especificación DTR define como utilizar las estaciones y concentradores en este modo conmutado. El concentrador DTR funciona como un retransmisor de tramas en lugar de ser un repetidor de bits, tal que cada enlace desde el concentrador a las estaciones es un enlace dedicado con acceso inmediato; no se usa paso de testigo.

ESPECIFICACIÓN DE LA CAPA FÍSICA DE IEEE 802.5

El estándar 802.5 ofrece un amplio abanico de velocidades y medios de transmisión, como así se muestra en la Tabla 14.3. El estándar fija un máximo para el tamaño de las tramas igual a 4.550 octetos a 4 Mbps y 18.200 octetos para 16 Mbps y 100 Mbps. Estos valores son distintos a los 1.518 octetos de IEEE 802.3. A 4 Mbps y a 16 Mbps se puede usar para el control del acceso al medio tanto el paso de testigo como la técnica de DTR conmutada. A 100 Mbps, la utilización de la técnica DTR es obligatoria. El comité 802.5 está trabajando en la actualidad en la versión a 1 Gbps.

A 4 Mbps y 16 Mbps, la señalización es Manchester diferencial. En el caso de fibras ópticas, la señal codificada con Manchester diferencial se transmite utilizando una señalización on-off. Es decir, uno de los niveles de señal se representa mediante la presencia de luz y el otro mediante ausencia de luz. A 100 Mbps, el 802.5 adopta la especificación de la capa física, incluyendo la señalización, de Ethernet a 100 Mbps.

CONTROL DE ACCESO AL MEDIO FDDI

FDDI es un esquema en anillo con paso de testigo análogo a la especificación IEEE 802.5 diseñada para aplicaciones LAN y MAN. Existen varias diferencias ideadas para admitir la alta velocidad de transferencia de datos de FDDI (100 Mbps).

Tabla 14.3. Alternativas para el medio de transmisión en la capa física IEEE 802.5.

Velocidad de transmisión	4	16	100
Medio de transmisión	UTP, STP o fibra	UTP, STP o fibra	UTP, STP o fibra
Técnica de señalización	Manchester diferencial	Manchester diferencial	MLT-3 o 4B5B/NRZI
Tamaño máximo de la trama (octetos)	4.550	18.200	18.200
Control de acceso	TP o DTR	TP o DTR	DTR

UTP = (par trenzado no apantallado, «unshielded twisted pair»)
STP = (par trenzado apantallado, «shielded twisted pair»)
TP = (control de acceso con paso de testigo, «token passing access control»)
DTR = (anillo con paso de testigo dedicado, «dedicated token ring»)

Trama MAC

La Figura 14.8 muestra el formato de la trama para el protocolo FDDI. La normalización define el contenido de este formato en términos de símbolos, donde cada símbolo corresponde con 4 bits de datos. Se usan símbolos debido a que, en la capa física, los datos se codifican en grupos de cuatro bits. Sin embargo, las entidades MAC deben tratar bits individuales, de modo que la discusión que sigue se refiere a veces a símbolos de cuatro bits y otras veces a bits individuales. Una trama distinta a un testigo consta de los siguientes campos:

- **Preámbulo:** sincroniza la trama con el reloj de cada estación. La estación que originó la trama usa un campo de 16 símbolos libres (64 bits); estaciones sucesivas pueden cambiar la longitud del campo de acuerdo con los requisitos de temporización. El símbolo libre es un patrón completo de no datos (violaciones de código). La forma real de un símbolo de no datos depende de la codificación de la señal en el medio.
- **Delimitador de comienzo (SD, Starting Delimiter):** indica el comienzo de la trama. Se codifica como JK, donde tanto J como K son símbolos de no datos.
- **Control de trama (FC, Frame Control):** tiene el formato de bits CLFFZZZZ, donde C indica si la trama es síncrona o asíncrona (explicado más adelante); L indica el uso de direcciones de 16 o 48 bits; FF indica si es una trama LLC, de control MAC o reservada. Para una trama de control, los restantes cuatro bits indican el tipo de trama de control.
- **Dirección de destino (DA, Destination Address):** especifica la estación o estaciones a las que va dirigida la trama. Puede ser una única dirección física, una dirección de grupo multidestino o una dirección de difusión. El anillo puede contener una mezcla de longitudes de dirección de 48 bits.
- **Dirección origen (SA, Source Address):** especifica la estación que envió la trama.
- **Información:** contiene datos LLC o información relacionada con una función de control.
- **Secuencia de comprobación de la trama (FCS, Frame Check Sequence):** comprobación de redundancia cíclica de 32 bits referente a los campos FC, DA, SA y de información.
- **Delimitador de fin (ED, Ending Delimiter):** contiene un símbolo de no datos (violación de código) y marca el final de la trama sin contar el campo FS.
- **Estado de trama (FS, Frame Status):** contiene los indicadores de detección de error (E), dirección reconocida (A) y trama copiada. Cada indicador se representa mediante un símbolo, que es R para «reinicio» o «falso», y S para «activo» o «verdadero».

Una trama de testigo consta de los siguientes campos:

- **Preámbulo:** como antes.
- **Delimitador de comienzo:** como antes.

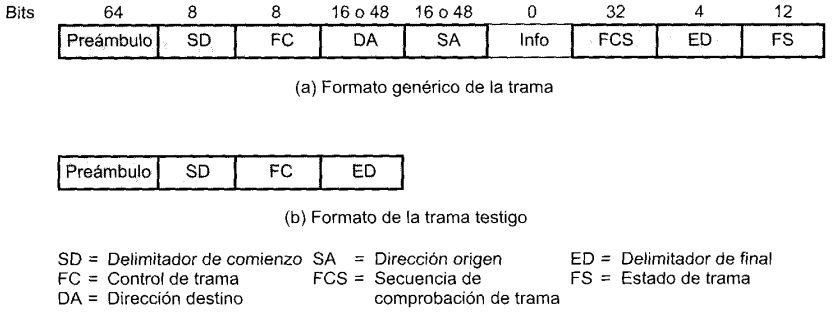


Figura 14.8. Formatos de la trama FDDI.

- **Control de trama (FC, Frame Control):** presenta el formato de bits 10000000 o 11000000 para indicar que se trata de un testigo.
- **Delimitador de fin (ED, Ending Delimiter):** contiene un par de símbolos de no datos (T) como fin de la trama de testigo.

Una comparación con la trama 802.5 (Figura 14.6) muestra que ambas son muy similares. La trama FDDI incluye un preámbulo para ayudar a la sincronización, más necesaria a velocidades de transmisión de datos superiores. En la misma FDDI se permiten tanto las direcciones de 16 bits como las de 48 bits, lo que da más flexibilidad que el esquema usado en todas las normalizaciones 802. Por último, existen algunas diferencias en los bits de control. Por ejemplo, FDDI no incluye bits de prioridad ni de reserva, y la reserva de capacidad, como se describe más adelante, se gestiona de forma diferente.

Protocolo MAC FDDI

El protocolo MAC FDDI básico (sin reserva ni capacidad) es fundamentalmente el mismo que IEEE 802.5, aunque presenta dos diferencias principales:

- En FDDI, una estación que espera el testigo lo toma cancelando (no repitiendo) la transmisión del mismo en cuanto reconoce que se trata de una trama de testigo. Tras la recepción completa del testigo capturado, la estación comienza a transmitir una o más tramas. La técnica 802.5 de modificación de bits para convertir un testigo en el comienzo de una trama de datos se considera impracticable dada la alta velocidad de transmisión de datos FDDI.
- En FDDI, una estación que ha transmitido tramas de datos libera un nuevo testigo en cuanto termina la transmisión, incluso si no ha comenzado a recibir su propia transmisión. Esta técnica es la misma que la de la opción de liberación de testigo de 802.5 comentada anteriormente. De nuevo, dada la alta velocidad de transmisión de datos, resulta demasiado ineficaz hacer que la estación espere al retorno de su trama como indica el funcionamiento normal en 802.5.

La Figura 14.9 muestra un ejemplo del funcionamiento del anillo. Después de que la estación A haya cogido el testigo, transmite la trama F1, y transmite inmediatamente un nuevo testigo. La trama F1 va dirigida a la estación C, que la copia mientras circula. La trama vuelve eventualmente a A, quien la absorbe. Mientras tanto B, coge el testigo enviado por A y transmite F2 seguida por un testigo. Esta acción se podría repetir cualquier número de veces, de modo que en cualquier instante de tiempo pueden circular varias tramas a través del anillo. Cada estación es responsable de absorber sus propias tramas, esta operación se hace considerando el campo de la dirección del origen.

Acerca del campo de estado de trama (FS) se puede hacer una consideración más. Cada estación puede comprobar la ocurrencia de errores en los bits que pasan por ella, de modo que pueden activar el indicador E si se detecta un error. Si una estación detecta su propia dirección, activa el indicador A y también puede copiar la trama, activando el indicador C. Esto permite a la estación origen, cuando absorbe una trama que transitó previamente, diferenciar tres condiciones:

- Estación inexistente/inactiva.
- Estación existente pero trama no copiada.
- Trama copiada.

Cuando se absorbe una trama, se pueden examinar los indicadores de estado (E, A y C) del campo FS para determinar el resultado de la transmisión. Sin embargo, si se descubre la ocurrencia de un error o un fallo en la recepción, la entidad de protocolo MAC no intenta retransmitir la trama, pero informa a LLC. Es responsabilidad de éste o de algún protocolo de una capa superior tomar una acción correctiva.

Reserva de capacidad

El esquema de prioridades usado en 802.5 no funciona en FDDI, ya que una estación envía a veces un testigo antes de que vuelva la trama que ha transmitido. Por tanto, el uso de un campo de reserva no es

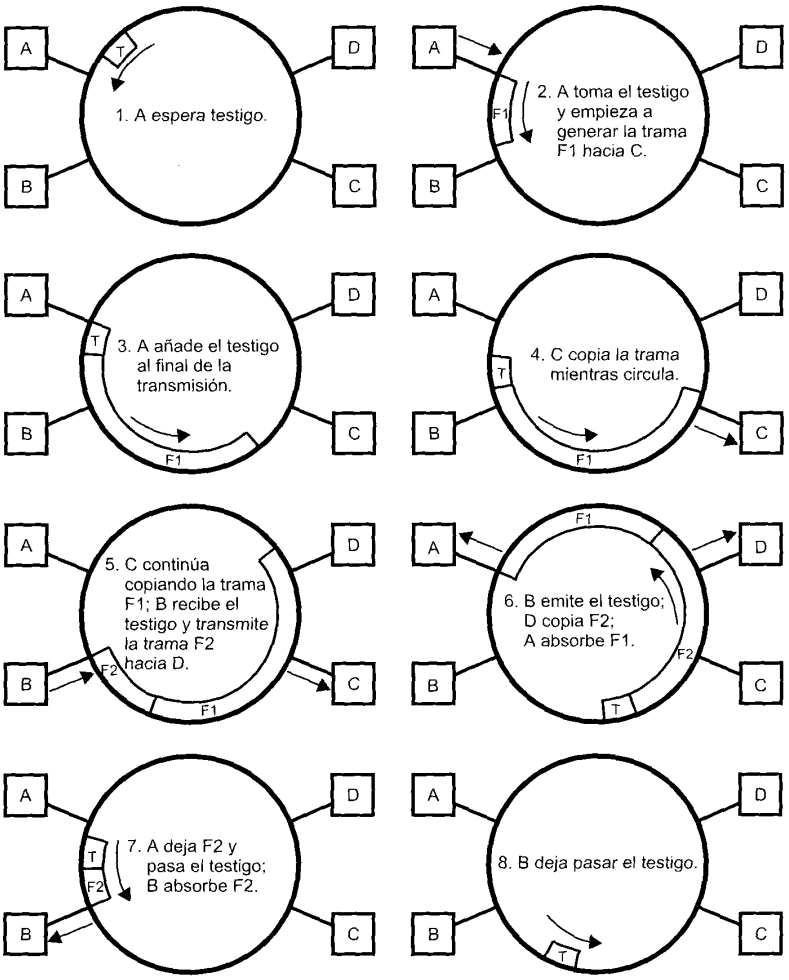


Figura 14.9. Ejemplo de funcionamiento de una red en anillo con paso de testigo.

efectivo. Además, el estándar FDDI, con el fin de satisfacer los requisitos de una LAN de alta velocidad, está pensado para proporcionar un mayor control sobre la capacidad de la red que el estándar 802.5. Específicamente, el esquema de reserva de capacidad en FDDI persigue la admisión de una mezcla de tráfico continuo y a ráfagas.

Para satisfacer este requisito, FDDI define dos tipos de tráfico: síncrono y asíncrono. Cada estación reserva una parte de la capacidad total (ésta puede ser cero); las tramas que transmite durante este tiempo se denominan tramas síncronas. Cualquier capacidad no reservada. O reservada pero no usada, se encuentra disponible para la transmisión de tramas asicionales, denominadas tramas asíncronas.

El esquema funciona como sigue. Se define un **tiempo de rotación del testigo objeto (TTRT, target token rotation time),** almacenando cada estación el mismo valor de TTRT. A algunas o a todas las

estaciones se les puede proporcionar una **reserva síncrona (SA_i, synchronous allocation)**, que puede diferir entre las distintas estaciones. Las reservas pueden ser tales que:

$$\text{DMax} + \text{FMax} + \text{TokenTime} + \sum SA_i \leq \text{TTRT}$$

donde

SA_i = reserva síncrona para la estación i
DMax = tiempo de propagación de una vuelta completa en el anillo
FMax = tiempo necesario para transmitir una trama de longitud máxima (4.500 octetos)
Tiempo de testigo = tiempo necesario para transmitir un testigo.

La asignación de valores para SA_i se establece mediante un protocolo de gestión. El protocolo asegura que se satisface la ecuación anterior. Inicialmente, cada estación tiene una reserva nula y debe solicitar un cambio en ésta. La aceptación de reserva síncrona es opcional; una estación que no admite reserva síncrona sólo puede transmitir tráfico asíncrono.

Todas las estaciones tienen el mismo valor del TTRT y un valor SA_i asignado independientemente de cada estación. Además, en cada estación se mantienen varias variables necesarias para el funcionamiento del algoritmo de reserva de capacidad:

- Contador de rotación de testigo (TRT).
- Contador de posesión del testigo (THT).
- Contador de retraso (LC).

Cada estación se inicia con un valor de TRT igual a TTRT y LC puesto a cero[5]. Cuando el contador está habilitado, TRT comienza a contar hacia abajo. Si se recibe un testigo antes de que TRT expire, TRT es reiniciado a TTRT. Si TRT llega a cero antes de que se reciba un testigo, LC se incrementa a 1 y TRT se inicia a TTRT, comenzándose de nuevo a contar hacia abajo. Si TRT expira por segunda vez antes de que se reciba un testigo, LC se incrementa a 2, el testigo se considera perdido y se inicia el proceso de reclamación (descrito más adelante). Así, LC graba el número de veces, si se ha producido alguna, que ha expirado el TRT desde que el testigo fue recibido por última vez en esta estación. Se considera que el testigo ha llegado antes si el TRT no ha expirado desde que la estación recibió el testigo; es decir, si LC = 0.

Cuando una estación recibe el testigo, su reacción dependerá de si éste ha llegado pronto o con retraso. Si el testigo ha llegado pronto, la estación salva el tiempo restante de TRT en THT, reinicia TRT y lo habilita:

$$\text{THT} \leftarrow \text{TRT}$$
$$\text{TRT} \leftarrow \text{TTRT}$$
habilitación TRT

Después de esto, la estación puede transmitir de acuerdo con las siguientes reglas:

1. Puede transmitir tramas síncronas durante un tiempo SA_i.
2. Después de transmitir tramas síncronas, o si no había tramas síncronas que transmitir, se habilita THT. La estación puede comenzar la transmisión de tramas síncronas mientras THT > 0.

Si una estación recibe el testigo y éste llega con retraso, LC se pone a 0 y TRT continúa decrementándose. La estación puede entonces transmitir tramas síncronas durante un tiempo SA_i, no pudiendo transmitir ninguna trama síncrona.

[5] *Nota:* todos los valores de los contadores en el estándar son números negativos, incrementándose el contador hacia cero. Por claridad, en la discusión se hace uso de números positivos.

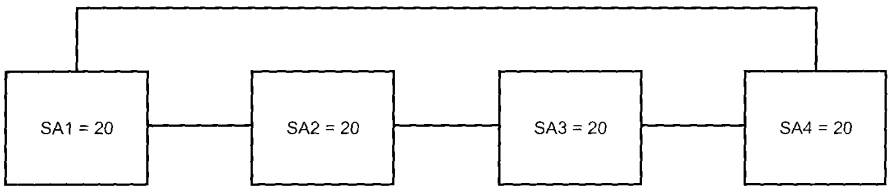
Este esquema está diseñado para asegurar que el tiempo de observaciones de un testigo es del orden de TTRT o menor. De este tiempo, una cantidad específica está siempre disponible para tráfico síncrono, y cualquier exceso de capacidad se encuentra disponible para tráfico asíncrono. Debido a la fluctuación aleatoria del tráfico, el tiempo real de circulación del testigo puede exceder TTRT, como se demuestra más adelante.

La Figura 14.10 ofrece un ejemplo simplificado de un anillo con 4 estaciones. Se hacen las siguientes suposiciones:

- El tráfico consiste en tramas de longitud fija.
- TTRT = 100 veces el tiempo de duración de una trama.
- SA_i = 20 veces el tiempo de duración de una trama para cada estación.
- Cada estación está siempre preparada par enviar su reserva síncrona completa así como tantas tramas asíncronas como sea posible.
- El coste suplementario total durante una vuelta completa del testigo es de 4 veces el tiempo de duración de una trama (una vez el tiempo de duración de una trama por estación).

Una fila de la tabla corresponde a una vuelta del testigo en el anillo. Para cada estación, se muestra el instante de llegada del testigo, seguido por el valor de TRT en el momento de la llegada, seguido por el número de tramas síncronas y asíncronas transmitidas mientras la estación posee el testigo.

El ejemplo comienza después de un periodo durante el que no se han enviado tramas de datos, de manera que el testigo ha estado circulando tan rápido como ha sido posible (4 veces el tiempo de duración de la trama). Así cuando la estación 1 recibe el testigo en el instante de tiempo 4, determina un tiempo de circulación de 4 (su TRT = 96). Es posible por tanto enviar no sólo sus 20 tramas síncronas sino también 96 tramas asíncronas; recordemos que THT no está habilitado hasta después de que una estación haya enviado sus tramas síncronas. La estación 2 experimenta un tiempo de circulación de 120



Tiempo de llegada	TRT	Síncr.	Asíncr.	Tiempo de llegada	TRT	Síncr.	Asíncr.	Tiempo de llegada	TRT	Síncr.	Asíncr.	Tiempo de llegada	TRT	Síncr.	Asíncr.
0	100	0	0	1	100	0	0	2	100	0	0	3	100	0	0
4	96	20	**96**	121	80*	20	0	142	60*	20	0	163	40*	20	0
184	20*	20	0	205	96*	20	0	226	76*	20	0	247	56*	20	0
258	36*	20	0	289	12	20	**12**	322	80*	20	0	343	60*	20	0
364	40*	20	0	385	4	20	**4**	410	92*	20	0	431	72*	20	0
452	52*	20	0	473	12	20	**16**	506	96*	20	0	527	76*	20	0
548	56*	20	0	569	4	20	**4**	594	8	20	**8**	623	80*	20	0
644	60*	20	0	665	4	20	**4**	690	4	20	**4**	715	88*	20	0
736	68*	20	0	757	8	20	**8**	786	4	20	**4**	811	82*	20	0
832	72*	20	0	853	4	20	**4**	878	8	20	**8**	907	96*	20	0
928	76*	20	0	949	4	20	**4**	974	4	20	**4**	999	4	20	**4**
1.024	80*	20	0	1.045	4	20	**4**	1.070	4	20	**4**	1.095	4	20	**4**

*LC = 1; en cualquier otro caso LC = 0

Figura 14.10. Funcionamiento del esquema de reserva de capacidad en FDDI.

Tabla 14.4. Alternativas para el medio de transmisión en la capa física en FDDI.

Medio de transmisión	Fibra óptica	Par trenzado
Velocidad de transmisión (Mbps)	100	100
Codificación	4B/5B/NRZI	MLT-3
Número máximo de repetidores	100	100
Longitud máxima entre repetidores	2 km	100 m

(20 tramas + 96 tramas + 4 tramas suplementarias), pero, si embargo, no está autorizada a transmitir sus 20 tramas síncronas. Observemos que si cada estación continúa transmitiendo su número máximo de tramas síncronas permitidas, el tiempo de circulación crece hasta 180 (en el instante de tiempo 184), pero pronto se estabiliza en 100 aproximadamente. Con una utilización síncronas total de 80 y un coste suplementario de 4 veces el tiempo de duración de una trama, existe una capacidad promedio disponible para transmisiones asíncronas de 16 veces el tiempo de duración de una trama.

El lector se preguntará por qué hay tanto una especificación para FDDI y una especificación 802.5 a 100 Mbps, denominada anillo con paso de testigo a alta velocidad (HSTR, high-speed token ring). FDDI se desarrolló antes que el HSTR y su objetivo es proporcionar conectividad en entornos LAN y MAN mediante paso de testigo. El objetivo de HSTR es proporcionar redes LAN de alta velocidad que sean compatibles y se puedan interconectar con componentes 802.5 de baja velocidad. El formato de las tramas en HSTR es el mismo que el de 802.5 de baja velocidad, de igual forma, el algoritmo para puentes con encaminamiento desde el origen es también común. Debido a que el HSTR opera exclusivamente en modo de acceso conmutado (DTR), no tiene que abordar los problemas que si están presentes en FDDI, relacionados con el paso de testigo y la asignación de la capacidad del anillo.

ESPECIFICACIÓN DE LA CAPA FÍSICA EN FDDI

El estándar FDDI especifica una topología en anillo operando a 100 Mbps. Se incluyen dos medios (Tabla 14.4) El medio de fibra óptica usa codificación 4B/5B-NRZI. Se especifican dos medios de par trenzado: par trenzado apantallado de clase 5[6] de 100 ohmios y par trenzado apantallado de 150 ohmios. Se usa codificación MLT-3 en ambos medios de par trenzado. Véase Apéndice 14A para un estudio de estos esquemas de codificación.

14.3. REDES LAN ATM

En el documento sobre redes de usuario preparado conjuntamente por Apple, Bellcore, Sun, y Xerox [ABSX92] se identifican tres generaciones de redes LAN:

- **Primera generación:** identificada por las redes LAN CSMA/CD y en anillo con paso de testigo. La primera generación proporcionaba conectividad entre terminal-estación y admitía arquitecturas cliente/servidor a velocidades de transmisión de datos moderadas.
- **Segunda generación:** identificada con FDDI. La segunda generación responde a la necesidad de las redes troncales y para dar servicio de conectividad a estaciones de trabajo de altas prestaciones.

[6] Véase el Capítulo 4 para un estudio del cable de par trenzado no apantallado de clase 5.

- **Tercera generación:** correspondiente a redes LAN ATM. La tercera generación se ha diseñado para proporcionar los rendimientos conjuntos y garantizar el transporte de datos en tiempo real, necesarios en aplicaciones multimedia.

Requisitos típicos de la tercera generación de redes LAN son:

- Admisión de clase de servicio múltiples y garantizadas. Una aplicación de vídeo en directo, por ejemplo, puede requerir una conexión garantizada de 2 Mbps para garantizar unas prestaciones aceptables, mientras que un programa de transferencia de ficheros puede hacer uso de una clase de servicio menos exigente.
- Posibilidad de procedimiento escalable con capacidad de crecimiento, tanto en lo que se refiere a la capacidad por estación (para permitir aplicaciones que necesitan grandes volúmenes de datos hacia y desde una única estación) como a la capacidad conjunta (para permitir el crecimiento de instalaciones desde unos pocos hasta varios cientos de estaciones de altas prestaciones).
- Facilitar la interconexión de redes de tecnología LAN y WAN.

ATM ha sido diseñada inicialmente para satisfacer estos requisitos. Haciendo uso de caminos y canales virtuales se pueden admitir varias clases de servicios, considerando un establecimiento preconfigurado (conexiones permanentes) o teniendo en cuenta la demanda (conexiones conmutadas). ATM resulta fácilmente escalable mediante la incorporación de más nodos de conmutación ATM y haciendo uso de velocidades de transmisión de datos superiores (o inferiores) para los dispositivos conectados. Por último, con la creciente aceptación del transporte en celdas en redes de área amplia, el uso de ATM en una red preexistente posibilita la integración transparente de redes LAN y WAN.

El término LAN ATM se ha empleado por vendedores e investigadores par aplicarlo a una gran variedad de configuraciones. Como mínimo, una LAN ATM implica el uso del protocolo de transporte ATM en algún lugar dentro de las premisa locales. Entre los posibles tipos de redes LAN se encuentran:

- **Pasarela a ATM WAN:** un conmutador ATM funciona como un dispositivo de encaminamiento y un concentrador de tráfico para conectar una red preexistente con una red WAN ATM.
- **Conmutador ATM troncal:** la interconexión de otras redes LAN se realiza a través de un único conmutador ATM o mediante una red local de conmutadores ATM.
- **ATM de grupo de trabajo:** las estaciones de trabajo multimedia de altas prestaciones y otros sistemas finales se conectan directamente con un conmutador ATM.

Éstas son las configuraciones «puras». En la práctica se usan dos o los tres tipos de redes para crear una LAN ATM.

La Figura 14.11 muestra un ejemplo de una LAN ATM troncal que incluye enlaces hacia el mundo exterior. En este ejemplo la red ATM local consta de cuatro conmutadores interconectados con enlaces punto a punto de alta velocidad operando a las velocidades de transmisión de datos estándares de 155 y 622 Mbps. En la configuración preexistente hay otras tres redes LAN, cada una de ellas con una conexión directa a uno de los conmutadores ATM. La velocidad de transmisión de datos desde un conmutador ATM conectado a una LAN se ajusta a la velocidad de datos de esta LAN. Por ejemplo, la conexión con la red FDDI es de 100 Mbps. Así, el conmutador debe incluir cierta capacidad de almacenamiento temporal y de conversión de velocidad para transformar la velocidad de datos de la LAN conectada a una velocidad ATM. El conmutador ATM debe implementar también algún tipo de protocolo de conversión del protocolo MAC empleado en la LAN a la secuencia de celdas ATM usada en la red ATM. Un enfoque sencillo consiste en que cada conmutador ATM que se conecta con una LAN funcione como un puente o como un dispositivo de encaminamiento[7].

Una configuración LAN ATM como la mostrada en la Figura 14.11 ofrece un método relativamente sencillo para insertar una red troncal de alta velocidad en un entorno local. A medida que crece la

[7] La funcionalidad de puentes y dispositivos de encaminamiento se estudia con detalle en los Capítulos 13 y 15.

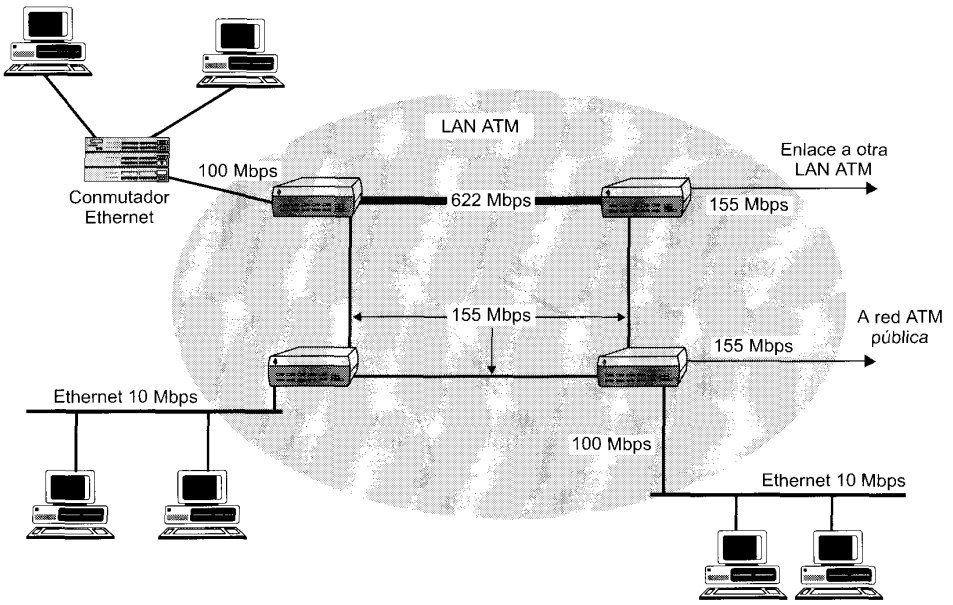


Figura 14.11. Ejemplo de configuración de red LAN ATM.

demanda, se puede incrementar fácilmente la capacidad de la red troncal mediante la incorporación de más conmutadores, aumentando el rendimiento de cada uno de ellos e incrementando la velocidad de transmisión de los enlaces entre conmutadores. Con esta estrategia se puede aumentar la carga de las LAN individuales y puede crecer el número de LAN.

Sin embargo, esta sencilla LAN ATM troncal no satisface todas las necesidades de comunicaciones locales. En particular, en la configuración troncal, los sistemas finales (estaciones de trabajo, servidores, etc.) permanecen conectados a redes LAN de medio compartido con las limitaciones impuestas por éstas sobre la velocidad de transmisión de datos.

Una solución más avanzada y potente es el empleo de un centro con tecnología ATM. La Figura 14.12 sugiere las posibilidades que puede ofrecer este enfoque. Cada centro ATM incluye un conjunto de puertos que funcionan a distintas velocidades de transmisión y hacen uso de diferentes protocolos. Generalmente, estos centros constan de varios módulos montados en un chasis, cada uno de ellos conteniendo puertos de velocidad y protocolo determinados.

La diferencia básica entre el centro ATM mostrado en la Figura 14.12 y los nodos ATM de la Figura 14.11 es la forma en que se gestiona cada uno de los sistemas finales. Obsérvese que en el centro ATM cada sistema final tiene un enlace punto a punto dedicado con el centro. Cada sistema final incluye el hardware y el software de comunicaciones necesarios para conectarse a un tipo específico de LAN, pero, en cada caso, la red LAN sólo contiene dos dispositivos: el sistema final y el centro. Por ejemplo, cada dispositivo conectado a un puerto Ethernet a 10 Mbps hace uso del protocolo CSMA/CD a 10 Mbps. Sin embargo, dado que cada sistema final tiene su propia línea dedicada, el efecto es que cada sistema final tiene su propia Ethernet a 10 Mbps dedicada. Por tanto, cada sistema final puede funcionar a una velocidad de transmisión máxima cercana a 10 Mbps.

El uso de una configuración como las de las Figuras 14.11 o 14.12 presenta la ventaja de que se pueden continuar usando las instalaciones y el hardware LAN existentes, también denominadas LAN tradicionales, mientras se adopta la tecnología ATM. La desventaja consiste en que el empleo de un

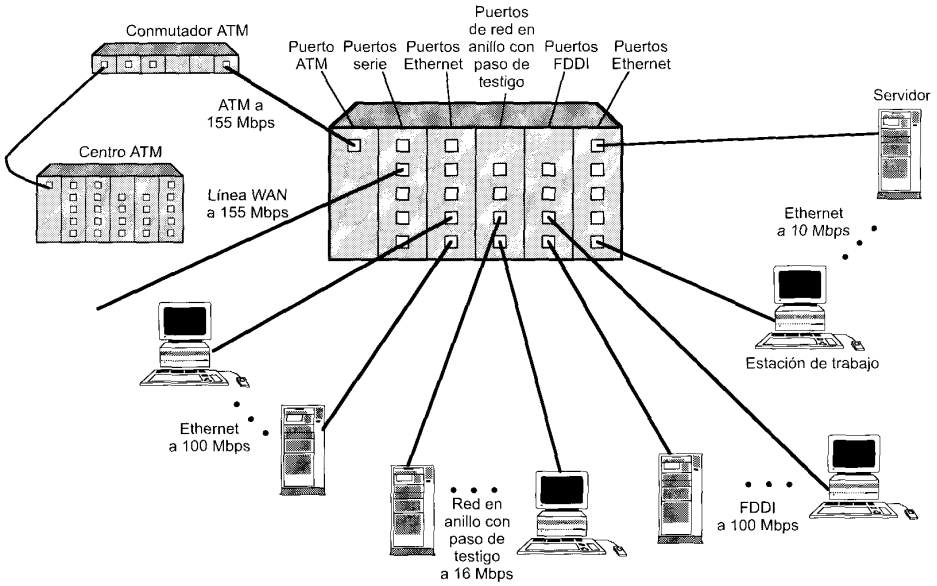


Figura 14.12. Configuración de centro LAN ATM.

entorno en que existan diversos protocolos necesita la implementación de algún método de conversión entre ellos. Una aproximación más sencilla, pero que requiere que los sistemas finales estén equipados con capacidades ATM, es la implementación de una red LAN ATM «pura».

Una cuestión no tratada en la discusión anterior es el problema de la intercomunicación de sistemas finales en distintos tipos de LAN interconectadas. Los sistemas finales conectados directamente a una de las LAN tradicionales implementan la capa MAC apropiada para ese tipo de LAN. Los sistemas finales conectados directamente a una red ATM implementan los protocolos ATM y AAL. Como resultado, deben considerarse tres áreas de compatibilidad:

- Interacción entre un sistema final en una red ATM y un sistema final en una LAN tradicional.
- Interacción entre un sistema final en una LAN tradicional y un sistema final en otra LAN tradicional del mismo tipo (por ejemplo, dos redes IEEE 802.3).
- Interacción entre un sistema final en una LAN tradicional y un sistema final en otra LAN tradicional de distinto tipo (por ejemplo, una red IEEE 802.3 y una IEEE 802.5).

14.4. CANAL DE FIBRA ÓPTICA

A medida que ha crecido la velocidad y la capacidad de memoria de los computadores personales, estaciones de trabajo y servidores, y a medida que las aplicaciones se han hecho más complejas con más seguridad en gráficos y vídeo, ha aumentado la necesidad de procesadores de mayor velocidad en el envío de datos. Este requisito afecta a dos métodos de comunicaciones de datos con el procesador: canal de entrada/salida y comunicaciones de red.

Un canal de entrada/salida es un enlace de comunicaciones punto a punto directo o uno multipunto, generalmente hardware y diseñado para conseguir altas velocidades de transmisión en distancias muy cortas. El canal de entrada/salida transfiere datos entre una memoria temporal en el dispositivo origen y

una memoria temporal en el dispositivo de destino, limitándose sólo a desplazar los contenidos de usuario desde un dispositivo al otro sin tener en cuenta el formato o significado de los datos. La lógica asociada al canal proporciona generalmente el control mínimo necesario para gestionar la transferencia además de la detección de errores hardware. Los canales de entrada/salida gestionan generalmente transferencias entre procesadores y dispositivos periféricos tales como discos, equipos gráficos, equipos CD-ROM y dispositivos de entrada/salida de vídeo.

Una red es un conjunto de puntos de acceso interconectados con una estructura software de protocolos que posibilita la comunicación. La red admite generalmente diferentes tipos de transferencia de datos, haciendo uso de software para implementar los protocolos de red y para proporcionar control de flujo y detección y recuperación de errores. Como se ha discutido en este texto, las redes gestionan generalmente las transferencias entre sistemas finales en distancias locales, metropolitanas o de área amplia.

El canal de fibra está diseñado para combinar las características más sobresalientes de estas tecnologías —la sencillez y velocidad de las comunicaciones de canal— con la flexibilidad e interconectividad que caracterizan a las comunicaciones de red basadas en protocolos. Esta fusión de enfoques permite a los diseñadores de sistemas combinar la conexión tradicional de periféricos, la interconexión de redes estación-estación, la agrupación de procesadores débilmente acoplados y el uso de aplicaciones multimedia en una misma interfaz multiprotocolo. Entre los tipos de recursos orientados a canal incorporados en la arquitectura de protocolos del canal de fibra se encuentran:

- Modificadores de tipos de datos para encaminar la carga útil contenida en tramas sobre memorias temporales de interfaz específicas.
- Elementos del nivel de enlace asociados con operaciones individuales de entrada/salida.
- Especificaciones de interfaz de protocolo para dar soporte a arquitecturas de canal de entrada/salida existentes, tales como la interfaz SCSI («small computer system interface»).

Entre los tipos de recursos orientados a red incorporados en la arquitectura de protocolos del canal de fibra se encuentran los siguientes:

- Multiplexación completa de tráfico entre múltiples destinos.
- Conectividad igual a igual (paritaria) entre cualquier par de puertos en una red de canal de fibra.
- Posibilidad de interconexión con otras tecnologías.

ELEMENTOS DEL CANAL DE FIBRA

Los elementos principales de una red de canal de fibra son los sistemas finales, denominados *nodos*, y la red propiamente dicha, que consta de uno o más elementos de conmutación. El conjunto de elementos de conmutación se denomina *estructura*. Estos elementos se encuentran interconectados mediante enlaces punto a punto entre puertos a través de nodos individuales y conmutadores. La comunicación consiste en la transmisión de las tramas a través de los enlaces punto a punto.

Cada nodo incluye uno o más puertos, llamados N_puertos, para la interconexión. Análogamente, cada elemento de conmutación de la estructura incluye varios puertos, llamados F_puertos. La interconexión se realiza mediante enlaces bidireccionales entre puertos. Cualquier nodo puede comunicarse con otro nodo conectado a la misma estructura haciendo uso de los servicios de ésta. Todo el encaminamiento de tramas entre N_puertos lo lleva a cabo la estructura. Las tramas se pueden almacenar temporalmente en la estructura, haciendo posible que se conecten a ésta nodos con distintas velocidades de transmisión.

Como se muestra en la Figura 14.13, una estructura puede implementarse como un único elemento de estructura con nodos conectados (una simple disposición en estrella) o como una red más general de elementos de estructura. En cualquier caso, la estructura es responsable del almacenamiento temporal y encaminamiento de tramas entre los nodos origen y destino.

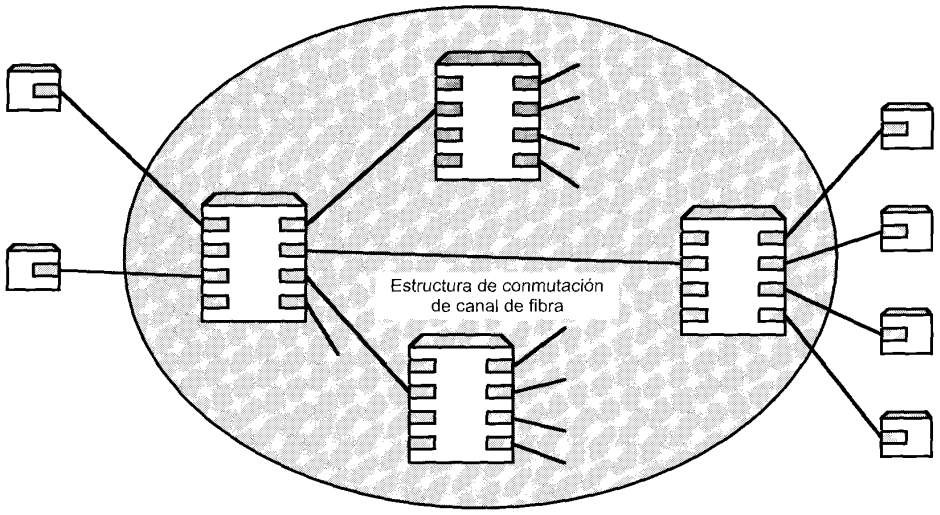


Figura 14.13. Red de canal de fibra.

La red de canal de fibra es bastante diferente de las LAN IEEE 802. En contraste con las LAN típicas de medio compartido, el canal de fibra es más parecido a una red tradicional de conmutación de circuitos o de paquetes. Así, el canal de fibra no necesita estar relacionado con cuestiones de control de acceso al medio. Dado que se basa en una red de conmutación, el canal de fibra escala fácilmente, en términos de N_puertos, la velocidad de transmisión de datos y la distancia cubierta. Este enfoque proporciona una gran flexibilidad. El canal de fibra se puede acomodar fácilmente a nuevos medios y velocidades de transmisión mediante la incorporación de nuevos conmutadores y F_puertos a una estructura ya existente. Así, una inversión realizada no se pierde ante una actualización a nuevas tecnologías y equipamiento. Además, la arquitectura de protocolos en niveles admite las interfaces de entrada/salida y los protocolos de red existentes, preservando la inversión realizada.

ARQUITECTURA DE PROTOCOLOS DEL CANAL DE FIBRA

El estándar de canal de fibra se organiza en cinco niveles, definiendo cada uno de ellos una función o conjunto de funciones relacionadas. El estándar no establece una correspondencia entre niveles y las implementaciones reales, con una interfaz específica entre niveles adyacentes. Es más, el estándar se refiere al nivel como un «documento artificio» usado para funciones relacionadas con el grupo. Las capas son las siguientes:

- **Medio físico FC-0:** incluye fibra óptica para aplicaciones de larga distancia, cable coaxial para altas velocidades a cortas distancias y par trenzado apantallado para bajas velocidades sobre cortas distancias.
- **Protocolo de transmisión FC-1:** define el esquema de codificación de señal 8B/10B, que se describe en el Apéndice 14A.
- **Protocolo de fragmentación o delimitación FC-2:** incluye topologías definidas, formato de trama, control de flujo y de errores y agrupación de tramas en entidades lógicas llamadas secuencias y permutas.
- **Servicios comunes FC-3:** incluye multidestino.

Tabla 14.5. Distancia máxima para los distintos tipos de medios de canal de fibra óptica.

	800 Mbps	400 Mbps	200 Mbps	100 Mbps
Fibra de modo simple	10 km	10 km	10 km	—
Fibra multimodo de 50 μm	0,5 km	1 km	2 km	—
Fibra multimodo de 62,5 μm	175 m	1 km	1 km	—
Cable coaxial de vídeo	50 m	71 m	100 m	100 m
Cable coaxial en miniatura	14 m	19 m	28 m	42 m
Par trenzado apantallado	28 m	46 m	57 m	80 m

- **Transformación FC-4:** define la conversión de distintos protocolos de canal y de red a canal de fibra, incluyendo IEEE 802, ATM, IP y la interfaz SCSI.

Una de las mayores ventajas del estándar de canal de fibra es permitir distintas opciones para el medio físico, su velocidad y la topología de la red. En la Tabla 14.5 se resumen las opciones posibles para el canal de fibra en cuanto a medios de transmisión y velocidades. Cada elemento de la tabla especifica la distancia máxima del enlace punto a punto (entre puertos) definida para un medio de transmisión a una velocidad dada. Estos medios se pueden mezclar en una configuración completa. Por ejemplo, se podría usar un enlace óptico de modo simple para conectar conmutadores en diferentes edificios, enlaces ópticos multimodo para conectar una distribución vertical interna y enlaces de par trenzado apantallado o de cable coaxial para las estaciones individuales.

14.5. LAN INALÁMBRICAS

El comité IEEE 802.11 ha desarrollado un conjunto de normalizaciones para redes LAN inalámbricas. La terminología y algunas de las características específicas de 802.11 son exclusivas de este estándar y no se reflejan en todos los productos comerciales. Sin embargo, es útil familiarizarse con el estándar dado que sus características son representativas de las capacidades necesarias en LAN inalámbricas.

En la Figura 14.14 se indica el modelo desarrollado por el grupo de trabajo 802.11. El bloque más elemental de una LAN inalámbrica es un conjunto de servicios básicos (BSS, Basic Services Set), consistente en varias estaciones ejecutando el mismo protocolo MAC y compitiendo para acceder al mismo medio compartido. Un BSS puede ser aislado o puede conectarse con un sistema troncal de distribución a través de un punto de acceso, que funciona como un puente. El protocolo MAC puede ser completamente distribuido o controlado por una función de coordinación central localizada en el punto de acceso. El conjunto de servicios básicos corresponde generalmente con lo que se conoce en la bibliografía como una celda o célula.

Un conjunto de servicios de ampliación (ESS, Extended Services Set) consta de dos o más servicios básicos interconectados por un sistema de distribución. Generalmente, el sistema de distribución es una LAN troncal cableada. El conjunto de servicios de ampliación aparece en el nivel de control de enlace lógico (LLC) como una única LAN lógica.

El estándar define tres tipos de estaciones según la movilidad:

- **Sin transición.** Una estación de este tipo es estacionaria o se mueve sólo en el rango de comunicaciones directas de las estaciones de comunicaciones de un único BSS.
- **Transición BSS.** Este tipo comprende estaciones que se desplazan de un BSS a otro BSS en el mismo ESS. En este caso, el envío de datos a la estación requiere que la capacidad de direccionamiento esté preparada para reconocer la nueva localización de la estación.

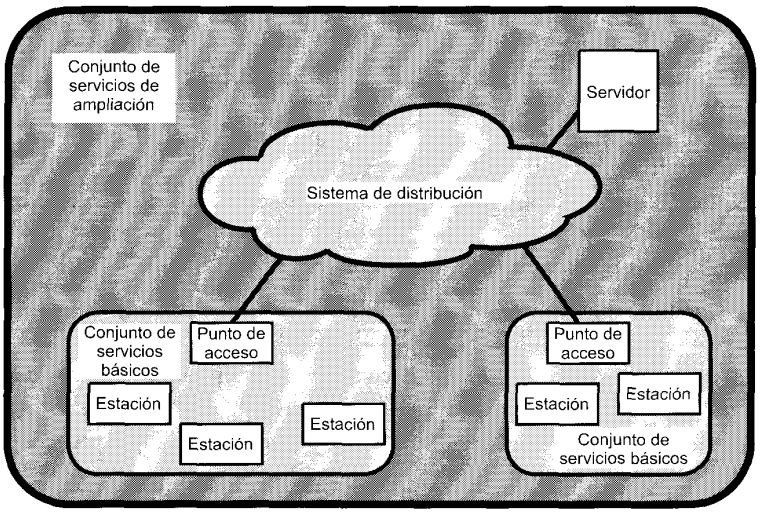


Figura 14.14. Arquitectura IEEE 802.11.

- **Transición ESS.** Se define como el desplazamiento de una estación desde un BSS en un ESS a un BSS en otro ESS. Este caso se admite sólo en el sentido de que la estación se puede desplazar, no pudiéndose garantizar el mantenimiento de conexiones de capas superiores incluido en 802.11. De hecho, es probable que se produzca una interrupción del servicio.

ESPECIFICACIÓN DEL MEDIO FÍSICO

En la normalización 802.11 actual se definen tres esquemas de transmisión:

- **Infrarrojos** a 1 y 2 Mbps funcionando con una longitud de onda comprendida entre 850 y 950 nm.
- **Espectro expandido de secuencia directa** operando en la banda ISM de 2,4 GHz. Se pueden utilizar 7 canales como máximo, cada uno de ellos con una velocidad de transmisión de 1 o 2 Mbps.
- **Espectro expandido de salto de frecuencia** funcionando en la banda ISM de 2,4 GHz, con una velocidad de transmisión de 1 o 2 Mbps.

Dos proyectos en marcha trabajan sobre opciones a 2,4 GHz operando a 3 Mbps para salto de frecuencia y a 8 Mbps para secuencia directa, y opciones de espectro expandido a 5 GHz operando a 20 Mbps.

CONTROL DE ACCESO AL MEDIO

El grupo de trabajo 802.11 consideró dos tipos de propuestas para un algoritmo MAC: protocolos de acceso distribuido, que, como CSMA/CD, distribuyen la decisión de transmitir entre todos los nodos usando un mecanismo de detección de portadora, y protocolos de acceso centralizado, que implican la gestión centralizada de la transmisión. Un protocolo de acceso distribuido tiene sentido en una red *ad hoc* de estaciones de trabajo paritarias, pudiendo resultar también atractivo para otras configuraciones de LAN inalámbricas que presentan principalmente tráfico a ráfagas. Un protocolo de acceso centralizado es de uso natural en configuraciones en las que varias estaciones inalámbricas se encuentran conectadas entre sí y con alguna estación base conectada a una LAN cableada troncal; es especialmente útil si alguno de los datos es sensible al tiempo o de alta prioridad.

El resultado final del 802.11 es un algoritmo MAC llamado MAC inalámbrico de principio distribuido (DFWMAC, Distributed Foundation Wireless MAC), que proporciona un mecanismo de control de acceso distribuido con un control centralizado opcional implementado sobre él. En la Figura 14.15 se ilustra la arquitectura. La subcapa inferior de la capa MAC es la función de coordinación distribuida (DCF, Distributed Coordination Function), que emplea un algoritmo de contención o competición para proporcionar acceso a todo el tráfico. El tráfico asíncrono ordinario usa directamente DCF. La función de coordinación puntual (PCF, Point Coordination Function) es un algoritmo MAC centralizado utilizado para proporcionar un servicio sin competición. PCF se implementa sobre DCF y aprovecha las características de DCF para asegurar el acceso a sus usuarios. Consideremos estas dos subcapas.

Función de coordinación distribuida

La subcapa DCF hace uso de un sencillo algoritmo CSMA. Si una estación desea transmitir una trama MAC, escucha el medio. Si el medio se encuentra libre, la estación puede transmitir; si no debe esperar hasta que se haya completado la transmisión en curso antes de poder transmitir. DCF no incluye una función de detección de colisiones (es decir, CSMA/CD) puesto que la detección de colisión no resulta práctica en redes inalámbricas. El rango dinámico de las señales en el medio es muy elevado, de manera que una estación que transmita no puede distinguir de forma efectiva entre las señales débiles de entrada del ruido y los efectos de su propia transmisión.

Para asegurar el correcto funcionamiento de este algoritmo, DCF incluye un conjunto de retardos que equivale a un esquema de prioridades. Comencemos considerando un único retardo conocido como espacio intertrama (IFS). En la práctica existen tres valores diferentes de IFS, pero el algoritmo se comprende mejor ignorando inicialmente este detalle. Haciendo uso de un IFS, las reglas de acceso CSMA son:

1. Una estación con una trama a transmitir sondea el medio. Si éste está libre, la estación espera ver si el medio permanece libre durante un tiempo igual a IFS. Si es así, la estación puede transmitir inmediatamente.
2. Si el medio está ocupado (bien porque la estación lo encuentra inicialmente así o porque está ocupado durante el tiempo libre IFS), la estación aplaza la transmisión y continúa supervisando el medio hasta que finalice la transmisión en curso.

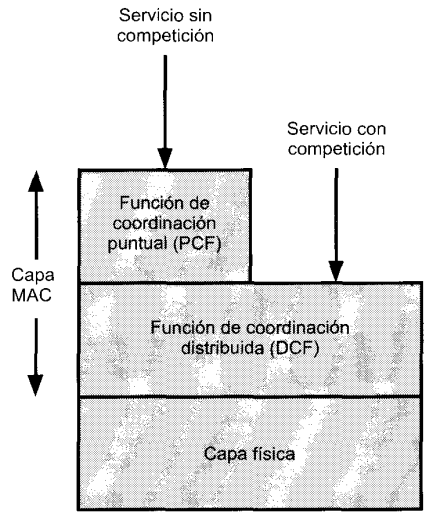


Figura 14.15. Arquitectura de protocolos IEEE 802.11.

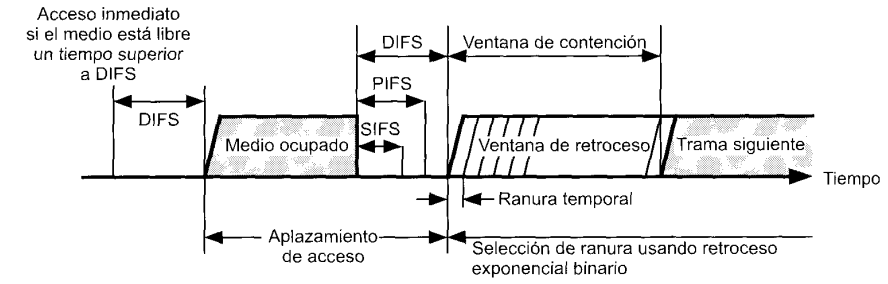
3. Una vez que ha ocurrido esto, la estación espera otro IFS. Si el medio permanece libre durante este periodo, la estación espera según un esquema de retroceso exponencial binario y sondea de nuevo el medio. Si éste se encuentra libre aún, la estación puede transmitir.

Como en Ethernet, la técnica de retroceso exponencial binario proporciona un método para gestionar una carga alta. Si una estación intenta transmitir y encuentra ocupado el medio, espera un cierto tiempo y lo intenta de nuevo. Sucesivos intentos de transmisión fallidos provocan tiempos de retroceso cada vez mayores.

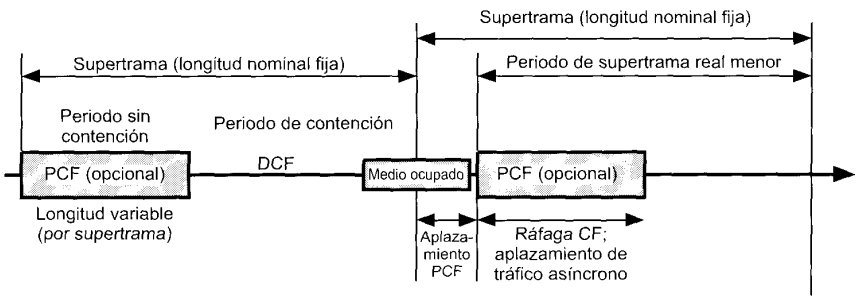
El esquema anterior se ha mejorado para que DCF proporcione un acceso basado en prioridades simplemente mediante el uso de tres valores de IFS:

- **SIFS (IFS corto):** es el IFS más breve, y se usa para todas las acciones de respuesta inmediata como se explica más adelante.
- **PIFS (función de coordinación puntual IFS):** IFS de longitud intermedia, empleado por el controlador centralizado en el esquema PCF cuando realiza sondeos.
- **DIFS (función de coordinación distribuida IFS):** es el IFS mayor y se utiliza como retardo mínimo para tramas asíncronas que compiten para conseguir el acceso.

En la Figura 14.16a se ilustra el uso de estos valores temporales. Consideremos primero el SIFS. Cualquier estación que use SIFS para determinar la oportunidad de transmitir tiene, de hecho, la prioridad superior, ya que siempre conseguirá el acceso en preferencia a una estación que espera una cantidad de tiempo igual a PIFS o DIFS. SIFS se utiliza en las siguientes circunstancias:



(a) Método de acceso básico



(b) Construcción de supertrama PCF

Figura 14.16. Temporización MAC IEEE 802.11.

- **Confirmación (ACK):** cuando una estación recibe una trama dirigida sólo a ella (no multidestino ni de difusión), responde con una trama ACK (acknowledge) después de esperar un tiempo SIFS. Esto presenta dos efectos deseables. En primer lugar, dado que no se usa la detección de colisión, la probabilidad de colisiones es mayor que en CSMA/CD, permitiendo la trama ACK de nivel MAC la recuperación eficiente de éstas. En segundo lugar, SIFS se puede emplear para proporcionar un envío eficiente de una unidad de datos de protocolo LLC que necesite varias tramas MAC. En este caso se produce la siguiente situación. Una estación con una PDU LLC multitrama a transmitir envía las tramas MAC de una en una. Tras un SIFS, el receptor confirma cada una de las tramas. Cuando el origen recibe una trama ACK, inmediatamente (tras un SIFS) envía la siguiente trama de la secuencia. El resultado es que una vez que una estación ha luchado por conseguir el canal, mantendrá el control de éste hasta que haya enviado todos los fragmentos de una PDU LLC.
- **Permiso para enviar (CTS):** una estación puede asegurar que su trama de datos se enviará emitiendo primero una pequeña trama de petición de envío (RTS, Request To Send). La estación a la que va dirigida esta trama debería responder inmediatamente con una trama CTS (Clear To Send) si está lista para recibir. El resto de estaciones reciben el RTS y aplazan el uso del medio hasta que detectan un CTS correspondiente o hasta que expire un contador de tiempo.
- **Respuesta ante sondeo:** ésta se explica en la discusión sobre PCF más adelante.

El siguiente intervalo IFS más largo es el PIFS, usado por el controlador centralizado para llevar a cabo el envío de sondeos, y tiene prioridad sobre tráfico de contención normal. Sin embargo, las tramas transmitidas usando SIFS tienen prioridad sobre un sondeo PCF.

Por último, el intervalo DIFS se usa para todo tráfico asíncrono ordinario.

Función de coordinación puntual

La función de coordinación puntual (PCF, Point Coordination Function) es un método de acceso alternativo implementado en un nivel superior a DCF. El procedimiento consiste en la realización de un sondeo por parte del gestor de sondeo centralizado (coordinador puntual). El coordinador puntual hace uso de PIFS cuando realiza sondeos. Dado que PIFS es menor que DIFS, el coordinador puntual puede tomar el medio y bloquear todo el tráfico asíncrono mientras realiza sondeos y recibe respuestas.

Consideremos la siguiente situación extrema. Una red inalámbrica se configura de modo que varias estaciones con tráfico sensible al tiempo son controladas por el coordinador puntual, mientras que el resto del tráfico compite haciendo uso de CSMA para conseguir el acceso. El coordinador puntual podría realizar sondeos en forma de rotación circular a todas las estaciones configuradas para sondeo. Cuando se realiza un sondeo, la estación sondeada puede responder usando SIFS. Si el coordinador puntual recibe una respuesta, envía otro sondeo usando PIFS. Si no se recibe respuesta durante el tiempo esperado de exploración circular de todas las estaciones, el coordinador envía un sondeo.

Si se implementase el esquema del párrafo anterior, el coordinador puntual paralizaría todo el tráfico asíncrono mediante le envío repetido de sondeos. Para evitar esto se define un intervalo conocido como supertrama. Durante la primera parte de este intervalo, el coordinador puntual envía sondeos en forma de rotación circular a todas las estaciones configuradas para sondeo. El coordinador puntual está ocioso durante el resto de la supertrama, permitiendo un periodo de contención para acceso asíncrono.

En la Figura 14.16b se ilustra el uso de la supertrama. Al comienzo de ésta, el coordinador puntual puede tomar opcionalmente el control y enviar sondeos durante un periodo de tiempo dado. Este intervalo cambia debido al tamaño variable de la trama enviada por las estaciones correspondientes. El resto de la supertrama se encuentra disponible para un acceso basado en contención. Al final del intervalo de supertrama, el coordinador puntual compite para conseguir el medio usando PIFS. Si el medio se encuentra libre, el coordinador puntual obtiene inmediatamente el acceso y sigue un periodo de trama

completo. Sin embargo, el medio puede estar ocupado al final de una supertrama, en cuyo caso el coordinador puntual debe esperar hasta que el medio se encuentre libre para conseguir el acceso; esto da lugar a un periodo de supertrama menor para el siguiente ciclo.

14.6. LECTURAS Y SITIOS WEB RECOMENDADOS

En [STAL00] se discute en detalle todos los sistemas LAN presentados en este capítulo.

[SPUR96] proporciona un estudio conciso pero completo de todos los sistemas 802.3 a 10 y 100 Mbps, incluyendo especificaciones de configuración para un único segmento de cada tipo de medio, así como pautas sobre redes Ethernet multisegmento de edificios usando varios tipos de medios. [SEIF98] y [KADA98] comprenden excelentes tratamientos tanto sobre Ethernet a 100 Mbps como a velocidades de Gigabits. Asimismo, un buen artículo sobre Ethernet de Gigabits es [FRAZ99]. [CARL98] trata en cierta profundidad las LAN en anillo con paso de testigo. Por su parte, [MILL95] y [SHAH94] lo hacen sobre FDDI, profundizando el primero de ellos en aspectos de la capa física y el segundo sobre el protocolo MAC. [KAVA95] y [NEWM94] son buenos artículos de revisión acerca de la arquitectura y configuraciones LAN ATM, y [SACH96] sobre el canal de fibra. [CROW97] revisa el estándar de LAN inalámbricas 802.11.

Entre los libros con un riguroso tratamiento acerca de las prestaciones LAN/MAN se encuentran [STUC85], [SPRA91] y [BERT92].

BERT92 Bertsekas, D., y Gallager, R. *Data Networks*. Englewood Cliffs, NJ: Prentice Hall, 1992.

CARL98 Carlo, J., et al. *Understanding Token Ring Protocols and Standards*. Boston: Artech House, 1998.

CROW97 Crow, B., et al. «IEEE 802.11 Wireless Local Area Networks.» *IEEE Communications Magazine*, September 1997.

FRAZ99 Frazier, H., y Johnson, H. «Gigabit Ethernet: From 100 to 1,000 Mbps.» *IEEE Internet Computing*, January/February 1999.

HAMM86 Hammond, J., y O'Reilly, P. *Performance Analysis of Local Computer Networks*. Reading, MA: Addison-Wesley, 1986.

KADA98 Kadambi, J.; Crayford, I.; y Kalkunte, M. *Gigabit Ethernet*. Upper Saddle River, NJ: Prentice Hall, 1998.

KAVA95 Kavak, N. «Data Communication in ATM Networks.» *IEEE Network*, May/June 1995.

MILL95 Mills, A. *Understanding FDDI*. Englewood Cliffs, NJ: Prentice Hall, 1995.

NEWM94 Newman, P. «ATM Local Networks.» *IEEE Communications Magazine*, March 1994.

SACH96 Sachs. M., y Varma, A. «Fibre Channel and Related Standars.» *IEEE Communications Magazine*, August 1996.

SEIF98 Seifert, R. *Gigabit Ethernet*. Reading, MA: Addison-Wesley, 1998.

SHAH94 Shah, A., y Ramakrishnan, G. *FDDI: A High-Speed Network*. Englewood Cliffs, NJ: Prentice Hall, 1994.

SPRA91 Spragins, J.; Hammond, J.; y Pawlikowski, K. *Telecomunications Protocols and Design*. Reading, MA: Addison-Wesley, 1991.

SPUR96 Spurgeon, C. *Ethernet Configuration Guidelines*. San Jose, CA: Peer-to-Peer Communications, 1996.

STAL00 Stallings, W. *Local and Metropolitan Area Networks, 6th edition.* Upper Saddle River, NJ: Prentice Hall, 2000.

STUC85 Stuck, B., y Arthurs, E. *A Computer Communications Network Performance Analysis Primer.* Englewood Cliffs, NJ: Prentice Hall, 1985.

SITIOS WEB RECOMENDADOS

- **Laboratorio de interoperabilidad:** sitio Web de la Universidad de New Hampshire para equipos de test ATM, Ethernet a alta velocidad y otras redes LAN.
- **Alianza de Ethernet a Gigabits:** foro abierto con objeto de promover la cooperación industrial para el desarrollo de la Ethernet a Gigabits.

14.7. PROBLEMAS

14.1. Un inconveniente de las técnicas de contención o competición en redes LAN es no aprovechar la capacidad debido al hecho de que varias estaciones intentan acceder simultáneamente al canal. Supongamos que se divide el tiempo en ranuras discretas, con cada una de N estaciones intentando transmitir con probabilidad p durante cada ranura temporal. ¿Qué fracción de ranuras se desaprovecha debido a múltiples intentos de transmisión simultáneos?

14.2. Un protocolo sencillo de control de acceso al medio podría consistir en usar un esquema de multiplexación por división en el tiempo (TDM), tal como se describió en la Sección 8.2. A cada estación se le asigna una ranura de tiempo por ciclo de transmisión. Para redes en bus, la duración de cada ranura es el tiempo necesario para transmitir 100 bits más el retardo de propagación extremo a extremo. Para redes en anillo, suponga un retardo igual a la duración del intervalo de un bit por estación y que se usa una asignación en forma de rotación circular. Las estaciones supervisan todas las ranuras de tiempo para recepción. Supóngase una velocidad de propagación de 2×10^8 m/s. Para N estaciones, calcule el rendimiento por estación para:

a) Un bus de banda base de 1 km y 10 Mbps.

b) Un anillo a 10 Mbps con una longitud total de 1 km.

c) Un anillo a 10 Mbps con una longitud de 0,1 km entre repetidores.

d) Obtenga el rendimiento para todos los casos anteriores para 10 y 100 estaciones.

14.3. Considérense dos estaciones en un bus de banda base separadas una distancia de 1 km. Sea la velocidad de transmisión de datos 1 Mbps, la longitud de la trama 100 bits y la velocidad de propagación 2×10^8 m/s. Supongamos que cada estación genera tramas a una velocidad promedio de 10.000 tramas por segundo. Para el protocolo ALOHA, si una estación comienza a transmitir una trama en el instante de tiempo t, ¿cuál es la probabilidad de que se produzca colisión? Repita el proceso para ALOHA ranurado. Repita el proceso para ALOHA y ALOHA ranurado a 10 Mbps.

14.4. El algoritmo de retroceso exponencial binario se define en IEEE 802 como sigue:

> El retardo es un múltiplo entero de tiempo de ranura. El número de ranuras de tiempo de retardo antes del n-ésimo intento de retransmisión se elige como un entero aleatorio r distribuido uniformemente en el rango $0 \leqslant r < 2^K$, donde $K = \min(n, 10)$.

La duración de la ranura de tiempo es, aproximadamente, dos veces el retardo de propagación en el trayecto de ida y vuelta. Supongamos que siempre hay dos estaciones con una trama a transmitir. Después de una colisión, ¿cuál es el número medio de intentos de transmisión antes de que una estación lo consiga con éxito? ¿Y si siempre hay tres estaciones que tienen tramas que transmitir?

14.5. Suponga que la estación de destino en una LAN en anillo con paso de testigo elimina la trama de datos y envía inmediatamente una trama corta de confirmación al emisor, en lugar de dejar que la trama vuelva a éste. ¿Cómo se ve afectada la eficiencia?

14.6. Otra técnica de control de acceso al medio para redes en anillo es el anillo ranurado, donde varias ranuras de longitud fija circulan continuamente por el anillo. Cada ranura contiene un bit inicial para especificar que está libre u ocupada. Una estación que desea transmitir espera hasta que llega una ranura libre, la marca como ocupada e inserta una trama de datos mientras la ranura la atraviesa. La ranura ocupada da una vuelta completa al anillo para que la estación que la marcó como ocupada la marque como libre. ¿En qué sentido son complementarios (duales) el anillo con paso de testigo y el anillo ranurado?

14.7. Considérese un anillo ranurado de 10 km de longitud con una velocidad de transmisión de 10 Mbps y 500 repetidores, donde cada uno de ellos introduce un retardo de 1 bit. Cada ranura da cabida a un octeto de dirección origen, un octeto de dirección destino, dos octetos de datos y cinco bits de control, obteniendo una longitud total de 37 bits. ¿Cuántas ranuras hay en el anillo?

14.8. Compare los esquemas de reserva de capacidad de anillo con paso de testigo IEEE 802.5 y FDDI. ¿Cuáles son los pros y los contras relativos de cada uno?

14.9. Rehaga el ejemplo de la Figura 14.10 usando un TTRT de 12 tramas y suponiendo que ninguna de las estaciones tiene que transmitir nunca más de 8 tramas asíncronas.

14.10. Con codificación 8B6T, la velocidad de transmisión efectiva a través de un único canal es de 33 Mbps con una velocidad de señalización de 25 Mbaudios. Si se usase un esquema ternario puro, ¿cuál sería la velocidad de datos efectiva para una velocidad de señalización de 25 Mbaudios?

14.11. Con codificación 8B6T, el algoritmo DC niega a veces todos los símbolos ternarios en un grupo de código. ¿Cómo detecta el receptor esta condición? ¿Cómo discrimina el receptor entre un grupo de código negado y uno que no lo ha sido? Por ejemplo, el grupo de código para el octeto de datos 00 es $+-00+-$ y el grupo de código del octeto de datos 38 es la negación de éste, concretamente $-+00-+$.

14.12. Dibuje el diagrama de estados del decodificador MLT que se corresponde con el diagrama de estados del codificador de la Figura 14.17.

14.13. Esboce las formas de onda NRZ-L, NRZI, Manchester, Manchester diferencial y MLT-3 para la secuencia de bits 0101110.

APÉNDICE 14A CODIFICACIÓN DE SEÑALES DIGITALES PARA REDES LAN

En el Capítulo 5 vimos algunas de las técnicas usuales de codificación de datos digitales para transmisión, incluyendo Manchester y Manchester diferencial, que se usan en algunos estándares LAN. En este apéndice examinaremos algunos esquemas de codificación adicionales citados en este capítulo.

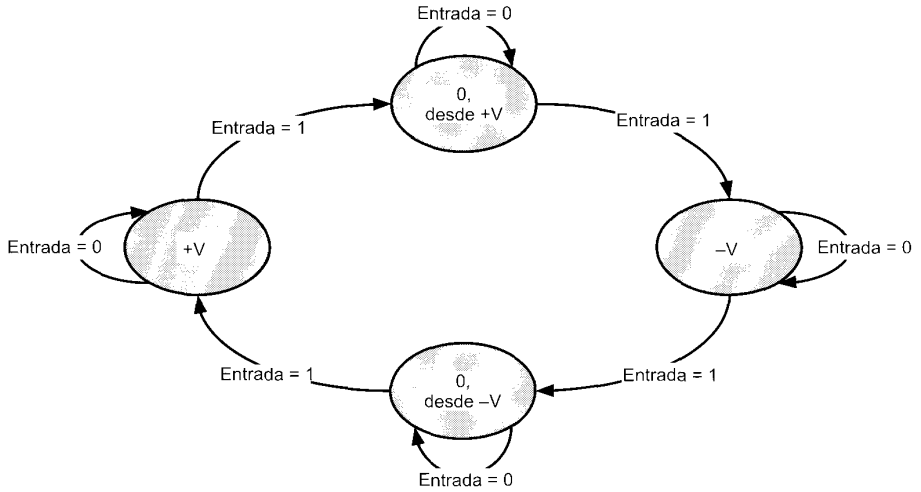


Figura 14.17. Diagrama de estados del codificador MLT-3.

4B/5B-NRZI

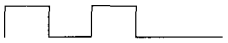
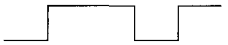
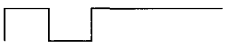
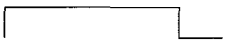
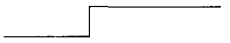
Este esquema, que es realmente una combinación de dos algoritmos de codificación, se usa tanto en 100BASE-X como en FDDI. Para comprender el significado de esta elección consideremos primero el sencillo esquema de codificación NRZ (no retorno a cero). Con NRZ, un estado de señal representa un uno binario y otro estado de señal un cero binario. El inconveniente de esta aproximación es la pérdida de sincronismo. Dado que las transiciones en el medio resultan impredecibles, no hay forma de que el receptor sincronice su reloj con el del emisor. Una solución a este problema es codificar los datos binarios de forma que se garantice la presencia de transiciones. Por ejemplo, los datos se podrían codificar primero empleando la codificación Manchester. La desventaja de esta aproximación es que la eficiencia es sólo del 50 %. Es decir, debido a que pueden existir nada menos que dos transiciones por intervalo de bit, se necesita una velocidad de señalización de 200 millones de elementos de señal por segundo (200 Mbaudios) para conseguir una velocidad de transmisión de 100 Mbps. Esto representa un coste y una carga técnica innecesarios.

Se puede conseguir una eficiencia superior haciendo uso del código 4B/5B, en el cual la codificación ser realiza en cada momento sobre 4 bits. Cada 4 bits de datos se codifican en un símbolo con cinco *bits de código*, de modo que cada bit de código contiene un único elemento de señal; el bloque de cinco bits de código se llama *grupo de código*. En efecto, cada grupo de 4 bits se codifica como 5 bits. La eficiencia se incrementa así hasta el 80 %: se consiguen 100 Mbps con 125 Mbaudios.

Para asegurar la sincronización se lleva a cabo un segundo paso de codificación: cada bit de código de la secuencia 4B/5B se trata como un valor binario y se codifica usando la técnica de no retorno a cero invertido (NRZI) (véase Figura 5.2). En este código, un 1 binario se representa como una transición al principio del intervalo de bit y un 0 binario sin transición al comienzo del intervalo de bit; es decir, no hay transiciones. La ventaja de NRZI es que emplea codificación diferencial. Recordemos del Capítulo 5 que en codificación diferencial la señal se decodifica comparando la polaridad de elementos de señal adyacentes en lugar del valor absoluto de un elemento de señal. Una ventaja de este esquema es que, en presencia de ruido y distorsión, resulta generalmente más fácil detectar una transición que comparar un valor con un umbral.

Ahora estamos en condiciones de describir el código 4B/5B y de comprender las decisiones tomadas. En la Tabla 14.6 se muestra la codificación de símbolos. Se muestra cada patrón de grupo de

Tabla 14.6. Grupos de código 4B/5B.

Datos de entrada (4 bits)	Grupo de código (5 bits)	Patrón NRZI	Interpretación
0000	11110		Dato 0
0001	01001		Dato 1
0010	10100		Dato 2
0011	10101		Dato 3
0100	01010		Dato 4
0101	01011		Dato 5
0110	01110		Dato 6
0111	01111		Dato 7
1000	10010		Dato 8
1001	10011		Dato 9
1010	10110		Dato A
1011	10111		Dato B
1100	11010		Dato C
1101	11011		Dato D
1110	11100		Dato E
1111	11101		Dato F
	11111		Libre
	11000		Comienzo de delimitador de secuencia, parte 1
	10001		Comienzo de delimitador de secuencia, parte 2
	01101		Fin de delimitador de secuencia, parte 1
	00111		Fin de delimitador de secuencia, parte 2
	00100		Error de transmisión
	Otro		Códigos no válidos

código de 5 bits junto con la realización NRZI. Dado que se codifican cuatro bits con un patrón de 5 bits, sólo se necesitan 16 de los 32 patrones posibles para la codificación de los datos. Los códigos seleccionados para representar los 16 bloques de datos de 4 bits son tales que existen al menos dos transiciones para cada código de grupo de 5 bits. No se permiten más de tres ceros en una fila a lo largo de uno o más grupos de código:

El esquema de codificación se puede resumir como sigue:

1. Se rechaza la realización de una simple codificación NRZ dado que no proporciona sincronismo; no aparecen transiciones en una secuencia de unos y ceros.
2. Los datos a transmitir deben ser primero codificados para asegurar la existencia de transiciones. Se elige el código 4B/5B frente a Manchester porque es más eficiente.
3. El código 4B/5B se codifica posteriormente usando NRZI, de modo que la señal diferencial resultante mejorará la fiabilidad en la recepción.
4. Los patrones de 5 bits específicamente elegidos para la codificación de los 16 patrones de datos de 4 bits se seleccionan con el fin de garantizar la no existencia de no más de tres ceros en una fila con objeto de conseguir una sincronización adecuada.

Los grupos de código no empleados para representar datos se declaran como no válidos o se les asigna un significado especial como símbolos de control. Estas asignaciones se enumeran en la Tabla 14.6. Los símbolos de no datos se encuadran en las siguientes categorías:

- **Libre:** el grupo de código libre se transmite entre secuencias de transmisión de datos. Consiste en un flujo constante de unos binarios, lo que se traduce con NRZI en un cambio continuo entre dos niveles de señal. Este patrón de relleno continuo establece y mantiene la sincronización y se usa en el protocolo CSMA/CD para indicar que el medio compartido se encuentra libre.
- **Comienzo de delimitador de secuencia:** se utiliza para delimitar el comienzo de una secuencia de transmisión de datos; consta de dos grupos de código diferentes.
- **Final de delimitador de secuencia:** empleado como fin de las secuencias de transmisión de datos normales; consta de dos grupos de código diferentes.
- **Error de transmisión:** este grupo de código se interpreta como un error de señalización. El uso normal de este indicador se establece en repetidores con el fin de propagar errores recibidos.

MLT-3

Aunque 4B/5B es efectivo para fibra óptica, no resulta tan apropiado como lo es para par trenzado. El motivo de este hecho es que la energía de la señal se concentra de manera que se producen emisiones de radiación no deseadas desde el cable. MLT-3, que se usa tanto en 100BASE-TX como en la versión de par trenzado de FDDI, está diseñado para solucionar este problema.

Se siguen los siguientes pasos:

1. **Conversión NRZI a NRZ**. La señal 4B/5B-NRZI de la 100BASE-X básica se convierte de nuevo a NRZ.
2. **Mezcla**. Se mezcla la secuencia de bits para producir una distribución de espectro más uniforme para el siguiente paso.
3. **Codificador**. La secuencia de bits mezclados se codifica usando el esquema conocido como MLT-3.
4. **Controlador**. Se transmite la codificación resultante.

El efecto del esquema MLT-3 es concentrar la mayor parte de la energía en la señal transmitida por debajo de los 30 MHz, lo que reduce las emisiones. Esto disminuye los problemas debidos a interferencias.

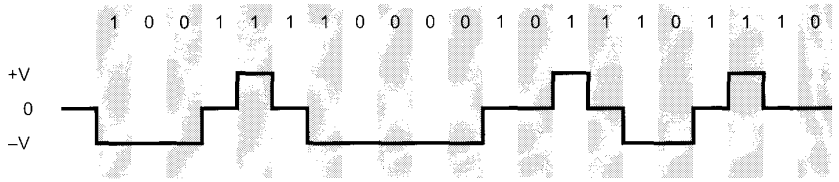


Figura 14.18. Ejemplo de codificación MLT-3.

La codificación MLT-3 produce una salida que tiene una transición para cada uno binario y que usa tres niveles: una tensión positiva (+V), una negativa (−V) y ausencia de ésta (0).

Las reglas de codificación se explican mejor con ayuda del diagrama de estados del codificador mostrado en la Figura 14.17:

1. Si el siguiente bit de entrada es cero, el siguiente valor de salida es el mismo que el valor precedente.
2. Si el siguiente bit de entrada es un uno, el siguiente valor de salida implica una transición:
   a) Si el valor de salida anterior fue +V o −V, el siguiente valor de salida es 0.
   b) Si el valor de salida precedente fue 0, el siguiente valor de salida es distinto de cero, y de signo opuesto al de la última salida distinta de cero.

En la Figura 14.18 se muestra un ejemplo. Cada vez que haya un 1 de entrada, existe una transición. Se alterna la aparición de +V y −V.

8B6T

El algoritmo de codificación 8B6T utiliza señalización ternaria. Con este tipo de señalización, cada elemento de señal puede tomar uno de tres valores posibles (tensión positiva, tensión negativa y tensión nula). Un código ternario puro es aquel en que se aprovecha la capacidad de transportar información de una señal ternaria. Sin embargo, este tipo de código no resulta atractivo por las mismas razones por las que se desestima un código binario puro (NRZ): pérdida de sincronización. A pesar de ello, existen esquemas denominados *métodos de codificación por bloques* que se aproximan a la eficiencia de un código ternario y solventan este inconveniente. En 100BASE-T4 se usa un nuevo esquema de codificación por bloques conocido como 8B6T.

En 8B6T los datos a transmitir se gestionan en bloques de 8 bits. Cada uno de estos bloques se transforma en un grupo de código de 6 símbolos ternarios. La secuencia de grupos de código se transmite

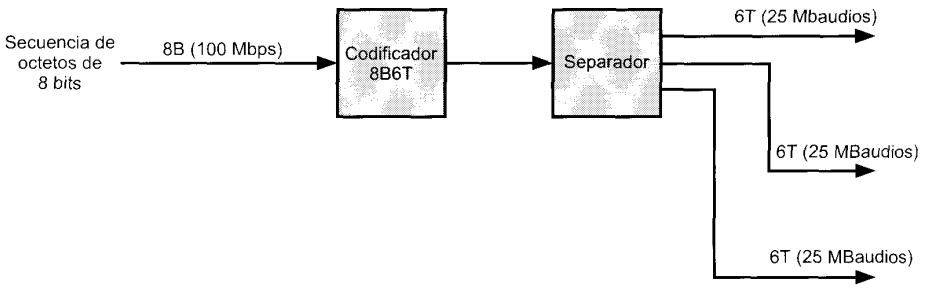


Figura 14.19. Esquema de transmisión 8B6T.

Tabla 14.7. Porción de la tabla de código 8B6T.

Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T	Octeto de datos	Grupo de código 6T
00	+ − 00 + −	10	+ 0 + − − 0	20	00 − + + −	30	+ − 00 − +
01	0 + − + − 0	11	+ + 0 − 0 −	21	− − + 00 +	31	0 + − − + 0
02	+ − 0 + − 0	12	+ 0 + − 0 −	22	+ + − 0 + −	32	+ − 0 − + 0
03	− 0 + + − 0	13	0 + + − 0 −	23	+ + − 0 − +	33	− 0 + − + 0
04	− 0 + 0 + −	14	0 + + − − 0	24	00 + 0 − +	34	− 0 + 0 − +
05	0 + − − 0 +	15	+ + 00 − −	25	00 + 0 + −	35	0 + − + 0 −
06	+ − 0 − 0 +	16	+ 0 + 0 − −	26	00 − 00 +	36	+ − 0 + 0 −
07	− 0 + − 0 +	17	0 + + 0 − −	27	− − + + + −	37	− 0 + + 0 −
08	− + 00 + −	18	0 + − 0 + −	28	− 0 − + + 0	38	− + 00 − +
09	0 − + + − 0	19	0 + − 0 − +	29	− − 0 + 0 +	39	0 − + − + 0
0A	− + 0 + − 0	1A	0 + − + + −	2A	− 0 − + 0 +	3A	− + 0 − + 0
0B	+ 0 − + − 0	1B	0 + -00 +	2B	0 − − + 0 +	3B	+ 0 − − + 0
0C	+ 0 − 0 + −	1C	0 − + 00 +	2C	0 − − + + 0	3C	+ 0 − 0 − +
0D	0 − + − 0 +	1D	0 − + + + −	2D	− − 00 + +	3D	0 − + + 0 −
0E	− + 0 − 0 +	1E	0 − + 0 − +	2E	− 0 − 0 + +	3E	− + 0 + 0
0F	+ 0 − − 0 +	1F	0 − + 0 + −	2F	0 − − 0 + +	3F	+ 0 − + 0 −

después a través de los tres canales de salida siguiendo el esquema de rotación circular (Figura 14.19). De esta forma, la velocidad de transmisión de datos en cada canal de salida es:

$$\frac{6}{8} \times 33\tfrac{1}{3} = 25 \text{ Mbaudios}$$

En la Tabla 14.7 se muestra una parte de la tabla de código 8B6T; la tabla completa transforma todos los patrones de 8 bits posibles en un único grupo de código de 6 símbolos ternarios. La transformación se elige en base a dos requisitos: sincronización y compensación de tensión continua (DC). Para sincronización, los códigos se seleccionan para maximizar el número medio de transiciones por grupo de código.

El segundo requisito consiste en mantener compensada la DC, de modo que la tensión promedia en la línea sea cero. Con este objetivo, todos los grupos de código seleccionados tienen un número igual de símbolos positivos y negativos o un superávit de un símbolo positivo. Para mantener el equilibrio se usa un algoritmo de compensación DC. Esencialmente, este algoritmo supervisa el peso acumulado de todos los grupos de código transmitidos a través de un par individual. Cada grupo de código tiene un peso 0 o 1. Para compensar, el algoritmo puede negar un grupo de código transmitido (cambia todos los símbolos + por símbolos − y todos los − por +), de forma que el peso acumulado al final de cada grupo de código es siempre 0 o 1.

8B/10B

El esquema de codificación usado en canal de fibra y en Ethernet de Gigabits es 8B/10, en el que cada 8 bits de datos se transforman en 10 bits para su transmisión. Este esquema sigue una filosofía similar al esquema 4B/5B empleado en FDDI discutido anteriormente. El esquema 8B/10B se desarrolló y patentó por IBM para su uso en su sistema interconectado ESCON a 200 Mbaudios [WIDM83]. Este esquema es más potente que el 4B/5B en términos de características de transmisión y capacidad de detección de errores.

Los diseñadores de este código enumeran las siguientes ventajas:

- Se puede implementar utilizando transceptores relativamente sencillos y fiables de bajo coste.

- Presenta una buena compensación, con mínimas desviaciones en la ocurrencia de un número igual de bits 0 y 1 a lo largo de una secuencia.
- Proporciona una buena densidad de transiciones para una fácil recuperación del sincronismo.
- Proporciona una capacidad útil de detección de errores.

El código 8B/10B es un ejemplo de código general mBnB, en el que m bits originales se transforman en n bits binarios para la transmisión. Haciendo $n > m$ se introduce redundancia en el código para proporcionar las características de transmisión deseadas.

El código 8B/10B realmente combina otros dos códigos, un código 5B/6B y otro 3B/4B. El uso de estos dos códigos es simplemente un artificio para simplificar la definición de la transformación y de la implementación: la transformación podía haberse definido directamente como un código 8B/10B. En cualquier caso, se define una transformación que traduce cada uno de los posibles bloques originales de 8 bits en un bloque de código de 10 bits. También existe una función llamada *control de disparidad*. Esencialmente, esta función hace un seguimiento del exceso de ceros frente a unos o de unos frente a ceros. La existencia de exceso en un sentido se conoce como disparidad. Si existe disparidad, y si el bloque de código actual aumenta ésta, el bloque de control de disparidad complementa el bloque de código de 10 bits. Esto tiene el efecto de eliminar la disparidad o al menos cambiarla de sentido con respecto a la actual.

APÉNDICE 14B: ANÁLISIS DE PRESTACIONES

La elección de una arquitectura LAN o MAN depende de varios factores, siendo la eficiencia uno de los más importantes. Una cuestión particular es el comportamiento (rendimiento, tiempo de respuesta) de la red ante la existencia de alta carga. En este apéndice se presenta una introducción a este tema, pudiéndose encontrar en [STAL00] una discusión más detallada del mismo.

EFECTO DEL RETARDO DE PROGRAMACIÓN Y DE LA VELOCIDAD DE TRANSMISIÓN

En el Capítulo 7 se introdujo el parámetro a, definido como

$$a = \frac{\text{Tiempo de propagación}}{\text{Tiempo de transmisión}}$$

En este contexto, nos centraremos en un enlace punto a punto, con un tiempo de propagación específico entre dos extremos y un tiempo de transmisión para una trama de tamaño fijo o promedio. Se mostró que el parámetro a se puede expresar como:

$$a = \frac{\text{Longitud del enlace de datos en bits}}{\text{Longitud de la trama en bits}}$$

Este parámetro es también importante en el contexto de redes LAN y MAN, y determina un límite superior para la utilización. Consideremos un mecanismo de acceso completamente eficiente que permita sólo una transmisión en un instante de tiempo dado. Tan pronto como finaliza una transmisión, comienza a transmitir otra estación. Además, la transmisión es sólo de datos, sin bits suplementarios. ¿Cuál es la máxima utilización de red posible? Ésta se puede expresar como la relación entre el rendimiento total de la red y su velocidad:

$$U = \frac{\text{Rendimiento}}{\text{Velocidad}} \tag{14.1}$$

Definamos ahora, como en el Capítulo 7,

R = velocidad del canal
d = distancia máxima ente cualesquiera dos estaciones
V = velocidad de propagación de la señal
L = longitud media o fija de trama

El rendimiento es el número de bits transmitidos por unidad de tiempo. Una trama contiene L bits, y la cantidad de tiempo dedicado a esta trama es el tiempo de transmisión real (L/R) más el retardo de propagación (d/V). De este modo,

$$\text{Rendimiento} = \frac{L}{d/V + L/R} \tag{14.2}$$

Pero por la definición anterior de a:

$$a = \frac{d/V}{L/R} = \frac{Rd}{LV} \tag{14.1}$$

Sustituyendo (14.2) y (14.3) en (14.1):

$$\mathcal{U} = \frac{1}{1 + a} \tag{14.4}$$

Obsérvese que esta expresión es diferente de la Ecuación (7.2) dada en el Apéndice 7A. Este hecho se debe a que la última considera un protocolo *semidúplex* (no se usan tramas de datos con incorporación de confirmación).

Por tanto, la utilización depende de a, lo que se puede comprender intuitivamente estudiando la Figura 14.20. En ella se muestra un bus de banda base con dos estaciones tan distantes como es posible

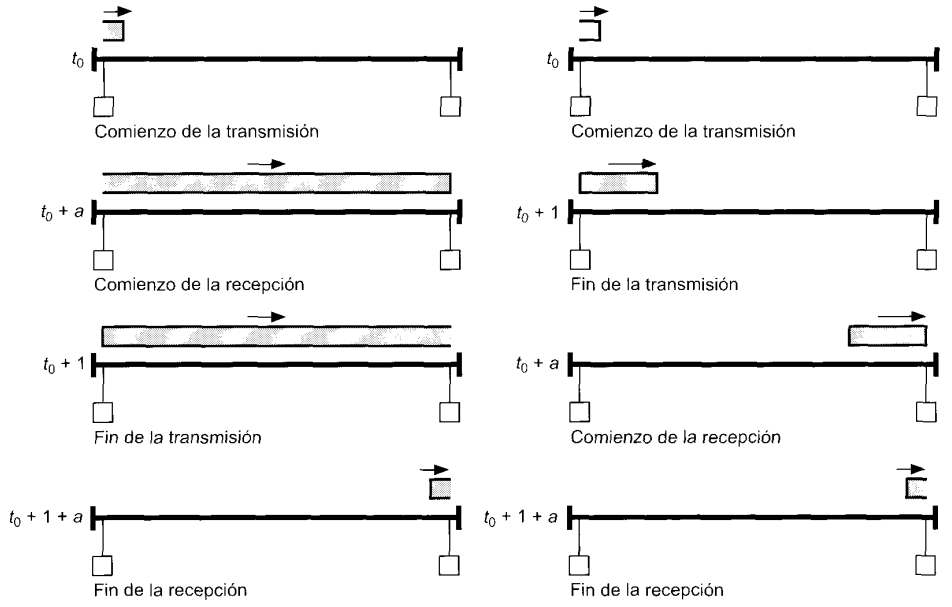


Figura 14.20. Efecto del parámetro a en la utilización en un bus de banda base.

(peor caso) que se turnan en el envío de tramas. Si normalizamos el tiempo de forma que el de transmisión de trama = 1, el tiempo de propagación = a. Para $a < 1$, la secuencia de eventos es como sigue:

1. Una estación comienza a transmitir en t_0.
2. La recepción empieza en $t_0 + a$.
3. La transmisión se completa en $t_0 + 1$.
4. La recepción finaliza en $t_0 + 1 + a$.
5. La otra estación comienza a transmitir.

Los eventos 2 y 3 se intercambian para $a > 1$. En ambos casos el tiempo total para un «turno» es $1 + a$ pero el tiempo de transmisión es sólo 1, por lo que la utilización será $1/(1 + a)$.

Lo mismo ocurre en el caso de la red en anillo de la Figura 14.21. Aquí suponemos que una estación transmite y después espera a recibir su propia transmisión antes de que otra estación pueda transmitir. Se sigue la misma secuencia de eventos que anteriormente.

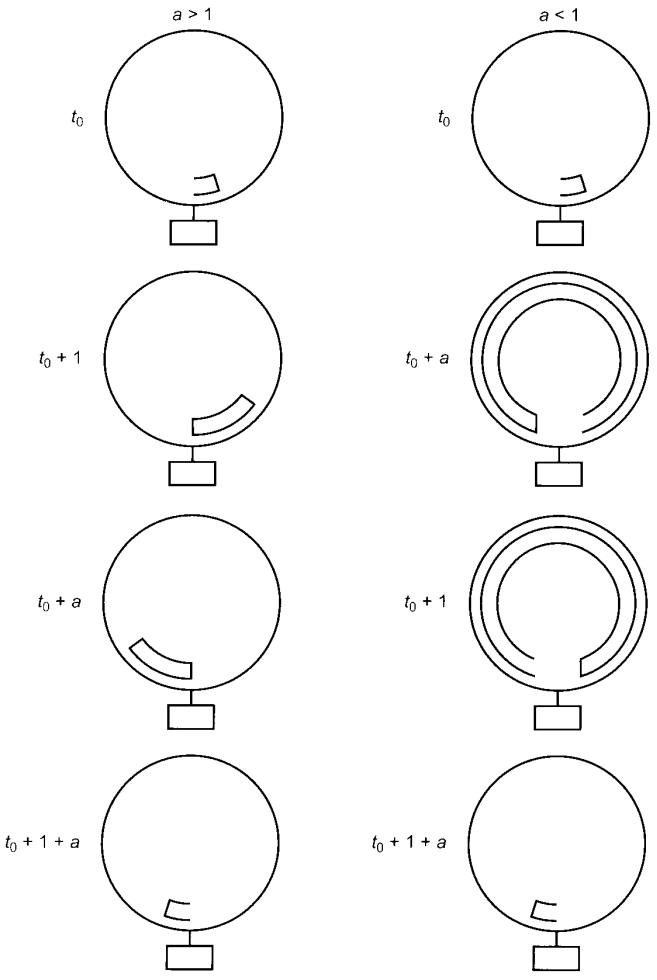


Figura 14.21. Efecto del parámetro *a* en la utilización en una red en anillo.

Tabla 14.8. Valores representativos de *a*.

Velocidad (Mbps)	Tamaño de trama (bits)	Longitud de la red (km)	*a*	1/(1 + *a*)
1	100	1	0,05	0,95
1	1.000	10	0,05	0,95
1	100	10	0,5	0,67
10	100	1	0,5	0,67
10	1.000	1	0,05	0,95
10	1.000	10	0,5	0,67
10	10.000	10	0,05	0,95
100	35.000	200	2,8	0,26
100	1.000	50	25	0,04

Los valores típicos de a se encuentran en el rango comprendido entre 0,01 y 0,1 para redes LAN y entre 0,1 y muy por encima de 1,0 para redes MAN. En la Tabla 14.8 se muestran algunos valores representativos para una topología en bus. Como se puede ver, la utilización decae para redes mayores y/o con velocidades superiores. Por esta razón desaparece la restricción de una sola trama para redes LAN como FDDI.

Por último, el análisis anterior supone un protocolo «perfecto» en el que se puede transmitir una nueva trama tan pronto como se reciba la trama anterior. En la práctica, el protocolo MAC añade bits suplementarios que hacen que empeore la utilización. Esto se demuestra en el siguiente apartado para las técnicas de paso de testigo y CSMA/CD.

MODELOS SENCILLOS DE EFICIENCIA PARA LAS TÉCNICAS DE PASO DE TESTIGO Y CSMA/CD

El objetivo de este apartado es proporcionar al lector una visión de las prestaciones relativas de los protocolos LAN más importantes —CSMA/CD, bus con paso de testigo y anillo con paso de testigo— mediante el desarrollo de dos modelos sencillos sobre prestaciones. Esperamos que este ejercicio ayude a comprender los resultados de análisis más rigurosos.

En estos modelos se supone una red local con N estaciones activas y un retardo de propagación normalizado máximo igual a a. Para simplificar el análisis se supone que cada estación está siempre lista para transmitir una trama, lo que nos permite desarrollar una expresión para la utilización máxima alcanzable (U). Aunque no se debería analizar la utilización como la única característica destacable de una red local, este parámetro es el más analizado y permite realizar comparaciones útiles acerca de prestaciones.

En primer lugar consideremos una red en anillo con paso de testigo. El tiempo consumido en el anillo se distribuye entre la transmisión de tramas de datos y el paso del testigo. Denominemos ciclo a la transmisión de una única trama de datos seguida por un testigo, y definamos:

C = tiempo promedio de un ciclo
T_1 = tiempo promedio para transmitir una trama de datos
T_2 = tiempo promedio en el paso del testigo

Debería estar claro que la razón de ciclo media es $1/C = 1/(T_1 + T_2)$. Intuitivamente,

$$U = \frac{T_1}{T_1 + T_2} \tag{14.5}$$

Es decir, el rendimiento, normalizado a la capacidad del sistema, es la fracción de tiempo consumido en la transmisión de los datos.

Centrémonos ahora en la Figura 14.21. El tiempo se normaliza de manera que el tiempo de transmisión de trama es igual a 1 y el tiempo de propagación es a. Obsérvese que el tiempo de propagación debe incluir los retardos de los repetidores. Para el caso $a < 1$ una estación transmite una trama en t_0, recibe la cabecera de su propia trama en $t_0 + a$ y completa la transmisión en $t_0 + 1$. La estación transmite entonces un testigo, lo que implica un tiempo promedio a/N hasta alcanzar la siguiente estación. Así, un ciclo dura $1 + a/N$ y el tiempo de transmisión es 1. Por tanto, $U = 1/(1 + a/N)$.

El razonamiento es ligeramente diferente para el caso $a > 1$. Una estación transmite en t_0, finaliza la transmisión en $t_0 + 1$ y recibe la cabecera de su trama en $t_0 + a$. En este momento se encuentra en condiciones de emitir un testigo, lo que implica un tiempo promedio a/N hasta alcanzar la siguiente estación. En consecuencia, el tiempo de ciclo es $a + a/N$ y $U = 1/(a(1 + 1/N))$.

En resumen,

Anillo con paso de testigo:

$$U = \begin{cases} \dfrac{1}{1 + a/N} & a < 1 \\ \dfrac{1}{a(1 + 1/N)} & a > 1 \end{cases} \tag{14.6}$$

Consideremos para CSMA/CD el tiempo del medio para organizarse en ranuras temporales de duración igual a dos veces el retardo de propagación extremo a extremo. Esto es una forma adecuada para considerar la actividad en el medio; la ranura temporal es igual al tiempo máximo, desde el inicio de la transmisión, necesario para detectar una colisión. Suponemos de nuevo que existen N estaciones activas. Es claro que si todas las estaciones tienen siempre una trama que transmitir, y lo hacen, no habrá más que colisiones en el medio. Por tanto, supongamos que cada estación limita con una probabilidad P su transmisión durante una ranura disponible.

El tiempo en el medio consta de dos tipos de intervalos. El primero es un intervalo de transmisión, de duración $1/2a$ ranuras. El segundo es un intervalo de contención, que es una secuencia de ranuras en las que se produce colisión o no existe transmisión. El rendimiento es la proporción de tiempo consumido en intervalos de transmisión [similar al razonamiento de la Ecuación (14.5)].

Para determinar la longitud promedio de un intervalo de contención comenzamos calculando A, la probabilidad de que exactamente una estación intente llevar a cabo una transmisión en una ranura y, en consecuencia, consiga el medio. Ésta es la probabilidad binomial de que cualquier estación intente transmitir y las otras no:

$$A = \binom{N}{1} P^1 (1 - P)^{N-1}$$

$$A = NP(1 - P)^{N-1}$$

Esta función alcanza un máximo sobre P cuando $P = 1/N$:

$$A = (1 - 1/N)^{N-1}$$

Estamos interesados en el máximo porque deseamos calcular el rendimiento máximo del medio. Debe quedar claro que éste se conseguirá si maximizamos la probabilidad de conseguir el medio con éxito. Esto implica que se debe forzar el cumplimiento de la siguiente regla: durante periodos de gran uso, una estación debería restringir su carga ofrecida a $1/N$. (Esto supone que cada estación conoce el valor de N. Con el fin de obtener una expresión para el máximo rendimiento posible, se considera válida esta suposición.) Por otra parte, durante periodos de tiempo de poco uso no se puede alcanzar la utilización máxima dado que la carga es demasiado pequeña; esta situación no resulta de interés para nuestros objetivos actuales.

Ahora podemos estimar la longitud media de un intervalo de contención, w, en ranuras:

$$\mathrm{E}[w] = \sum_{i=1}^{\infty} i \times \Pr\left[\begin{array}{l}\text{secuencia con } i \text{ ranuras con una colisión o no}\\ \text{transmisión, seguida por una ranura con una}\\ \text{transmisión}\end{array}\right]$$

$$= \sum_{i=1}^{\infty} i(1-A)^i A$$

La sumatoria converge a

$$\mathrm{E}[w] = \frac{1-A}{A}$$

Ahora se puede determinar la utilización máxima, que no es más que la longitud del intervalo de transmisión con respecto a un ciclo que consta del intervalo de transmisión y de otro de contención:

$$\textbf{CSMA/CD:} \qquad \mathcal{U} = \frac{1/2a}{1/2a + (1-A)/A} = \frac{1}{1 + 2a(1-A)/A} \tag{14.7}$$

En la Figura 14.22 se muestra el rendimiento normalizado como función de a para varios valores de N para las técnicas de paso de testigo y CSMA/CD. En ambos protocolos el rendimiento decrece a

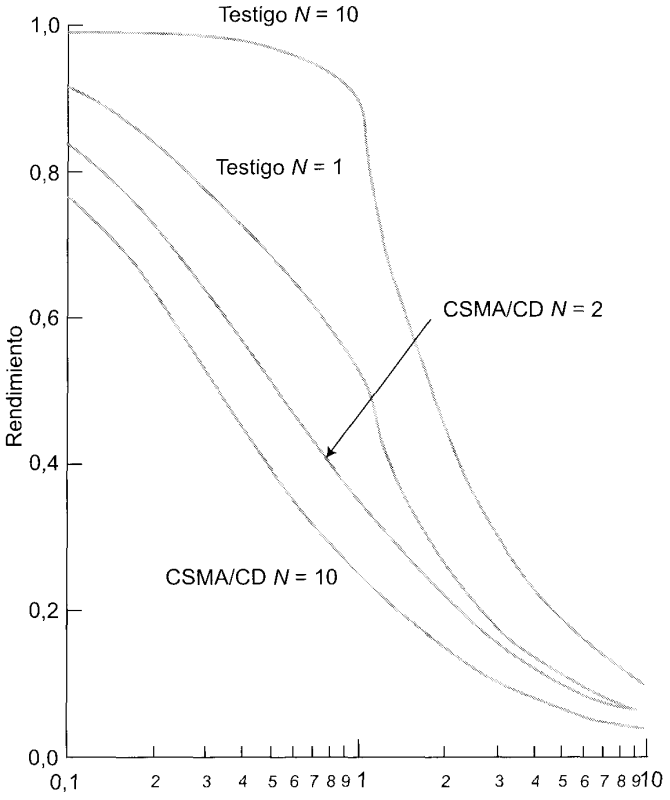


Figura 14.22. Rendimiento en función de a para las técnicas de paso de testigo y CSMA/CD.

medida que aumenta el parámetro a. Este resultado era de esperar, pero la gran diferencia entre los dos protocolos se muestra en la Figura 14.23, que representa el rendimiento en función de N. Las prestaciones de la técnica de paso de testigo mejoran en función de N, ya que se consume menos tiempo en el paso del testigo. Por el contrario, las prestaciones de la técnica CSMA/CD decrecen debido al incremento en la probabilidad de colisión o no transmisión.

Es interesante observar el comportamiento asintótico de U a medida que aumenta N.

Testigo:

$$\lim_{N \to \infty} U = \begin{cases} 1 & a < 1 \\ 1/a & a > 1 \end{cases} \tag{14.8}$$

Para CSMA/CD debemos saber que $\lim (1 - 1/N)^{N-1} = 1/e$. Por tanto, tenemos que:

CSMA/CD:

$$\lim_{N \to \infty} U = \frac{1}{1 + 3{,}44a} \tag{14.9}$$

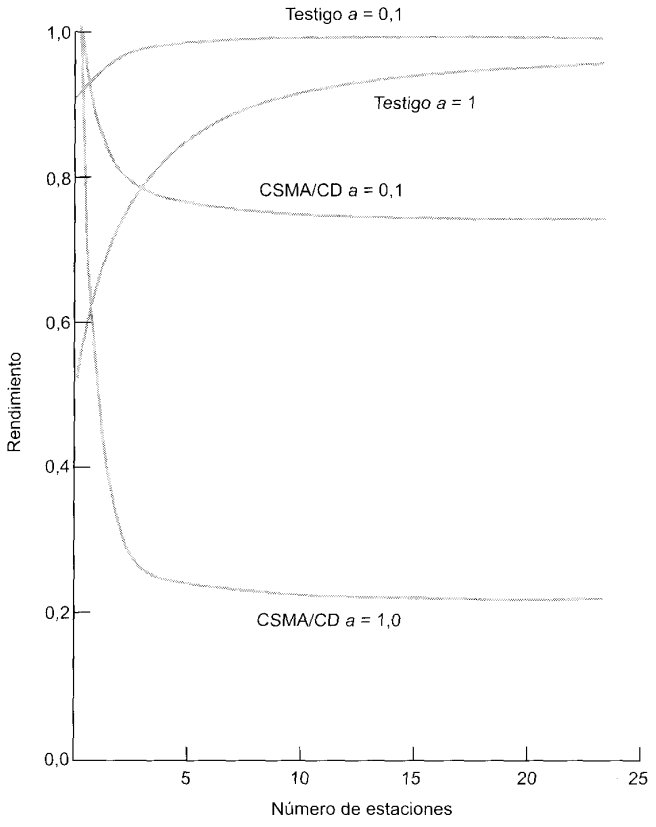


Figura 14.23. Rendimiento en función de N para las técnicas de paso de testigo y CSMA/CD.

PARTE V

PROTOCOLOS DE INTERCONEXIÓN

CUESTIONES A TRATAR EN LA PARTE QUINTA

Hasta ahora hemos tratado con tecnologías y técnicas utilizadas para intercambiar datos entre dos dispositivos. La Parte II trataba el caso en el que los dos dispositivos comparten un enlace de transmisión. Las Partes III y IV estaban relacionadas con el caso en el que una red de comunicación proporciona una capacidad de transmisión compartida para múltiples sistemas finales conectados.

En un sistema de procesamiento de datos distribuido se necesita mucho más. Los sistemas de procesamiento de datos (estaciones de trabajo, PC, servidores, grandes computadores) deben implementar un conjunto de funciones que les permitirán llevar a cabo algunas tareas de forma cooperativa. Este conjunto de funciones se organiza en una arquitectura de comunicaciones e implica la utilización de un conjunto de protocolos en capas, incluyendo protocolos de interconexión, transporte y de la capa de aplicación.

Antes de proceder con la Parte V, se aconseja al lector que revise el Capítulo 2, que introduce el concepto de arquitectura de protocolos y discute los elementos clave de un protocolo.

ESQUEMA DE LA PARTE V

CAPÍTULO 15. PROTOCOLOS DE INTERCONEXIÓN DE REDES

Con la proliferación de las redes, las facilidades de interconexión han llegado a ser componentes esenciales del diseño de red. El Capítulo 15 empieza con un examen de las necesidades de una facilidad de interconexión y los diversos enfoques de diseño que se pueden tomar para satisfacer estas necesidades. El resto del capítulo trata la utilización de los dispositivos de encaminamiento para la interconexión. Se examinan el protocolo de Internet (IP) y el nuevo IPv6. Finalmente, se explora la cuestión de la multidifusión a través de un conjunto de redes.

CAPÍTULO 16. FUNCIONAMIENTO DE LA INTERCONEXIÓN DE REDES

El tráfico que Internet y las redes privadas deben transportar lleva a un crecimiento y cambio continuos. La demanda generada por las aplicaciones tradicionales basadas en datos, como el correo electrónico

los grupos de noticias Usenet, la transferencia de ficheros y la conexión remota, es todo un reto para el desarrollo de estos sistemas. Pero el factor impulsor es la extraordinaria carga que supone la WWW (World Wide Web), que demanda respuestas en tiempo real, y el uso creciente de la voz, imágenes e incluso vídeo a través de arquitecturas de interconexión de redes.

Estos esquemas de interconexión están basados esencialmente en tecnologías de conmutación de paquetes por datagramas con dispositivos de encaminamiento funcionando como conmutadores. Estas tecnologías no se diseñaron para tratar voz o vídeo y se están adaptando para satisfacer las demandas que se le imponen. Aunque muchos prevén el reemplazo de este conglomerado de LAN basadas en Ethernet, WAN basadas en paquetes y dispositivos de encaminamiento basados en datagramas IP por un servicio de transporte ATM sin fisuras desde el puesto de trabajo hasta la red central, ese día parece lejano. Mientras tanto, la función de interconexión y de encaminamiento de estas redes debe de adecuarse para satisfacer las necesidades crecientes de esta carga.

El Capítulo 16 examina algunas de las herramientas y técnicas diseñadas para satisfacer las nuevas demandas, empezando con una discusión sobre las técnicas de encaminamiento, que pueden ayudar a suavizar una carga repentina imprevista. El resto del capítulo analiza los esfuerzos recientes para proporcionar un nivel dado de calidad de servicio (QoS) a varias aplicaciones. Los elementos más importantes de este nuevo enfoque son los servicios integrados, los servicios diferenciados y el protocolo de reserva RSVP.

CAPÍTULO 17. PROTOCOLO DE TRANSPORTE

El protocolo de transporte es la piedra angular del concepto global de una arquitectura de comunicaciones de computadores. También puede ser uno de los protocolos más complejos. El Capítulo 17 examina en detalle los mecanismos del protocolo de transporte y luego discute dos ejemplos importantes, TCP y UDP. La mayor parte del capítulo está dedicada a un análisis del conjunto complejo de mecanismos de TCP y a los esquemas de control de congestión en TCP.

CAPÍTULO 18. SEGURIDAD EN REDES

La seguridad en red ha llegado a ser cada vez más importante con el crecimiento del número e importancia de las redes. El Capítulo 18 proporciona una visión general de las técnicas y servicios de seguridad. El capítulo comienza con una visión global a las técnicas de cifrado para asegurar la confidencialidad, que incluye la utilización del cifrado convencional y de clave pública. Después se explora el área de la autentificación y de las firmas digitales. Se examinan los dos algoritmos más importantes de encriptado, DES y RSA, así como SHA-1, una función mezcla de un solo sentido importante para un determinado número de aplicaciones de seguridad. Finalmente, el capítulo discute el conjunto de estándares de seguridad en IP.

CAPÍTULO 19. APLICACIONES DISTRIBUIDAS

El propósito de una arquitectura de comunicaciones es dar soporte a aplicaciones distribuidas. El Capítulo 19 examina tres de las más importantes de estas aplicaciones; en cada caso, se discuten los principios generales, seguido de un ejemplo específico. Las aplicaciones discutidas son, gestión de red, los intercambios de la WWW y el correo electrónico. Los ejemplos correspondientes son SNMP, HTTP y SMTP y MIME. Antes de analizar estos ejemplos, el capítulo empieza con un examen de la Notación Sintáctica Abstracta Uno (ASN.1), que es el lenguaje estandarizado para definir aplicaciones distribuidas.

CAPÍTULO 15

Protocolos de interconexión de redes

- Un conjunto de redes consta de múltiples redes separadas que están interconectadas por dispositivos de encaminamiento. Los datos se intercambian en paquetes entre un sistema origen y un destino a través de un camino que implica a múltiples redes y dispositivos de encaminamiento. Normalmente, se utiliza un modo de operación no orientado a conexión o datagrama. Un dispositivo de encaminamiento acepta datagramas y los retransmite hacia su destino y es responsable de determinar la ruta, del mismo modo en el que actúa un nodo de conmutación de paquetes.
- El protocolo más comúnmente utilizado para la interconexión de redes es el Protocolo de Internet (IP, Internet Protocol). IP incorpora una cabecera a los datos de la capa inmediatamente superior (por ejemplo, TCP) para formar un datagrama IP. La cabecera incluye las direcciones origen y destino, información utilizada para la fragmentación y el reensamblado, un campo de tiempo-de-vida, un campo de tipo de servicio y una suma de comprobación.
- Se ha definido un protocolo IP de nueva generación, conocido como IPv6. IPv6 proporciona campos de dirección más grandes y una mayor funcionalidad que el actual IP.
- Adicionalmente al encaminamiento directo de un datagrama desde un origen a un único destino, otra capacidad importante de un conjunto de redes es la multidifusión, lo cual permite distribuir un datagrama desde una única fuente a múltiples destinos. Los dispositivos de encaminamiento implicados en esta transmisión deben designar un conjunto de dispositivos de encaminamiento para la entrega de forma que minimice el número de veces que hay que duplicar el datagrama en la ruta desde el origen único a los múltiples destinos.

Las redes de conmutación de paquetes y las de difusión de paquetes crecieron ante la necesidad de permitir a los usuarios de computadores tener acceso a los recursos existentes más allá de los que se disponen en un único sistema. De una forma similar, los recursos de una única red son a menudo insuficientes para las necesidades de los usuarios. Ya que las redes que podrían ser de interés exhiben muchas diferencias, no es práctico tratar de agruparlas todas en una única red. Más bien, lo que se necesita es la habilidad de interconectar varias redes para que se puedan comunicar dos estaciones cualesquiera de cualquier red.

La Tabla 15.1 muestra algunos de los términos más comúnmente utilizados y relacionados con la interconexión entre redes (internetworking). Un conjunto de redes interconectadas, desde el punto de vista del usuario, puede aparecer simplemente como una red más grande. Sin embargo, si cada una de las redes constituyentes retiene su identidad y se necesitan mecanismos especiales para la comunicación a través de múltiples redes, entonces a la configuración entera se le conoce como **conjunto de redes** (o **una internet**).

Cada red constituyente de una internet permite la comunicación entre los dispositivos conectados a esa red; estos dispositivos se conocen como **sistemas finales** (ESs, End Systems). Además, las redes se conectan por dispositivos denominados en los documentos ISO como **sistemas intermedios** (ISs, Intermediate Systems). Los ISs proporcionan caminos de comunicación y realizan las funciones de retransmisión y encaminamiento necesarias para que los datos se puedan intercambiar entre los dispositivos conectados en las diferentes redes de la internet.

Existen dos tipos de IS, los puentes y los dispositivos de encaminamiento que son dos tipos de IS de particular interés. Las diferencias entre ellos se derivan de los protocolos utilizados para la lógica de la interconexión entre las redes. En esencia, un **puente** opera en la capa 2 de la arquitectura de 7 capas del modelo para la Interconexión de Sistemas Abiertos (OSI) y actúa como un retransmisor de tramas entre redes parecidas; los puentes ya se examinaron en detalle en el Capítulo 13. Un **dispositivo de encaminamiento** opera en la capa 3 de la arquitectura OSI y encamina los paquetes entre redes potencialmente diferentes. Tanto los puentes como los dispositivos de encaminamiento suponen que se usa el mismo protocolo en la capa superior.

Tabla 15.1. Términos de interconexión entre redes.

Red de comunicación
Un sistema que proporciona un servicio de transferencia de datos entre estaciones conectadas a la red.

Internet
Una colección de redes de comunicación interconectadas por puentes o dispositivos de encaminamiento.

Intranet
Una *internet* corporativa que proporciona las aplicaciones claves de Internet, especialmente el *«world wide web»*. Una intranet opera dentro de una organización por motivos internos y puede existir aisladamente, como una internet auto-contenida o puede tener enlaces a Internet.

Sistema Final (ES)
Un dispositivo conectado a una de las redes de una *internet* que se utiliza para apoyar a las aplicaciones o servicios del usuario final.

Sistema intermedio (IS)
Un dispositivo utilizado para conectar dos redes y permitir la comunicación entre sistemas finales conectados a diferentes redes.

Puente («bridge»)
Un IS utilizado para conectar dos redes LAN que utilizan el mismo protocolo LAN. El puente actúa como un filtro de direcciones, recogiendo paquetes de una LAN que van dirigidos a un destino en otra LAN y pasándolos hacia adelante. El puente no modifica el contenido del paquete y ni incorpora nada al mismo. El puente opera en la capa 2 del modelo OSI.

Dispositivo de encaminamiento («router»)
Un IS utilizado para conectar dos redes que pueden o no ser similares. El dispositivo de encaminamiento utiliza un protocolo de *internet* presente en cada dispositivo de encaminamiento y en cada computador de la red. El dispositivo de encaminamiento opera en la capa 3 del modelo OSI.

Comenzaremos nuestro estudio de la interconexión de redes con una discusión de los principios subyacentes en varios enfoques de interconexión entre redes. Después examinaremos la técnica más importante para la interconexión entre redes: el dispositivo de encaminamiento no orientado a conexión. Después se describe el protocolo para interconexión más extendido, llamado sencillamente Protocolo Internet (del inglés Internet Protocol, IP). A continuación, se examina el protocolo de interconexión normalizado más reciente, conocido como IPv6. Finalmente, se exploran las cuestiones relativas a la Multidifusión IP.

La Figura 15.1 destaca la posición de los protocolos discutidos en este capítulo dentro de la arquitectura de protocolos TCP/IP.

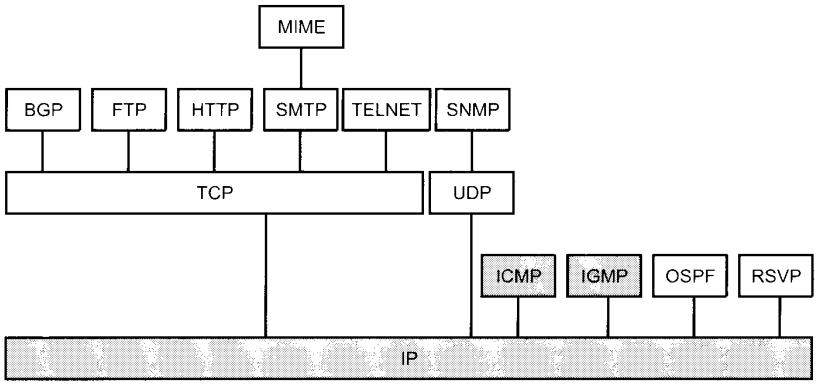


Figura 15.1. Protocolos de interconexión entre redes en contexto.

15.1. PRINCIPIOS DE LA INTERCONEXIÓN ENTRE REDES

REQUISITOS

Los requisitos globales para el sistema de interconexión entre redes son los que siguen a continuación:

1. Proporcionar una enlace entre redes. Como mínimo, se necesita una conexión física y de control del enlace.
2. Proporcionar el encaminamiento y entrega de los datos entre procesos en diferentes redes.
3. Proporcionar un servicio de contabilidad que realice un seguimiento de la utilización de las diferentes redes y dispositivos de encaminamiento y mantenga información de estado.
4. Proporcionar los servicios mencionados de forma que no se requiera la modificación de la arquitectura de red de cualquiera de las redes interconectadas. Esto significa que el sistema de interconexión entre redes se debe acomodar a las varias diferencias existentes entre las distintas redes. Algunas de estas diferencias son:
   - **Diferentes esquemas de direccionamiento:** las redes pueden usar diferentes nombres y direcciones de los puntos finales y diferentes esquemas de mantenimiento del directorio. Por tanto, se debe proporcionar un esquema de direccionamiento de red global así como un servicio de directorio.
   - **Diferente tamaño máximo de paquete:** puede que se necesite romper un paquete en unidades más pequeñas al pasar a otra red. Este proceso se denomina segmentación o fragmentación.
   - **Diferentes mecanismos de acceso a la red:** el mecanismo de acceso de la estación a la red podría ser diferente para estaciones de redes diferentes.
   - **Diferentes valores de expiración de los temporizadores**: normalmente, un servicio de transporte orientado a conexión esperará la confirmación de una recepción correcta de datos hasta que un temporizador expira, en cuyo caso retransmitirá su bloque de datos. En general, se requieren valores grandes del temporizador para realizar una entrega satisfactoria a través de redes múltiples. Los procedimientos que establecen los valores en la interconexión de redes deben permitir una transmisión satisfactoria que evite retransmisiones innecesarias.
   - **Recuperación de errores:** los procedimientos deben proporcionar un servicio que va desde no suministrar recuperación de errores hasta un servicio extremo-a-extremo (dentro de la red) seguro. El servicio de interconexión de redes no debería depender o no tendría que ser interferido por la naturaleza de la capacidad de recuperación de errores de las redes individuales.
   - **Informes de estado:** las diferentes redes dan informes de estado y de rendimiento de una forma diferente. Debe ser posible que el sistema de interconexión proporcione información de la actividad de interconexión a los procesos interesados y autorizados.
   - **Técnicas de encaminamiento:** el encaminamiento dentro de la red puede depender de la detección de fallos y de las técnicas de control de congestión particulares de cada red. El sistema de interconexión entre redes debe ser capaz de coordinar estas técnicas para encaminar los datos adaptativamente entre las estaciones de las diferentes redes.
   - **Control de acceso del usuario:** cada red tendrá su propia técnica de control de acceso de los usuarios (autorización para usar la red). Estas técnicas se deben solicitar por el sistema de interconexión según se necesite. Además, se podría requerir una técnica diferente de control de acceso a la interconexión entre redes.
   - **Conexión, sin conexión:** las redes individuales pueden proporcionar un servicio orientado a conexión (por ejemplo, circuitos virtuales) o no orientados a conexión (datagramas). Es de-

seable que el servicio entre redes no dependa de la naturaleza del servicio de conexión de las redes individuales.

Algunos de estos requisitos los satisface el protocolo de Internet (IP). Otros requieren un control adicional y software de aplicación, como se verá en este capítulo y en el siguiente.

ENFOQUE SOBRE LA ARQUITECTURA

Una característica clave en una arquitectura de interconexión de redes es si el modo de operación es orientado a conexión o no orientado a conexión.

Funcionamiento orientado a conexión

En el modo de operación orientado a conexión, se supone que cada red proporciona un servicio en la forma de conexión. Esto es, se establece una conexión lógica de red (por ejemplo, circuito virtual) entre cualquier par de DTE conectados a la misma red. Con esta idea en mente, podemos resumir la opción de operación con conexión como sigue:

1. Los IS (sistemas intermedios) se utilizan para conectar dos o más subredes; cada IS aparece como un DTE a cada una de las redes a las que está conectado.
2. Cuando el DTE A quiere intercambiar datos con el DTE B, se establece una conexión lógica entre ellos. Esta conexión lógica consiste en la concatenación de una secuencia lógica de conexiones a través de subredes. Esta secuencia es tal que forma un camino desde el DTE A al DTE B.
3. Las conexiones lógicas individuales dentro de una red están realizadas por varios IS. Cualquier tráfico que llega a un IS en una conexión lógica se retransmite en una segunda conexión lógica y viceversa.

No siempre se da el caso de que las redes constituyentes de un conjunto de redes proporcionen un servicio orientado a conexión. Por ejemplo, una red de área local IEEE 802 o FDDI proporcionan un servicio definido por el control lógico del enlace (LLC). Dos de las opciones de LLC proporcionan servicios no orientados a conexión. Por lo tanto, en realidad, estas redes tiene una forma de transmisión estilo datagrama. Así, en este caso, el servicio de la red se debe realzar. Un ejemplo de cómo se podría realizar ésto es que los IS implementen X.25 encima de LLC a través de la LAN.

Un dispositivo de encaminamiento orientado a conexión realiza la siguientes funciones claves:

- **Retransmisión:** las unidades de datos que llegan de una red vía el protocolo de la capa de red se retransmiten a otra red. El tráfico se conduce a través de conexiones lógicas que están unidas por los dispositivos de encaminamiento.
- **Encaminamiento:** cuando se va a establecer una conexión lógica extremo-a-extremo, consistente en una secuencia de conexiones lógicas, cada dispositivo de encaminamiento en la secuencia debe realizar una decisión de encaminamiento que determina el siguiente salto en la secuencia.

Así, en la capa 3, se realiza la operación de retransmisión. Se supone que todos los sistemas finales comparten protocolos comunes en la capa 4 (transporte) y superiores, para obtener una comunicación extremo-a-extremo satisfactoria.

Un ejemplo del enfoque orientado a conexión es el estándar X.75, utilizado para interconectar redes de conmutación de paquetes X.25. En la práctica, el enfoque orientado a conexión no se utiliza normalmente. El enfoque dominante es el no orientado a conexión, utilizando IP.

Funcionamiento sin conexión

Mientras que el modo de funcionamiento con conexión se corresponde con un mecanismo de circuito virtual de una red de conmutación de paquetes (Figura 10.5a), el modo de operación sin conexión se

corresponde con un mecanismo de datagramas de una red de conmutación de paquetes (Figura 10.5b). Cada unidad de datos del protocolo de red se trata independientemente y se encamina desde el DTE origen al DTE destino a través de una serie de dispositivos de encaminamiento y redes. Para cada unidad de datos transmitida por A, A realiza una decisión sobre qué dispositivo de encaminamiento debería recibir la unidad de datos. La unidad de datos salta a través del conjunto de redes de un dispositivo de encaminamiento al siguiente hasta que alcanza la subred destino. En cada dispositivo de encaminamiento se hace una decisión de encaminamiento (independientemente para cada unidad de datos) relativa al siguiente salto. Así, diferentes unidades de datos pueden viajar por diferentes rutas entre el DTE origen y destino.

Todos los DTE y todos los dispositivos de encaminamiento comparten un protocolo de la capa de red común conocido genéricamente como protocolo Internet. Dentro del proyecto internet de DARPA se desarrolló un protocolo Internet (IP) inicial y publicado como RFC 791, y ha llegado a ser un estándar Internet. Debajo de un protocolo de conexión de redes, existe la necesidad de tener un protocolo para acceder a la red particular. Así, normalmente hay dos protocolos en la capa de red operando en cada DTE y dispositivo de encaminamiento: una subcapa superior que proporciona la función de interconexión, y una capa inferior que proporciona el acceso a la red.

15.2. INTERCONEXIÓN ENTRE REDES SIN CONEXIÓN

En esta sección, se examinan las funciones esenciales de un protocolo de interconexión. Por comodidad, nos vamos a referir concretamente al Estándar Internet IP, pero se debe entender que la narración de esta sección se aplica a cualquier protocolo de interconexión no orientado a conexión, como es el caso de IPv6 y el protocolo de interconexión no orientado a conexión definido por ISO.

FUNCIONAMIENTO DE UN ESQUEMA DE INTERCONEXIÓN NO ORIENTADO A CONEXIÓN

IP proporciona un servicio sin conexión, o datagrama, entre sistemas finales. La opción sin conexión tiene una serie de ventajas. Éstas son:

- Un sistema de interconexión sin conexión es flexible. Puede trabajar con una gran variedad de redes, algunas de las cuales serán también sin conexión. En esencia, IP requiere muy poco de las redes sobre las que actúa.
- Un servicio de interconexión sin conexión se puede hacer bastante robusto. Se puede utilizar el mismo argumento realizado para un servicio de red datagrama frente a un servicio con circuitos virtuales. Para una discusión en profundidad, se recomienda al lector la Sección 10.1.
- Un servicio de interconexión sin conexión es el mejor servicio para un protocolo de transporte sin conexión, ya que no impone información suplementaria innecesaria.

La Figura 15.2 muestra un ejemplo típico en el que se usa IP, en el que dos LAN se interconectan mediante una red WAN de conmutación de paquetes X.25. La figura muestra el funcionamiento del protocolo de interconexión para los datos intercambiados entre el computador A en una LAN (red 1) y el computador B en otra LAN (red 2) a través de una WAN. La figura muestra el formato de la unidad de datos en cada etapa. Los sistemas finales y los dispositivos de encaminamiento deben todos compartir un protocolo de interconexión común. Además, los sistemas finales deben compartir el mismo protocolo que hay encima de IP. Los dispositivos de encaminamiento intermedios sólo necesitan implementar hasta el protocolo IP.

El protocolo IP en A recibe bloques de datos desde las capas superiores del software en A para que los envíe a B. IP incorpora una cabecera especificando, entre otras cosas, la dirección global Internet de B. Esa dirección, lógicamente, consta de dos partes: un identificador de la red y un identificador del sistema final. La combinación de la cabecera IP y los datos de la capa superior se llama una unidad de

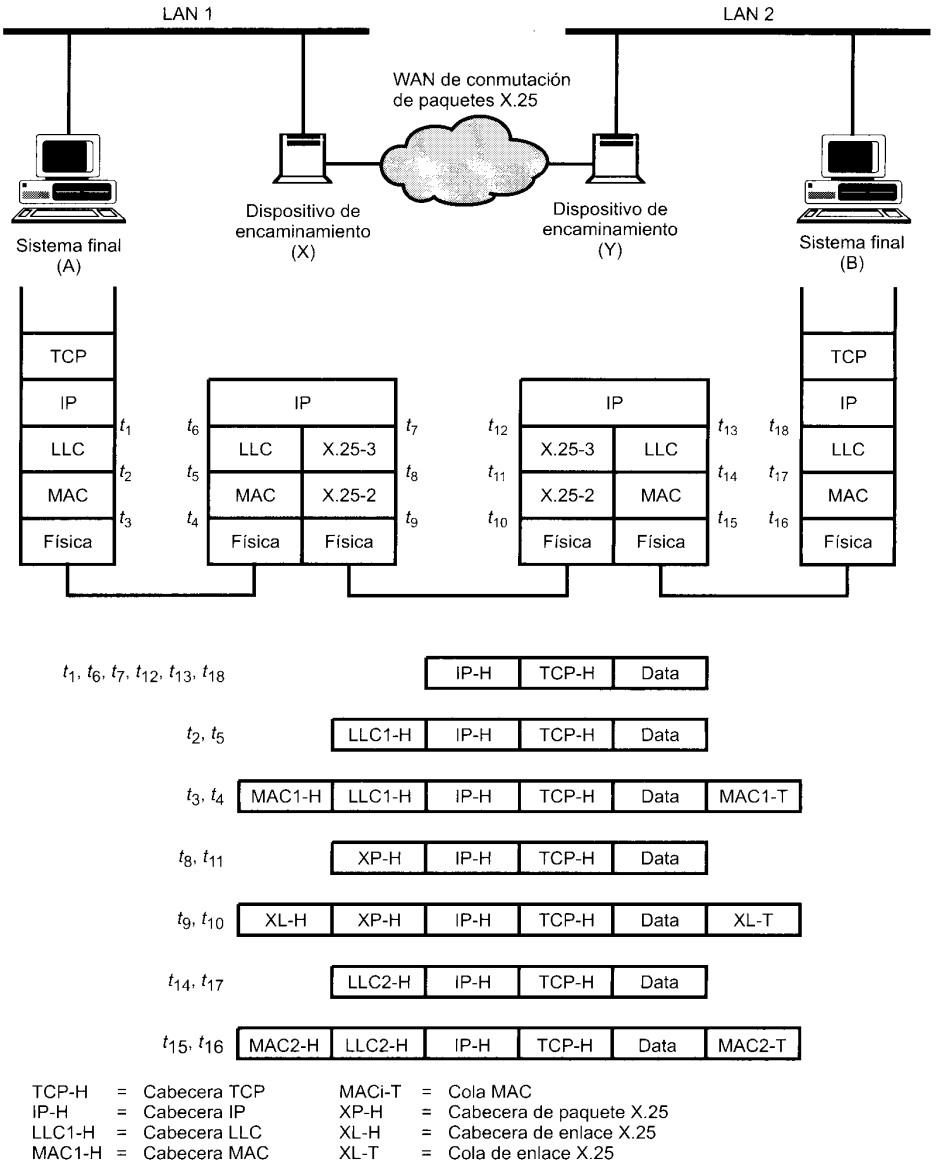


Figura 15.2. Funcionamiento del protocolo Internet.

datos del protocolo de interconexión (PDU), o simplemente un datagrama (véase Figura 2.11). El datagrama es posteriormente encapsulado con el protocolo de la LAN y enviado al dispositivo de encaminamiento, que elimina la cabecera LAN para leer la cabecera IP. El dispositivo de encaminamiento, entonces, encapsula el datagrama con los campos del protocolo X.25 y lo transmite a través de la WAN a otro dispositivo de encaminamiento. Este dispositivo de encaminamiento elimina los campos de X.25 y recupera el datagrama, al cual se le incorpora los campos LAN apropiados de la LAN 2 y se envía a B.

Examinemos con más detalle este ejemplo. El sistema final A tiene que enviar un datagrama al sistema final B; el datagrama incluye la dirección internet de B. El módulo IP en A reconoce que el destino (B) está en otra subred. Por lo tanto, el primer paso es enviar los datos a un dispositivo de encaminamiento, en este caso al dispositivo de encaminamiento X. Para hacer esto, IP pasa el datagrama a la capa inferior (en este caso la capa LLC) con instrucciones para que se envíe al dispositivo de encaminamiento X. LLC pasa esta información a la capa MAC, que inserta la dirección de la capa MAC del dispositivo de encaminamiento en la cabecera MAC. Así, el bloque de datos transmitido en la LAN 1 incluye datos de una aplicación que está por encima de TCP, más la cabecera TCP, una cabecera IP, la cabecera LLC y la cabecera y cola MAC (tiempo t_3 en la Figura 15.2).

A continuación, el paquete viaja a través de la red 1 hasta el dispositivo de encaminamiento X. El dispositivo de encaminamiento elimina los campos MAC y LLC y analiza el campo IP para determinar el destino último de los datos, en este caso B. El dispositivo de encaminamiento debe tomar ahora una decisión de encaminamiento. Existen tres posibilidades:

1. La estación destino B está conectada a una de las redes a las que el dispositivo de encaminamiento está conectado. En este caso, el dispositivo de encaminamiento envía el datagrama directamente al destino.
2. Se tienen que atravesar uno o más dispositivos de encaminamiento para alcanzar el destino. En este caso, de debe tomar una decisión de encaminamiento: ¿A qué dispositivo de encaminamiento se debe enviar el datagrama? En ambos casos 1 y 2, el módulo IP en el dispositivo de encaminamiento envía el datagrama a la capa inferior con la dirección de la red destino. Hay que indicar que aquí se está hablando de una dirección de una capa inferior referente a esta red.
3. El dispositivo de encaminamiento no conoce la dirección destino. En este caso, el dispositivo de encaminamiento devuelve un mensaje de error a la fuente del datagrama.

En este ejemplo, los datos deben pasar a través del dispositivo de encaminamiento Y antes de alcanzar su destino. Por lo tanto, el dispositivo de encaminamiento X construye un nuevo paquete incorporando a la unidad de datos IP la cabecera X.25, conteniendo la dirección del dispositivo de encaminamiento Y. Cuando este paquete llega al dispositivo de encaminamiento Y, se elimina la cabecera. El dispositivo de encaminamiento determina que esta unidad de datos IP va dirigida a B, que está conectado directamente a la red a la cual está conectado el dispositivo de encaminamiento. Éste, por tanto, construye una trama con dirección destino la de B y la envía en la LAN 2. Los datos finalmente llegan a B, donde se eliminan las cabeceras LAN e IP.

En cada dispositivo de encaminamiento, antes de que se reenvíen los datos, se podría necesitar segmentar la unidad de datos para acomodarlos a la red de salida suponiendo que en ésta hay una limitación menor en el tamaño máximo del paquete. Cada nueva unidad de datos se integra en un paquete de la capa inferior y se coloca en cola para su transmisión. El dispositivo de encaminamiento podría también limitar la longitud de sus colas para cada red a la que está conectado para evitar que una red lenta perjudique a una rápida. Una vez que se alcanza el límite de la cola, las unidades de datos adicionales se descartan.

El proceso descrito antes continúa a través de tantos dispositivos de encaminamiento como necesite la unidad de datos para alcanzar su destino. Como con un dispositivo de encaminamiento, el sistema final destino recupera la unidad de datos IP a partir de los segmentos obtenidos de la red. Si ha habido segmentación, el módulo IP en el sistema final destino almacena temporalmente los datos que llegan hasta que el mensaje original puede ser totalmente reensamblado. Después, este bloque de datos se pasa a la capa superior del sistema final.

Este servicio ofrecido por un protocolo de interconexión es del tipo no seguro. Esto es, el protocolo de interconexión no garantiza que todos los datos se entreguen al destino o que los datos que se entregan lleguen en el orden adecuado. Es responsabilidad de la capa superior (por ejemplo, TCP) tratar los errores que ocurran. Esta técnica proporciona un alto grado de flexibilidad.

Con esta forma de abordar el protocolo de interconexión, cada unidad de datos se pasa de dispositivo de encaminamiento a dispositivo de encaminamiento para ir de la fuente al destino. Ya que la entre-

ga no se garantiza, no hay ningún requisito particular de seguridad en cualquiera de las redes. Así, el protocolo funcionará con cualquier combinación de tipos de red. Ya que la secuencia de entrega no está garantizada, las unidades de datos sucesivas pueden seguir diferentes caminos a través del conjunto de redes. Esto le permite al protocolo reaccionar frente a la congestión y los fallos en las redes cambiando las rutas.

CUESTIONES DE DISEÑO

Con este breve esbozo del funcionamiento de una interconexión entre redes controlada por IP, podemos ahora volver atrás y examinar algunas cuestiones de diseño con un mayor detalle.

- Encaminamiento.
- Tiempo de vida de los datagramas.
- Segmentación y reensamblado.
- Control de errores.
- Control de flujo.

Conforme desarrollemos esta discusión, el lector notará muchas similitudes con las cuestiones de diseño y las técnicas relevantes en una red de conmutación de paquetes. Para ver la razón de esto, considere la Figura 15.3 que compara una arquitectura de interconexión con una arquitectura de red de conmutación de paquetes. Los dispositivos de encaminamiento (R1, R2, R3) en el conjunto de redes corresponden a los nodos de conmutación de paquetes (P1, P2, P3) en la red, y las redes (N1, N2, N3) en el conjunto de redes se corresponde con los enlaces de transmisión (T1, T2, T3) en las redes. Los dispositivos de encaminamiento realizan esencialmente las mismas funciones que los nodos de conmutación de paquetes, y usan las redes intermedias de una forma análoga a los enlaces de transmisión.

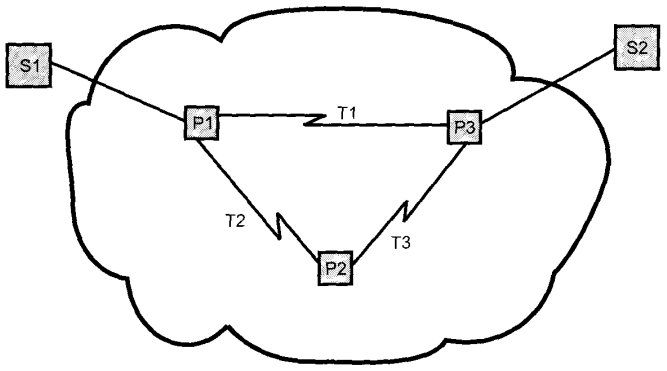
Encaminamiento

El encaminamiento se efectúa por medio del mantenimiento de una tabla de encaminamiento en cada dispositivo de encaminamiento y en cada sistema final que da, para cada red posible de destino, el siguiente dispositivo de encaminamiento al que se deberá enviar el datagrama internet.

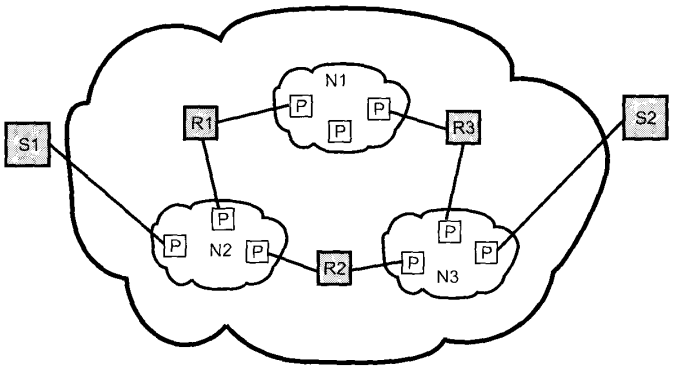
La tabla de encaminamiento puede ser estática o dinámica. Una tabla estática puede contener rutas alternativas por si algún dispositivo de encaminamiento no está disponible. Una tabla dinámica es más flexible a la hora de enfrentarse a condiciones de error y congestión. En Internet, por ejemplo, cuando un dispositivo de encaminamiento se desconecta, todos sus vecinos emitirán un informe de estado, permitiendo a otros dispositivos de encaminamiento y estaciones que actualicen sus tablas de encaminamiento. Es posible utilizar un esquema similar para el control de congestión. Este último caso es particularmente importante a causa de la diferencias en capacidad entre las redes locales y las de área amplia. El Capítulo 16 discute los protocolos de encaminamiento.

Las tablas de encaminamiento también se pueden utilizar para ofrecer otros servicios de interconexión entre redes, como seguridad y prioridad. Por ejemplo, las redes individuales se podrían clasificar para gestionar datos de hasta un nivel de seguridad dado. El mecanismo de encaminamiento debe asegurar que los datos de cierto nivel de seguridad no se les permita pasar a través de redes no acreditadas para gestionar tales datos. Otra técnica de encaminamiento es el encaminamiento por la fuente. La estación fuente especifica la ruta mediante la inclusión de una lista secuencial de dispositivos de encaminamiento en el datagrama. Esto, de nuevo, podría ser útil por motivos de seguridad o prioridad.

Finalmente, mencionaremos un servicio relacionado con el encaminamiento: el registro de la ruta. Para registrar la ruta, cada dispositivo de encaminamiento incorpora su dirección internet a una lista de direcciones que lleva el datagrama. Esta característica es útil con el objetivo de realizar operaciones comprobación y depuración.



(a) Arquitectura de red de conmutación de paquetes



(b) Arquitectura de interconexión

Figura 15.3. La interconexión como una red (basado en [HIND83]).

Tiempo de vida de los datagramas

Si se utiliza un encaminamiento dinámico u otro alternativo, existe la posibilidad de que un datagrama viaje indefinidamente a través del conjunto de redes. Esto no es aconsejable por dos razones. Primero, un datagrama circulando indefinidamente consume recursos. Segundo, como veremos en el Capítulo 17 un protocolo de transporte depende de la existencia de un límite en la vida de un datagrama. Para evitar estos problemas, cada datagrama se puede marcar con un tiempo de vida. Una vez que ha transcurrido este tiempo de vida, el datagrama se descarta.

Una forma sencilla de implementar esta función es usar un contador de saltos. Cada vez que un datagrama pasa a través de un dispositivo de encaminamiento, se decrementa el contador. Alternativamente, el tiempo de vida podría ser una medida de tiempo auténtica. Esto requiere que los dispositivos de encaminamiento conozcan de alguna forma el tiempo transcurrido desde que el datagrama o un fragmento cruzó por última vez un dispositivo de encaminamiento, para conocer cuánto tiene que decrementar el campo de tiempo de vida. Esto requeriría algún mecanismo global de sincronización. La ventaja de usar una medida real de tiempo es que se puede utilizar en el algoritmo de reensamblaje descrito a continuación.

Segmentación y reensamblado

Las redes individuales en un conjunto de redes pueden especificar tamaños máximos de paquetes diferentes. Sería ineficiente e inmanejable tratar de imponer un tamaño de paquete uniforme a través de las redes. Así, ocurre que los dispositivos de encaminamiento pueden necesitar segmentar los datagramas de entrada en unidades más pequeñas, llamadas fragmentos, antes de transmitirlos en la red siguiente.

Si los datagramas se pueden segmentar (quizás más de una vez) durante sus viajes, la cuestión que surge es que dónde se deben reensamblar. La solución más fácil es realizar el reensamblaje solamente en el destino. La principal desventaja de este método es que los fragmentos sólo se pueden hacer más pequeños a medida que los datos se mueven a través del conjunto de redes. Esto puede perjudicar la eficiencia de algunas redes. Por otra parte, si los dispositivos de encaminamiento intermedios pueden reensamblar aparecen las siguientes desventajas:

1. Se requieren grandes memorias temporales en los dispositivos de encaminamiento y existe el riesgo de que todo el espacio de memoria temporal se use para almacenar datagramas parciales.
2. Todos los fragmentos de un datagrama deben pasar a través del mismo dispositivo de encaminamiento de salida. Esto imposibilita el uso del encaminamiento dinámico.

En IP, los fragmentos de los datagramas se reensamblan en el sistema final destino. La técnica de segmentación de IP usa los siguientes campos en la cabecera IP:

- Identificador de la unidad de datos (ID).
- Longitud de los datos.
- Desplazamiento.
- Indicador de más datos.

El *ID* es un medio de identificar de forma única un datagrama originado en un sistema final. En IP, el ID consta de las direcciones fuente y destino, un identificador del protocolo que genera los datos (por ejemplo, TCP) y un número de secuencia suministrado por el protocolo. La *longitud de los datos* indica la longitud del campo datos de usuario expresado en octetos, y el campo *desplazamiento* es la posición de un fragmento de los datos de usuario en el campo de datos en el datagrama original, en múltiplos de 64 bits.

El sistema final origen crea un datagrama con una longitud de datos igual a la longitud entera del campo de datos, con *desplazamiento* = 0 y el indicador de *más datos* establecido a 0 (falso). Para segmentar un datagrama grande en dos piezas, un módulo IP en un dispositivo de encaminamiento realiza las siguientes tareas:

1. Crea dos nuevos datagramas y copia los campos de la cabecera del datagrama original en los datagramas nuevos.
2. Divide el campo de datos de usuario en dos porciones aproximadamente iguales con límites de 64 bits, situando cada porción en cada datagrama nuevo. La primera porción debe ser un múltiplo de 64 bits (8 octetos).
3. Establece la *longitud de datos* del primer datagrama a la longitud de los datos insertados, establece a uno el indicador de *más datos* (cierto). El campo *desplazamiento* no se cambia.
4. Establece la *longitud de datos* del segundo datagrama a la longitud de los datos insertados, y añade la longitud de la primera porción de datos dividida por 8 al campo *desplazamiento*. El indicador de *más datos* permanece igual.

La Figura 15.4 muestra un ejemplo. El procedimiento se puede generalizar fácilmente a una división de *n*-caminos.

Para reensamblar un datagrama, debe haber suficiente espacio de memoria temporal en el momento de reensamblar. Conforme los fragmentos con el mismo ID llegan, los campos de datos se insertan en la posición correcta en la memoria temporal hasta que el campo datos entero se reensambla, lo que se

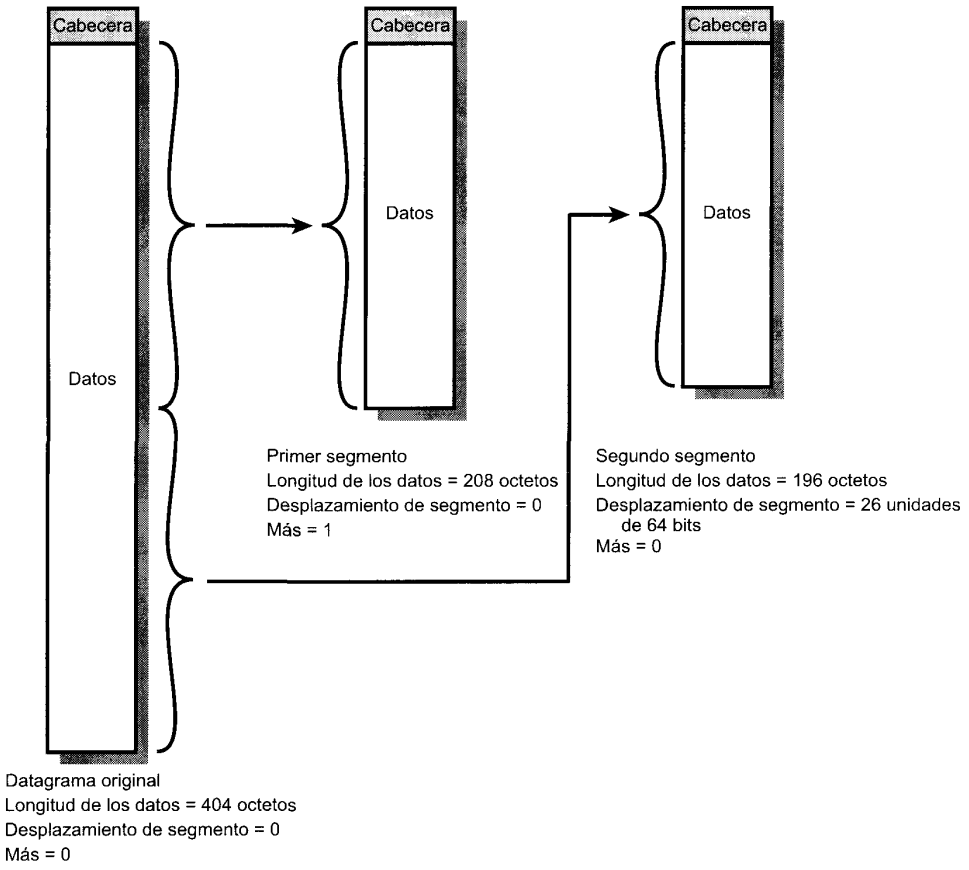


Figura 15.4. Ejemplo de segmentación.

consigue cuando existe un conjunto contiguo de datos comenzando con un *desplazamiento* de cero y terminando con datos de un segmento con el indicador de *más datos* puesto a falso.

Una eventualidad con la que hay que enfrentarse es que uno o más fragmentos no hayan llegado: el servicio IP no garantiza la entrega. Se necesitan algunos métodos para decidir abandonar una tentativa de reensamblaje con objeto de liberar espacio de memoria temporal. Comúnmente se utilizan dos técnicas. La primera, asigna un tiempo de vida de reensamblaje al primer segmento que llega. Éste se regula con un reloj en tiempo real local asignado por la función de reensamblaje y decrementado mientras los fragmentos del datagrama original se van almacenado en memoria temporal. Si el tiempo expira antes de completar el reensamblaje, los fragmentos recibidos se descartan. Una segunda técnica consiste en hacer uso del tiempo de vida del datagrama, que es parte de la cabecera de cada uno de los fragmentos entrantes. El campo de vida se continúa decrementando por la función de reensamblaje; como con la primera técnica, si el tiempo de vida expira antes de completar el reensamblaje, los fragmentos recibidos se descartan.

Control de errores

El sistema de interconexión entre redes no garantiza la distribución satisfactoria de cada datagrama. Cuando un dispositivo de encaminamiento descarta un datagrama, el dispositivo de encaminamiento de-

bería intentar devolver alguna información al origen, si es posible. El protocolo Internet origen puede usar esta información para modificar su estrategia de transmisión y notificarlo a las capas superiores. Para informar de que un datagrama específico ha sido descartado, se necesita algún medio de identificar datagramas.

Los datagramas se pueden descartar por una serie de razones, incluyendo la expiración del tiempo de vida, congestión y error en la suma de comprobación. En este último caso, no es posible realizar una notificación ya que el campo de la dirección fuente puede haber sido dañado.

Control de flujo

El control de flujo en la interconexión permite a los dispositivos de encaminamiento y/o las estaciones receptoras limitar la razón a la cual se reciben los datos. Para un servicio del tipo sin conexión que estamos describiendo, los mecanismos de control de flujo son limitados. El mejor enfoque parece ser enviar paquetes de control de flujo, requiriendo una reducción del flujo de datos a otros dispositivos de encaminamiento y a las estaciones fuente. Se verá un ejemplo de esta situación con ICMP, que se discutirá en la sección siguiente.

15.3. EL PROTOCOLO INTERNET

El protocolo Internet (IP) es parte del conjunto de protocolos TCP/IP y es el protocolo de interconexión entre redes más utilizado. Como con cualquier protocolo estándar, IP se especifica en dos partes:

- La interfaz con la capa superior (por ejemplo, TCP), especificando los servicios que proporciona IP.
- El formato real del protocolo y los mecanismos asociados.

En esta sección, se examinan primero los servicios de IP y después el protocolo IP. A esto seguirá una discusión del formato de la dirección IP. Finalmente, se describe el protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol), que es una parte integral de IP.

SERVICIOS IP

Los servicios que se van a proporcionar entre las capas de protocolos adyacentes (por ejemplo, entre IP y TCP) se expresan en términos de primitivas y parámetros. Una primitiva especifica la función que se va a ofrecer y los parámetros se utilizan para pasar datos e información de control. La forma real de una primitiva depende de la implementación. Un ejemplo es una llamada a subrutina.

IP proporciona dos primitivas de servicio en la interfaz con la siguiente capa superior (Figura 15.5). La primitiva Send (envío) se utiliza para solicitar la retransmisión de una unidad de datos. La primitiva Deliver (entrega) utiliza IP para notificar a un usuario la llegada de una unidad de datos. Los parámetros asociados con estas dos primitivas son los siguientes:

- **Dirección origen:** dirección global de red de la entidad IP que envía la unidad de datos.
- **Dirección destino:** dirección global de red de la entidad IP de destino.
- **Protocolo:** entidad de protocolo recipiente (un usuario IP).
- **Indicadores del tipo de servicio**: utilizado para especificar el tratamiento de la unidad de datos en su transmisión a través de los componentes de las redes.
- **Identificador:** utilizado en combinación con las direcciones origen y destino y el protocolo usuario para identificar de una forma única a la unidad de datos. Este parámetro se necesita para reensamblar e informar de errores.

Send {	Deliver {
Dirección origen	Dirección origen
Dirección destino	Dirección destino
Protocolo	Protocolo
Indicadores del tipo de servicio	Indicadores del tipo de servicio
Identificador	
Indicador de no fragmentación	
Tiempo de vida	
Longitud de los datos	Longitud de los datos
Datos de opción	Datos de opción
Datos	Datos
}	}

Figura 15.5. Primitivas y parámetros de servicio IP.

- **Indicador de no fragmentación:** indica si IP puede segmentar los datos para realizar el transporte.
- **Tiempo de vida:** medida en segundos.
- **Longitud de los datos:** longitud de los datos que se transmiten.
- **Datos de opción:** opciones solicitadas por el usuario IP.
- **Datos:** datos de usuario que se van a transmitir.

Hay que indicar que los parámetros *identificador*, *indicador de no fragmentación* y *tiempo de vida* se encuentran presentes en la primitiva Send pero no lo están en la primitiva Deliver. Estos tres parámetros proporcionan instrucciones a IP pero no son incumbencia del usuario IP destino.

El usuario IP que hace el envío incluye el parámetro *tipo de servicio* para solicitar una calidad de servicio particular. El usuario puede especificar uno o más de los servicios enumerados en la Tabla 15.2. Este parámetro se puede utilizar para orientar en las decisiones de encaminamiento. Por ejemplo, si un dispositivo de encaminamiento tiene varias opciones alternativas para elegir el siguiente salto en el encaminamiento del datagrama, podría elegir una red con una tasa de transferencia de datos mayor si se ha elegido la opción de gran rendimiento. Este parámetro también se pasa al protocolo de acceso a la red para que se use en redes individuales en caso de que sea posible. Por ejemplo, si se selecciona un nivel de precedencia y la red soporta niveles de precedencia o prioridad, el nivel de precedencia se traducirá al correspondiente en el nivel de red para este salto.

Los parámetros de *opciones* permiten futuras extensiones y la inclusión de parámetros que normalmente no se invocan. Las opciones actualmente definidas son:

- **Seguridad:** permite que se incorpore una etiqueta de seguridad al datagrama.

Tabla 15.2. Opciones de calidad del servicio IP.

Precedencia	Una medida de la importancia relativa del datagrama. Se utilizan ocho niveles de precedencia. IP tratará de proporcionar un tratamiento preferencial a los datagramas con precedencias superiores.
Seguridad	Se puede especificar uno de dos niveles: normal o alto. Un valor alto indica una petición para que se hagan intentos de minimizar la probabilidad de que este datagrama se pierda o resulte dañado.
Retardo	Se puede especificar uno de dos niveles: normal o bajo. Un valor bajo indica una petición para minimizar el retardo que experimentará este datagrama.
Rendimiento	Se puede especificar uno de dos niveles: normal o alto. Un valor alto indica una petición para maximizar el rendimiento para este datagrama.

- **Encaminamiento por la fuente:** constituye una lista secuencial de direcciones de dispositivos de encaminamiento que especifica la ruta a seguir.
- **Registro de la ruta:** se reserva un campo para registrar la secuencia de dispositivos de encaminamiento visitados por el datagrama.
- **Identificación de secuencia:** identifica recursos reservados utilizados para un servicio de secuencia. Este servicio proporciona un tratamiento especial del tráfico volátil periódico (por ejemplo, voz).
- **Marcas de tiempo:** la entidad IP origen y algunos o todos los dispositivos de encaminamiento intermedios incorporan una marca temporal (con una precisión de milisegundos) a las unidades de datos conforme van pasando por ellos.

PROTOCOLO IP

El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP, mostrado en la Figura 15.6. Los campos son los siguientes:

- **Versión (4 bits):** indica el número de la versión del protocolo, para permitir la evolución del protocolo.
- **Longitud de la cabecera Internet (IHL, Internet Header Length) (4 bits):** longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de cinco, correspondiente a una longitud de la cabecera mínima de 20 octetos.
- **Tipo de servicio (8 bits):** especifica los parámetros de seguridad, prioridad, retardo y rendimiento.
- **Longitud total (16 bits):** longitud total del datagrama, en octetos.
- **Identificador (16 bits):** un número de secuencia que, junto a la dirección origen y destino y el protocolo usuario se utilizan para identificar de forma única un datagrama. Por lo tanto, el identificador debe ser único para la dirección origen del datagrama, la dirección destino y el protocolo usuario durante el tiempo en el que el datagrama permanece en el conjunto de redes.
- **Indicadores (3 bits):** solamente dos de estos tres bits están actualmente definidos. El bit «Más» se usa para segmentación y reensamblado, como se ha explicado previamente. El bit de «no fragmentación» prohíbe la fragmentación cuando es 1. Este bit es útil para conocer si el destino tiene la capacidad de reensamblar fragmentos. Sin embargo, si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo de una red en la ruta. Por tanto, cuando el bit vale 1, es aconsejable utilizar encaminamiento por la fuente para evitar redes con tamaños de paquete máximos pequeños.

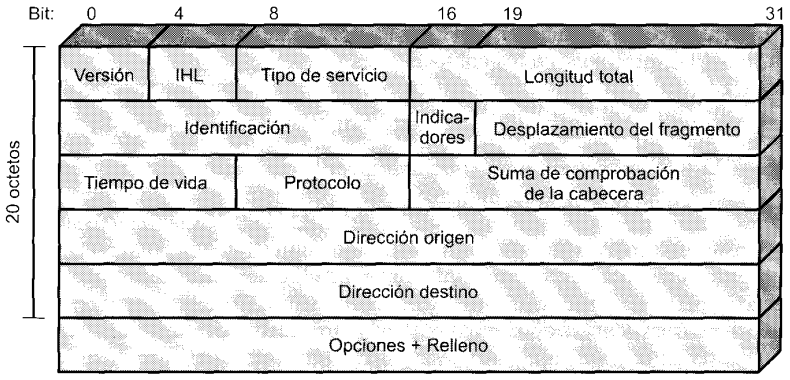


Figura 15.6. Cabecera IPv4.

- **Desplazamiento del fragmento (13 bits):** indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits. Esto implica que todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 64 bits.
- **Tiempo de vida (8 bits):** especifica cuanto tiempo, en segundos, se le permite a un datagrama permanecer en la red. Cada dispositivo de encaminamiento que procesa el datagrama debe decrementar este campo al menos en una unidad, de forma que el tiempo de vida es de alguna forma similar a una cuenta de saltos.
- **Suma de comprobación de la cabecera (16 bits):** un código de detección de errores aplicado sólamente a la cabecera. Ya que algunos campos de la cabecera pueden cambiar durante el viaje (por ejemplo, el tiempo de vida, campos relacionados con la segmentación), este valor se verifica y recalcula en cada dispositivo de encaminamiento. El campo suma de comprobación es la suma complemento a uno de todas las palabras de 16 bits en la cabecera. Por motivos de cálculo, este campo se inicializa a sí mismo a un valor de todo cero.
- **Dirección origen (32 bits):** codificada para permitir una asignación variable de bits para especificar la red y el sistema final conectado a la red especificada, como se discute posteriormente.
- **Dirección destino (32 bits):** igual que el campo anterior.
- **Opciones (variable):** contiene las opciones solicitadas por el usuario que envía los datos.
- **Relleno (variable):** se usa para asegurar que la cabecera del datagrama tiene una longitud múltiplo de 32 bits.
- **Datos (variable):** el campo de datos debe tener una longitud múltiplo de 8 bits. La máxima longitud de un datagrama (campo de datos más cabecera) es de 65.535 octetos.

Debería quedar claro como se traducen los servicios IP especificados en la primitivas Send y Deliver en los campos del datagrama IP.

DIRECCIONES IP

Los campos dirección origen y destino en la cabecera IP contienen cada uno una dirección internet de 32 bits global, que generalmente consta de un identificador de red y un identificador de computador.

Clases de red

La dirección está codificada para permitir una asignación variable de bits para especificar la red y el computador, como se muestra en la Figura 15.7. Este esquema de codificación proporciona flexibilidad al asignar las direcciones a los computadores y permite una mezcla de tamaños de red en un conjunto de redes. En particular, existen tres clases de redes que se pueden asociar a las siguientes condiciones:

- **Clase A:** pocas redes, cada una con muchos computadores.
- **Clase B:** un número medio de redes, cada una con un número medio de computadores.
- **Clase C:** muchas redes, cada una con pocos computadores.

En un entorno particular, podría ser mejor utilizar todas las direcciones de una misma clase. Por ejemplo, en una conjunto de redes de una entidad, consistente en un gran número de redes de área local departamentales, se necesitaría usar direcciones Clase C exclusivamente. Sin embargo, el formato de las direcciones es tal que es posible mezclar las tres clases de direcciones en el mismo conjunto de redes; esto es lo que se hace en el caso de la misma Internet. En el caso de un conjunto de redes formado por pocas redes grandes, muchas redes pequeñas y algunas redes de tamaño mediano, es apropiado utilizar una mezcla de clases de direcciones.

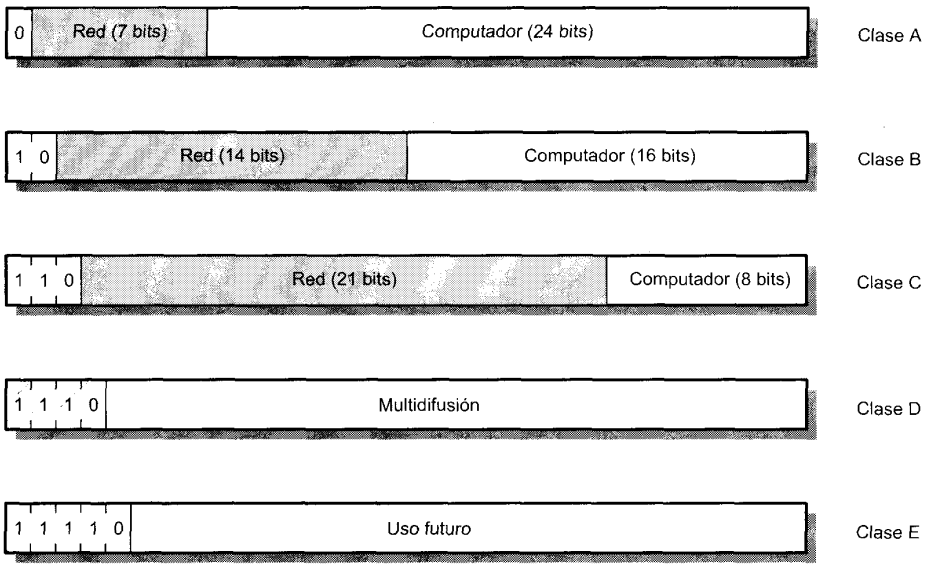


Figura 15.7. Formatos de dirección IP.

Las direcciones IP se escriben normalmente en lo que se llama, notación punto decimal, utilizando un número decimal para representar cada uno de los octetos de la dirección de 32 bits. Por ejemplo, la dirección IP 11000000 11100100 00010001 00111001 se escribe como 192.228.17.57.

Hay que darse cuenta que todas las direcciones de red Clase A empiezan con un 0 binario. Las direcciones de red con el primer octeto puesto a 0 (en binario 00000000) o que sea 127 (en binario 01111111) están reservadas, por lo tanto existen 126 números de red potenciales de Clase A, en los cuales su primer octeto en formato punto decimal está en el rango de 1 a 126. Las direcciones de red de Clase B comienza con un número binario 10, de forma que su primer número decimal está entre 128 y 191 (en binario entre 10000000 y 10111111). El segundo octeto también forma parte de la dirección de Clase B, de forma que existe $2^{14} = 16.384$ direcciones de Clase B. Para las direcciones de Clase C el primer número decimal va de 192 a 223 (de 11000000 a 11011111). El número total de direcciones de Clase C es de $2^{21} = 2.097.152$.

Subredes y máscaras de subred

El concepto de subred fue introducido para señalar la siguiente necesidad. Considere un conjunto de redes que incluye una o más WAN y un determinado número de sitios, cada uno de ellos con un determinado número de LAN. Nos gustaría tener una complejidad arbitraria de estructuras de LAN interconectadas dentro de la organización, aislando al resto del conjunto de redes frente a un crecimiento explosivo en el número de redes y la complejidad en el encaminamiento. Una solución a este problema es asignar a un único número de red todas las LAN en un sitio. Desde el punto de vista del resto del conjunto de redes, existe una única red en ese sitio, lo cual simplifica el direccionamiento y el encaminamiento. Para permitir que los dispositivos de encaminamiento funcionen correctamente, a cada LAN se le asigna un número de subred. La parte de *computador* en la dirección internet se divide en un número de subred y un número de computador para acomodar este nuevo nivel de direccionamiento.

Dentro de una red divida en subredes, los dispositivos de encaminamiento locales deben encaminar sobre la base de un número de red extendido consistente de la porción de *red* de la dirección IP y el número de subred. Las posiciones a nivel de bit que contienen este número de red extendido se indican

mediante la máscara de dirección. El uso de esta máscara de dirección permite a un computador determinar si un datagrama de salida va destinado a otro computador en la misma LAN (entonces se envía directamente) o a otra LAN (se envía a un dispositivo de encaminamiento). Se supone que se utiliza algún otro medio (por ejemplo, mediante la configuración manual) para crear la máscara de dirección y darla a conocer a los dispositivos de encaminamiento locales.

La Tabla 15.3a muestra los cálculos que se realizan con la utilización de la máscara de subred. Hay que darse cuenta que el efecto de la máscara de subred es borrar el campo de computador que indica el computador real en una subred. Lo que permanece es el número de red y el número de subredes. La Figura 15.8 muestra un ejemplo de utilización de subredes. La figura muestra un complejo local consistente en tres LAN y dos dispositivos de encaminamiento. Para el resto del conjunto de redes este complejo es una red única con una dirección de Clase C de la forma 192.228.17.*x*, donde los tres octetos más a la izquierda son el número de red y el octeto más a la derecha contiene un número de computador *x*. Ambos dispositivos de encaminamiento R1 y R2 se configuran con una máscara de subred con el valor 255.255.255.224 (véase Tabla 15.3a). Por ejemplo, si un datagrama con una dirección destino 192.228.17.57 llega a R1 desde el resto del conjunto de redes o desde la LAN Y, R1 aplica la máscara de subred para determinar que esta dirección hace referencia a una dirección de la subred 1, la cual es la LAN X, y si es así enviarlo a la LAN X. De forma similar, si llega un datagrama con esa dirección destino a R2 desde la LAN Z, R2 aplica la máscara y determina a partir de su base de datos que el datagrama destinado a la subred 1 se debe enviar a R1. Los computadores también utilizan la máscara de subred para hacer decisiones de encaminamiento.

La máscara de subred por defecto para una clase de direcciones dada es una máscara nula (Tabla 15.3b), lo cual produce el mismo número de red y de computador que en el caso de una dirección sin subredes.

Tabla 15.3. Direcciones IP y máscaras de subred [STEI95].

(a) Representaciones punto decimal y binaria de las direcciones IP y las máscaras de subred

	Representación binaria	**Punto decimal**
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.111000000	255.255.255.224
Operación AND bit-a-bit de la dirección y la máscara (número de red/subred resultante)	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

(b) Máscaras de subred por defecto

	Representación binaria	**Punto decimal**
Máscara de Clase A por defecto	11111111.00000000.00000000.00000000	255.0.0.0
Ejemplo de máscara de Clase A	11111111.11000000.00000000.00000000	255.192.0.0
Máscara de Clase B por defecto	11111111.11111111.00000000.00000000	255.255.0.0
Ejemplo de máscara de Clase B	11111111.1111111.11111000.00000000	255.255.248.0
Máscara de Clase C por defecto	11111111.11111111.11111111.00000000	255.255.255.0
Ejemplo de máscara de Clase C	11111111.11111111.11111111.11111100	255.255.255.252

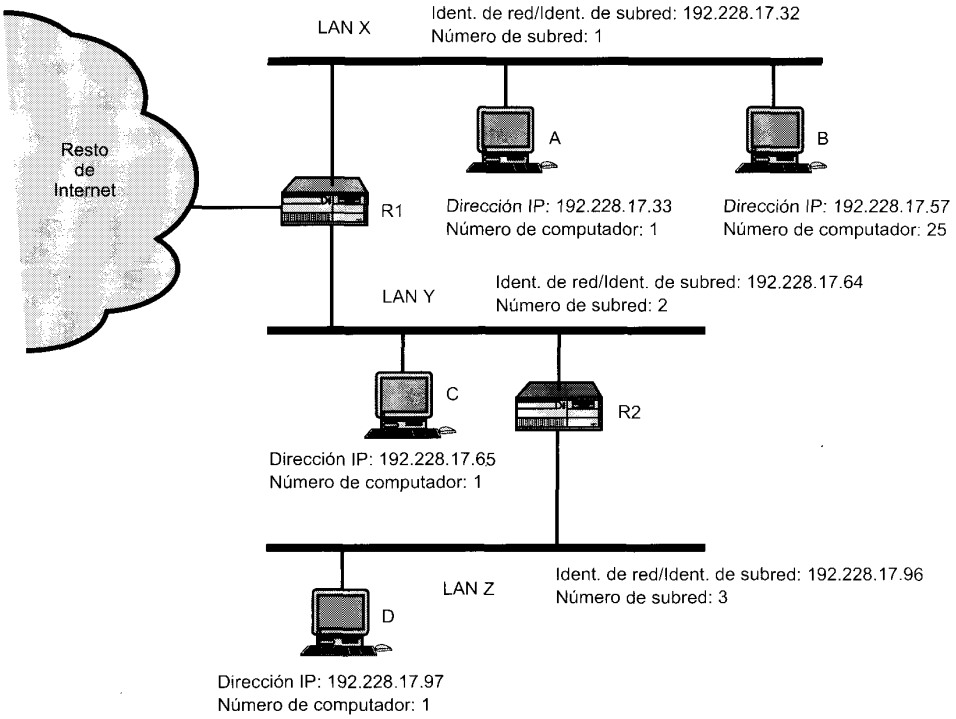


Figura 15.8. Ejemplo de utilización de subredes.

PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET (ICMP)

El estándar IP especifica que una implementación que cumpla las especificaciones del protocolo debe también implementar ICMP (RFC 792). ICMP proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. En esencia, ICMP proporciona información de realimentación sobre problemas del entorno de la comunicación. Algunas situaciones donde se utiliza son: cuando un datagrama no puede alcanzar su destino, cuando el dispositivo de encaminamiento no tiene la capacidad de almacenar temporalmente para reenviar el datagrama y cuando el dispositivo de encaminamiento indica a una estación que envíe el tráfico por una ruta más corta. En la mayoría de los casos, el mensaje ICMP se envía, en respuesta a un datagrama, bien por un dispositivo de encaminamiento en el camino del datagrama o por el computador destino deseado.

Aunque ICMP está, a todos los efectos, en el mismo nivel que IP en el conjunto de protocolos TCP/IP, es un usuario de IP. Cuando se construye un mensaje ICMP se pasa a IP, que encapsula el mensaje con una cabecera IP y después transmite el datagrama resultante de la forma habitual. Ya que los mensajes ICMP se transmiten en datagramas IP, no se garantiza su entrega y su uso no se puede considerar seguro.

La Figura 15.9 muestra el formato de varios tipos de mensajes ICMP. Todos los mensajes ICMP empiezan con una cabecera de 64 bits que consta de los siguientes campos:

- **Tipo (8 bits):** especifica el tipo de mensaje ICMP.
- **Código (8 bits):** se usa para especificar parámetros del mensaje que se pueden codificar en uno o unos pocos bits.

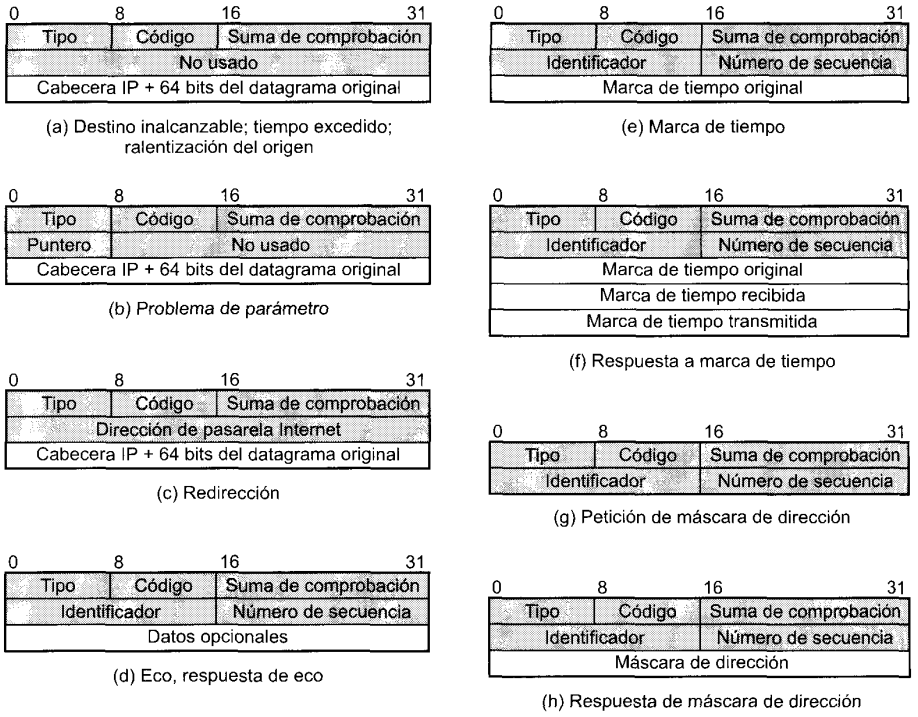


Figura 15.9. Formatos de mensajes ICMP.

- **Suma de comprobación (16 bits):** Suma de comprobación del mensaje ICMP entero. Se utiliza e mismo algoritmo de suma de comprobación que en IP.
- **Parámetros (32 bits):** se usa para especificar parámetros más largos.

A estos campos les siguen generalmente campos de información adicional que especifican aún má el contenido del mensaje.

En aquellos casos en los que los mensajes ICMP se refieren a datagramas, el campo de informació incluye la cabecera IP entera más los primeros 64 bits del campo de datos del datagrama original. Est permite al computador origen comparar el mensaje ICMP que llega con el datagrama anterior. La razó de incorporar los primeros 64 bits del campo de datos es que permite al módulo IP en el computado determinar qué protocolo del nivel superior o protocolos estaban implicados. En particular, los primero 64 bits incluirían una porción de la cabecera TCP u otra cabecera del nivel de transporte.

Los mensajes ICMP pueden ser del siguiente tipo:

- Destino inalcanzable.
- Tiempo excedido.
- Problema de parámetro.
- Ralentización del origen.
- Redirección.
- Eco.
- Respuesta a eco.
- Marca de tiempo.
- Respuesta a la marca de tiempo.

- Petición de máscara de dirección.
- Respuesta de máscara de dirección.

El mensaje **destino inalcanzable** cubre un cierto número de posibilidades. Un dispositivo de encaminamiento puede devolver este mensaje si no sabe cómo alcanzar la red destino. En algunas redes, un dispositivo de encaminamiento conectado a una de estas redes puede ser capaz de determinar si un computador particular es inalcanzable, y devolver este tipo de mensaje. El mismo computador destino puede devolver este tipo de mensaje si el protocolo de usuario o algún punto de acceso al servicio de un nivel superior no está alcanzable. Esto puede ocurrir si el correspondiente campo en la cabecera IP no tiene el valor correcto. Finalmente, si un dispositivo de encaminamiento debe segmentar un datagrama pero el indicador de no segmentación está establecido, se devuelve también el mensaje «destino inalcanzable».

Un dispositivo de encaminamiento devolverá el mensaje **tiempo excedido** si el tiempo de vida del datagrama ha expirado. Un computador enviará este mensaje si no puede completar el reensamblaje en un tiempo determinado.

Un error sintáctico o semántico en la cabecera IP causará que un dispositivo de encaminamiento o un computador devuelva un mensaje de **problema de parámetro**. Por ejemplo, puede existir un argumento incorrecto en una opción. El campo parámetro de la respuesta contiene un puntero al octeto en la cabecera original donde se detectó el error.

El mensaje **ralentización del origen** proporciona una forma rudimentaria de control de flujo. Este mensaje lo pueden enviar tanto un dispositivo de encaminamiento como un computador destino a un computador origen solicitando que reduzca la razón de datos a la que envía el tráfico al destino internet. Cuando se recibe este tipo de mensaje, un computador origen debe disminuir la razón de datos a la que envía el tráfico al destino especificado hasta que no reciba más mensajes de ralentización del origen. El mensaje de ralentización del origen lo puede generar tanto un dispositivo de encaminamiento como un computador que deba descartar datagramas debido a que su memoria temporal está llena. En este caso, el dispositivo de encaminamiento o el computador enviarán un mensaje de ralentización del origen por cada datagrama que descarta. Además, un sistema se puede anticipar a la congestión y enviar este tipo de mensaje cuando su memoria esté a punto de llegar a su capacidad máxima. En ese caso, el datagrama referido en el mensaje de ralentización del origen podrá ser entregado correctamente. Así, la recepción de un mensaje de ralentización del origen no implica la entrega o la no entrega del correspondiente datagrama.

Un dispositivo de encaminamiento envía un mensaje **redirección** a un computador conectado directamente a un dispositivo de encaminamiento para informarle de una ruta mejor para un destino particular. A continuación se da un ejemplo de su uso utilizando la Figura 15.8. El dispositivo de encaminamiento, R1, recibe un datagrama del computador C en la red Y a la que está conectado R1. El dispositivo de encaminamiento R1 comprueba su tabla de encaminamiento y obtiene la dirección del siguiente dispositivo de encaminamiento, R2, en la ruta del datagrama a la red destino, Z. Si R2 y el computador identificado por la dirección internet origen del datagrama están en la misma red, R1 envía un mensaje de redirección al computador C. Este mensaje informa al computador para que envíe su tráfico para la red Z directamente al dispositivo de encaminamiento R2, ya que éste es el camino más corto al destino. El dispositivo de encaminamiento envía el datagrama original a su destino (vía R2). La dirección de R2 se encuentra en el campo de parámetros del mensaje de redirección.

Los mensajes **eco** y **respuesta a eco** proporcionan un mecanismo para comprobar que la comunicación entre dos entidades es posible. El receptor de un mensaje de eco está obligado a devolver el mensaje en un mensaje de respuesta a eco. Al mensaje de eco se le asocia un identificador y un número de secuencia que coinciden con los de paquete respuesta de eco. El identificador se puede utilizar como un punto de acceso al servicio para identificar una sesión particular, y el número de secuencia se puede incrementar en cada petición de eco enviada.

Los mensajes **marca de tiempo** y **respuesta a marca de tiempo** proporcionan un mecanismo para muestrear las características en cuanto a retardo del conjunto de redes. El emisor de un mensaje marca

de tiempo puede incluir un identificador y un número de secuencia en el campo parámetros e incluye el tiempo en el cual se envío el mensaje (marca de tiempo original). El receptor registra, en el mensaje respuesta la marca de tiempo, el tiempo en que recibió el mensaje y el tiempo en que transmitió el mensaje de respuesta. Si el mensaje de marca de tiempo se envía usando un encaminamiento por la fuente estricto, se puede determinar las características de retardo de una ruta particular.

Los mensajes **petición de máscara de dirección** y **respuesta a máscara de dirección** son útiles en un entorno que incluya subredes. Los mensajes de petición y respuesta de máscara de dirección permiten a un computador conocer la máscara de dirección usada en la LAN a la que está conectado. El computador emite por difusión un mensaje de petición de máscara de dirección en la LAN. El dispositivo de encaminamiento en la LAN responde con un mensaje de respuesta a máscara de red que contiene la máscara de dirección.

15.4. IPv6

El Protocolo Internet (IP) ha sido el fundamento de Internet y virtualmente de todas las redes privadas de múltiples suministradores. Este protocolo está alcanzando el fin de su vida útil y se ha definido un nuevo protocolo conocido como IPv6 (IP versión 6) para, en última instancia, reemplazar a IP[1].

Primero examinaremos la motivación para desarrollar una nueva versión de IP y después analizaremos algunos de sus detalles.

IP DE NUEVA GENERACIÓN

El motivo que ha conducido a la adopción de una nueva versión ha sido la limitación impuesta por el campo de dirección de 32 bits en IPv4. Con un campo de dirección de 32 bits, en principio es posible asignar 2^{32} direcciones diferentes, alrededor de 4.000 millones de direcciones posibles. Se podría pensar que este número de direcciones era más que adecuado para satisfacer las necesidades en Internet. Sin embargo, a finales de la década de 1980 se percibió que habría un problema y este problema empezó a manifestarse a comienzos de la década de 1990. Algunas de las razones por las que es inadecuado utilizar estas direcciones de 32 bits son las siguientes:

- La estructura en dos niveles de la dirección IP (número de red, número de computador) es conveniente pero también es una forma poco económica de utilizar el espacio de direcciones. Una vez que se le asigna un número de red a una red, todas los números de computador de ese número de red se asignan a esa red. El espacio de direcciones para esa red podría estar poco usado, pero en lo que concierne a la efectividad del espacio de direcciones, si se usa un número de red entonces se consumen todas las direcciones dentro de la red.
- El modelo de direccionamiento de IP requiere que se asigne un número de red único a cada red IP independientemente si la red está realmente conectada a Internet.
- Las redes están proliferando rápidamente. La mayoría de los organismos establecen LAN múltiples, no un único sistema LAN. Las redes inalámbricas están adquiriendo un mayor protagonismo. Internet misma ha crecido explosivamente durante años.
- El uso creciente de TCP/IP en áreas nuevas producirá un crecimiento rápido en la demanda de direcciones únicas IP (por ejemplo, el uso de TCP/IP para interconectar terminales electrónicos de puntos de venta y para los receptores de televisión por cable).

[1] Se podría pensar que se han saltado varias versiones en este texto. La versión en uso de IP es actualmente la versión 4; las versiones previas de IP (de la 1 a la 3) fueron definidas sucesivamente y sustituidas hasta alcanzar IPv4. La versión 5 es el número asignado al protocolo de flujo, un protocolo de la capa internet orientado a conexión. De aquí el uso de la etiqueta versión 6.

- Normalmente, se asigna una dirección única a cada computador. Una disposición más flexible es permitir múltiples direcciones IP a cada computador. Esto por supuesto incrementa la demanda de direcciones IP.

Por lo tanto, la necesidad de un incremento en el espacio de direcciones ha impuesto la necesidad de una nueva versión de IP. Además, IP es un protocolo muy viejo y se han definido nuevos requisitos en las áreas de configuración de red, flexibilidad en el encaminamiento y facilidades para el tráfico.

En respuesta a estas necesidades, la Internet Engineering Task Force (IETF) emitió una solicitud de propuestas para una nueva generación de IP (IPng) en julio de 1992. Se recibieron varias propuestas y en 1994 emergió el diseño final de IPng. Uno de los hechos destacados del desarrollo fue la publicación del RFC 1752, «La recomendación para el protocolo de nueva generación de IP», publicado en enero de 1995. El RFC 1752 describe los requisitos de IPng, especifica el formato de la PDU y señala las técnicas de IPng en las áreas de direccionamiento, encaminamiento y seguridad. Existen otros documentos Internet que definen los detalles del protocolo, ahora llamado oficialmente IPv6; éstos incluyen una especificación general de IPv6 (RFC 2460), un RFC que trata con la estructura de direccionamiento de IPv6 (RFC 2373) y una larga lista más.

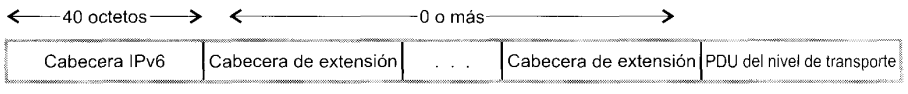
IPv6 incluye las siguientes mejoras sobre IPv4:

- **Un espacio de direcciones ampliado:** IPv6 utiliza direcciones de 128 bits en lugar de las direcciones de 32 bits de IPv4. Esto supone un incremento del espacio de direcciones por un factor de 2^{96}. Se ha señalado [HIND95] que esto permite espacios de direcciones del orden de 6×10^{23} por metro cuadrado de la superficie de la tierra. Incluso si la asignación de las direcciones fuera muy ineficiente, este espacio de direcciones parece seguro.
- **Un mecanismo de opciones mejorado:** las opciones de IPv6 se encuentran en cabeceras opcionales separadas situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los paquetes IPv6 en comparación a los datagramas IPv4[2]. Esto también hace que sea más fácil incorporar opciones adicionales.
- **Direcciones de autoconfiguración:** esta capacidad proporciona una asignación dinámica de direcciones IPv6.
- **Aumento de la flexibilidad en el direccionamiento:** IPv6 incluye el concepto de una dirección monodistribución (anycast), mediante la cual un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos. Se mejora la escalabilidad del encaminamiento multidistribución con la incorporación de un campo de acción a las direcciones multidistribución.
- **Facilidad para la asignación de recursos:** en lugar del campo tipo-de-servicio de IPv4, IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial. Esto ayuda al tratamiento del tráfico especializado como el de vídeo en tiempo real.

Todas estas características se exploran en el resto de la sección, excepto las características de seguridad, que se discuten en el Capítulo 18.

ESTRUCTURA IPv6

Una unidad de datos de protocolo de IPv6 (conocida como paquete) tiene el formato general siguiente:



[2] La unidad de datos de protocolo para IPv6 se denomina un paquete en lugar de datagrama, que es el término que se utiliza para las PDU de IPv4.

La única cabecera que se requiere se llama, para simplificar, como la cabecera IPv6. Esta tiene una longitud fija de 40 octetos, comparados con los 20 octetos de la parte obligatoria de la cabecera IPv4 (Figura 15.6). Se han definido la siguientes cabeceras de extensión:

- **Cabecera de opciones salto-a-salto:** define opciones especiales que requieren procesamiento en cada salto.
- **Cabecera de encaminamiento:** proporciona un encaminamiento ampliado, similar al encaminamiento por la fuente de IPv4.
- **Cabecera de fragmentación:** contiene información de fragmentación y reensamblaje.
- **Cabecera de autentificación:** proporciona la integridad del paquete y la autentificación.
- **Cabecera de encapsulamiento de la carga de seguridad:** proporciona seguridad.
- **Cabecera de las opciones para el destino:** contiene información opcional para que sea examinada en el nodo destino.

El estándar IPv6 recomienda que, en el caso de que se usen varias cabeceras de extensión, las cabeceras IPv6 aparezcan en el siguiente orden:

1. Cabecera IPv6: obligatoria, debe aparecer siempre primero.
2. Cabecera de las opciones salto-a-salto.
3. Cabecera de las opciones para el destino: para opciones a procesar por el primer destino que aparece en el campo dirección IPv6 de destino y por los destinos subsecuentes indicados en la cabecera de encaminamiento.

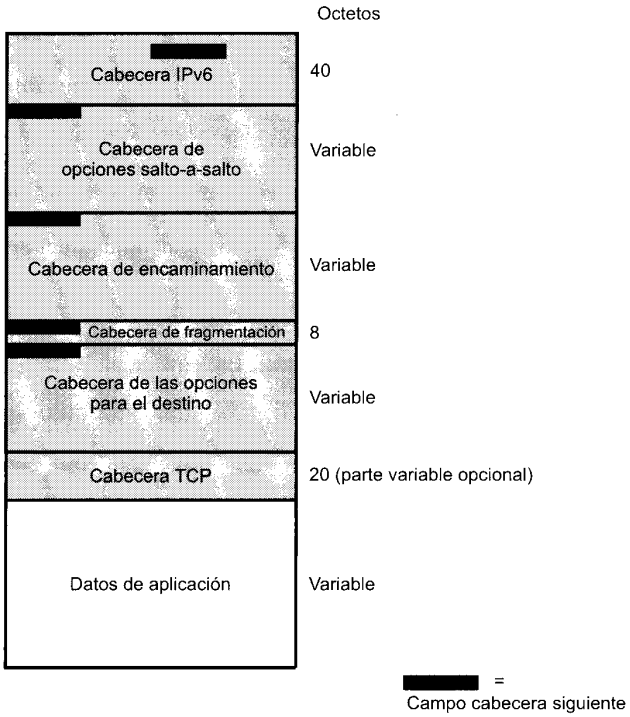


Figura 15.10. Paquete IPv6 con las cabeceras de extensión (conteniendo un segmento TCP).

4. Cabecera de encaminamiento.
5. Cabecera de fragmentación.
6. Cabecera de autentificación.
7. Cabecera de encapsulado de la carga de seguridad.
8. Cabecera de opciones para el destino: para opciones a procesar solamente por el destino final del paquete.

La Figura 15.10 muestra un ejemplo de un paquete IPv6 que incluye un ejemplar de cada cabecera, excepto aquellas relacionadas con la seguridad. Obsérvese que la cabecera IPv6 y cada cabecera de extensión incluyen el campo Cabecera siguiente. Este campo identifica el tipo de cabecera que viene a continuación. Si la siguiente cabecera es de extensión, entonces este campo contiene el identificador del tipo de esa cabecera. En caso contrario, este campo contiene el identificador del protocolo de la capa superior que está usando a IPv6 (normalmente un protocolo de la capa de transporte), utilizando el mismo valor que el campo protocolo IPv4. En la Figura 15.10, el protocolo de la capa superior es TCP, por lo tanto, los datos de la capa superior transportados por el paquete IPv6 constan de una cabecera TCP seguido por un bloque de datos de aplicación.

A continuación se examina la cabecera principal de IPv6 y después se examinan cada una de las extensiones.

CABECERA IPv6

La cabecera IPv6 tiene una longitud fija de 40 octetos, que consta de los siguientes campos (Figura 15.11):

- **Versión (4 bits):** número de la versión del protocolo Internet; el valor es 6.
- **Clase de tráfico (8 bits):** disponible para su uso por el nodo origen y/o los dispositivos de encaminamiento de reenvío para identificar y distinguir entre diferentes clases o prioridades de paquete IPv6. El uso de este campo está todavía en estudio.
- **Etiqueta de flujo (20 bits):** se puede utilizar por un computador para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red; se discute después.

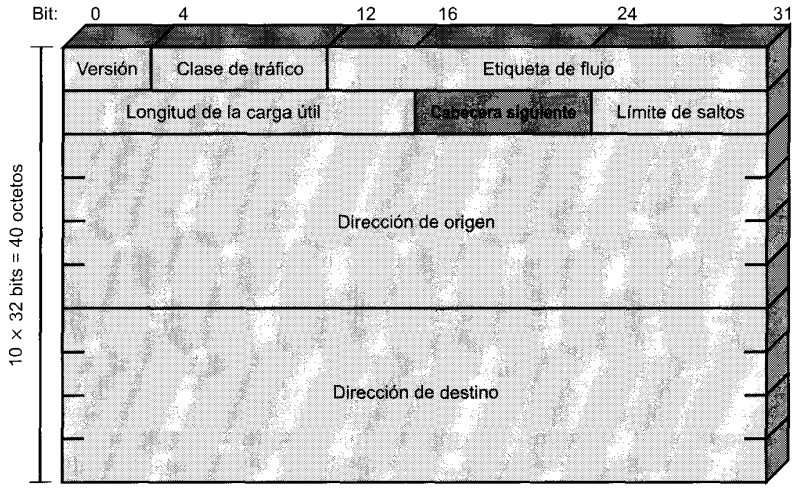


Figura 15.11. *Cabecera IPv6.*

- **Longitud de la carga útil (16 bits):** longitud del resto del paquete IPv6 excluida la cabecera, en octetos. En otras palabras, representa la longitud total de todas las cabeceras de extensión más la PDU de la capa de transporte.
- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.
- **Límite de saltos (8 bits):** el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado, y se decrementa en 1 en cada nodo que reenvía el paquete. El paquete se descarta si el límite de saltos se hace cero. Esto es una simplificación del procesamiento requerido por el campo tiempo-de-vida de IPv4. El consenso fue que el esfuerzo extra de contabilizar los intervalos de tiempo en IPv4 no incorporaba un valor significativo al protocolo.
- **Dirección origen (128 bits):** dirección del productor del paquete.
- **Dirección destino (128 bits):** dirección de destino deseado del paquete. Puede que éste no sea en realidad el último destino deseado si está presente la cabecera de encaminamiento, como se explicará después.

Aunque la cabecera IPv6 es más grande que la parte obligatoria de la cabecera IPv4 (40 octetos frente a 20 octetos), contiene menos campos (8 frente 12). Así, los dispositivos de encaminamiento tienen que hacer menos procesamiento por paquete, lo que agiliza el encaminamiento.

Clase de tráfico

El campo de clase de tráfico de 8 bits permite a una fuente identificar las características en el tratamiento de tráfico que desea cada paquete relativos a otros paquetes de la misma fuente. La intención es permitir varias formas de servicios diferenciados, como se discute en el Capítulo 16. Cuando se estaba escribiendo este libro, todavía no se había especificado el uso de este campo. El RFC 2466 ofrece las siguientes directrices:

- La interfaz de servicio con IPv6 debe permitir a los protocolos de la capa superior proporcionar el valor del campo de clase de tráfico.
- Los nodos que permitan un uso específico del campo de clase de tráfico se les permite cambiar el valor de estos bits en los paquetes que ellos originan, reenvían o reciben, de acuerdo a como se requiera para ese uso específico.
- Un protocolo de la capa superior no debe suponer que el valor de los bits de clase de tráfico en un paquete recibido es el mismo que el valor enviado por la fuente del paquete.

Etiqueta de flujo

El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen particular a un destino particular (monodistribución o multidistribución) y para el que el origen desea un tratamiento especial por parte de los dispositivos de encaminamiento. Un flujo está unívocamente identificado por la combinación de una dirección origen y una etiqueta de flujo de 20 bits distinta de cero. Así, todos los paquetes que van a formar parte del mismo flujo tienen asignada por el origen la misma etiqueta de flujo.

Desde el punto de vista del origen, un flujo será normalmente una secuencia de paquetes que se generan por una única aplicación en el origen y tienen los mismos requisitos del servicio de transferencia. Un flujo puede estar compuesto de una única conexión TCP o incluso de varias; un ejemplo de este último caso es una aplicación de transferencia de ficheros. Una única aplicación puede generar un único

flujo o varios flujos. Un ejemplo de este último caso es la conferencia multimedia, que podría tener un flujo para audio y otro para ventanas gráficas, cada una con diferentes requisitos de transmisión en términos de razón de datos, retardo y variación del retardo.

Desde el punto de vista de los dispositivos de encaminamiento, un flujo es una secuencia de paquetes que comparten atributos que afectan a cómo deben ser tratados por el dispositivo de encaminamiento. Éstos incluyen atributos de camino, asignación de recursos, requisitos sobre cómo descartar, contabilidad de paquetes transmitidos y de seguridad. El dispositivo de encaminamiento puede tratar los paquetes de diferentes flujos de forma diversa, incluyendo la asignación de diferentes tamaños de memoria temporal, dando diferente precedencia en términos de reenvío y solicitando de las redes diferentes cualidades de servicio.

Ninguna etiqueta de flujo tiene un significado especial; en consecuencia, el tratamiento especial que se ha de dar al flujo de paquetes se debe declarar de alguna forma. Por ejemplo, un origen podría negociar o solicitar a los dispositivos de encaminamiento un determinado tratamiento de forma anticipada por medio de un protocolo de control, o en el momento de la transmisión, mediante información insertada en alguna de las cabeceras de extensión del paquete, como puede ser en cabecera de opciones de salto-a-salto. Como ejemplo de tratamiento especial que se podría solicitar está el de algunos tipos de servicio que no están establecidos implícitamente como alguna forma de servicio en tiempo real.

En principio, todos los requisitos de un usuario para un flujo particular se podrían definir en una cabecera de extensión e incluirla en todos los paquetes. Si queremos dejar el concepto de flujo abierto para incluir una gran variedad de requisitos, esta técnica de diseño daría lugar a cabeceras de paquete muy grandes. La alternativa, adoptada por IPv6, es la etiqueta de flujo, en la que los requerimientos de flujo se definen antes de comenzar el flujo y se asigna al flujo una única etiqueta de flujo. En este caso, el dispositivo de encaminamiento debe guardar la información sobre los requisitos de flujo de cada flujo.

Se aplican las siguientes reglas a las etiquetas de flujo:

1. Los computadores o los dispositivos de encaminamiento que no soportan el campo de etiqueta de flujo deben poner a cero este campo cuando generan un paquete, no cambiar el campo cuando reenvían un paquete e ignorar el campo cuando reciben un paquete.

2. Todos los paquetes producidos en un origen dado con la misma etiqueta de flujo distinta de cero deben tener la misma dirección destino, dirección origen, el mismo contenido de la cabecera de opciones salto-a-salto (si esta cabecera se encuentra presente) y el mismo contenido en la cabecera de encaminamiento (si esta cabecera está presente). La intención es que un dispositivo de encaminamiento pueda decidir cómo encaminar y procesar el paquete simplemente buscando la etiqueta de flujo en una tabla y sin examinar el resto de la cabecera.

3. El origen asigna a cada flujo una etiqueta de flujo. Las etiquetas de flujo nuevas se deben elegir (seudo)aleatoriamente y uniformemente en el rango 1 a $2^{20} - 1$, teniendo en cuenta la restricción de que el origen no puede reutilizar una etiqueta de flujo para un flujo nuevo en el tiempo de vida del flujo existente. La etiqueta de flujo cero se reserva para indicar que no se está utilizando etiqueta de flujo.

Este último punto requiere alguna aclaración adicional. El dispositivo de encaminamiento debe mantener, presumiblemente en algún tipo de tabla, la información sobre las características de cada flujo activo que puede pasar por él. Para que sea capaz de reenviar los paquetes eficiente y rápidamente, la búsqueda en la tabla ha de ser eficiente. Una alternativa es tener una tabla con 2^{20} (sobre 16 millones) elementos, uno por cada etiqueta de flujo posible; esto impone una capacidad de memoria innecesaria en el dispositivo de encaminamiento. Otra alternativa es tener un elemento en la tabla por cada flujo activo, que incluya la etiqueta de flujo lo que requiere que el dispositivo de encaminamiento busque en la tabla entera cada vez que le llega un paquete. Esto impone una carga de procesamiento innecesaria en el dispositivo de encaminamiento. En lugar de esto, en la mayoría de los diseños de dispositivo de enca-

minamiento frecuentemente utilizan algún tipo de tabla de dispersión (hash). Con este enfoque se utiliza una tabla de tamaño moderado, y a cada flujo se le asigna un elemento de la tabla utilizando una función de mezcla de la etiqueta de flujo. Esta función de mezcla podría ser simplemente extraer los bits menos significativos (por ejemplo los 10 o 12 bits más bajos) de la etiqueta de flujo o algún cálculo sencillo con los 20 bits de la etiqueta de flujo. En cualquier caso, la eficiencia del planteamiento de funciones de mezcla normalmente depende de que las etiquetas de flujo estén distribuidas uniformemente en su rango posible (de aquí el requisito número 3 indicado anteriormente).

DIRECCIONES IPv6

Las direcciones de IPv6 tienen una longitud de 128 bits. Las direcciones se asignan a interfaces individuales en los nodos, no a los nodos mismos[3]. Una única interfaz puede tener múltiples direcciones únicas. Cualquiera de las direcciones asociadas a las interfaces de los nodos se puede utilizar para identificar de forma única al nodo.

La combinación de direcciones largas y direcciones múltiples por interfaz permite un eficiencia mejorada del encaminamiento con respecto a IPv4. En IPv4, generalmente las direcciones no tienen una estructura que ayude al encaminamiento y por lo tanto un dispositivo de encaminamiento necesita mantener un gran tabla con rutas de encaminamiento. Una dirección internet más grande permite agrupar las direcciones por jerarquías de red, por proveedores de acceso, por proximidad geográfica, por institución, etc. Estas agrupaciones deben conducir a tablas de encaminamiento más pequeñas y a tablas de consulta más rápidas. El permitir múltiples direcciones por interfaz posibilita a un subscriptor, que utiliza varios proveedores de acceso a través del mismo interfaz, tener direcciones distintas agrupadas bajo el espacio de direcciones de cada proveedor.

IPv6 permite tres tipos de direcciones:

- **Unidistribución (unicast):** un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- **Monodistribución (anycast):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección monodistribución se entrega a una de las interfaces identificadas por esa dirección (la más cercana, de acuerdo a la medida de distancia del protocolo de encaminamiento).
- **Multidistribución (multicast):** un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multidistribución se entrega a todas las interfaces identificadas por esa dirección.

CABECERA DE OPCIONES SALTO-A-SALTO

La cabecera de opciones salto-a-salto lleva información opcional que, si está presente, debe ser examinada por cada dispositivo de encaminamiento a lo largo del camino. Esta cabecera contiene los siguientes campos (Figura 15.12a):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecera de extensión (8 bits):** longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Opciones:** campo de longitud variable que consta de una o más definiciones de opción. Cada definición se expresa mediante tres subcampos: tipo de opción (8 bits), que identifica la opción; longitud (8 bits), que especifica la longitud en octetos del campo de datos de la opción; y datos de opción, que es una especificación de la opción de longitud variable.

[3] En IPv6, un nodo es cualquier dispositivo que implemente IPv6; esto incluye a los computadores y dispositivos de encaminamiento.

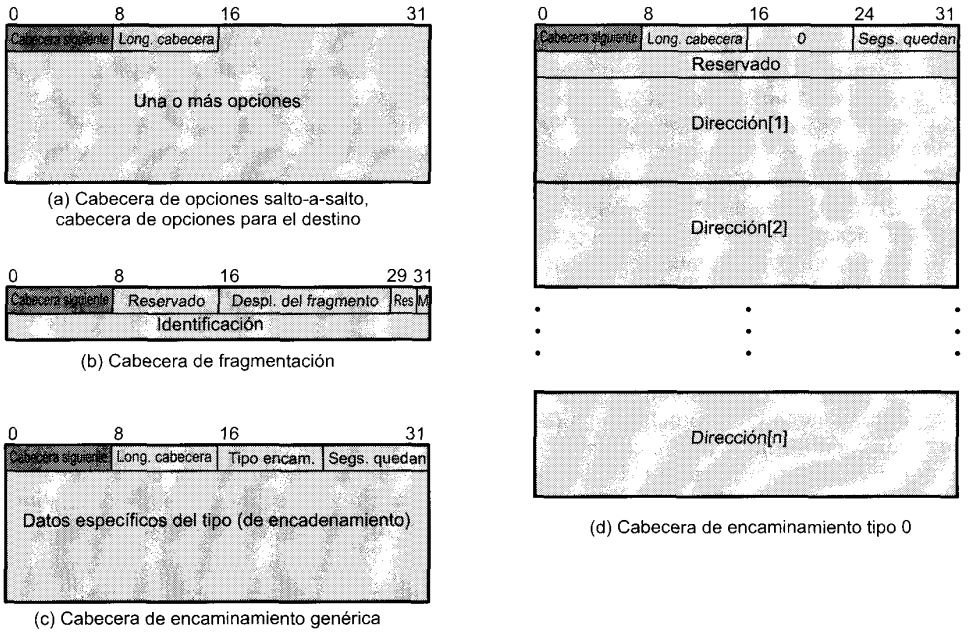


Figura 15.12. Cabeceras de extensión IPv6.

En realidad se utilizan los cinco bits menos significativos del campo tipo de opción para especificar una opción particular. Los bits más significativos indican la acción que tiene que realizar un nodo que no reconoce el tipo de opción, de acuerdo a:

- 00—ignorar esta opción y continuar procesando la cabecera.
- 01—descartar el paquete.
- 10—descartar el paquete y enviar un mensaje ICMP de problema de parámetro, código 2, a la dirección origen del paquete, indicando el tipo de opción no reconocida.
- 11—descartar el paquete y, solamente si la dirección destino el paquete no es una dirección multidistribución, enviar un mensaje ICMP de problema de parámetro, código 2, a la dirección origen del paquete, indicando el tipo de opción no reconocida.

El tercer bit especifica si el campo de datos de la opción no cambia (0) o si puede cambiar (1) en el camino desde el origen al destino. Los datos que pueden cambiar se deben excluir de los cálculos de autentificación, como se discutirá en el Capítulo 18.

Estas convenciones para el campo del tipo de opción también se aplican a la cabecera de opciones en el destino.

En el estándar IPv6, hasta ahora sólo se han especificado dos opciones: la opción de carga útil Jumbo y la opción de alerta al dispositivo de encaminamiento. La opción de carga útil Jumbo se utiliza para enviar paquetes con una carga útil mayor de 65.535 octetos. El campo de datos de esta opción tiene una longitud de 32 bits y da la longitud del paquete en octetos, excluyendo la cabecera IPv6. Para estos paquetes el campo de longitud de la carga en la cabecera IPv6 debe de estar a cero y no puede haber cabecera de fragmentación. Con esta opción, IPv6 permite tamaños de paquete de hasta 4.000 millones de octetos. Esto facilita la transmisión de paquetes de vídeo grandes y habilita a IPv6 a hacer el mejor uso de la capacidad disponible a través de cualquier medio de transmisión.

La opción de alerta al dispositivo de encaminamiento, cuando está presente, informa al dispositivo de encaminamiento que el contenido de este paquete es de interés para el dispositivo de encaminamiento y para tratar adecuadamente cualquier información de control. La ausencia de esta opción en un datagrama IPv6 informa al dispositivo de encaminamiento que el paquete no contiene información necesaria para el dispositivo de encaminamiento y por tanto puede encaminarlo de forma segura sin ningún análisis adicional. Los computadores que originan paquetes IPv6 se les obliga a que incluyan esta opción en ciertas circunstancias. El motivo de esta opción es proporcionar un apoyo suficiente a protocolos como RSVP (descrito en el Capítulo 16) que generan paquetes que necesitan ser examinados por dispositivos de encaminamiento intermedios por motivos de control de tráfico. En lugar de requerir a los dispositivos de encaminamiento intermedios que analicen en detalle la cabecera de extensión, esta opción alerta al dispositivo de encaminamiento cuando se requiere esta atención.

CABECERA DE FRAGMENTACIÓN

En IPv6, la fragmentación sólo puede ser realizada por el nodo origen, no por los dispositivos de encaminamiento a lo largo del camino del paquete. Para obtener las ventajas completas del entorno de interconexión, un nodo debe ejecutar un algoritmo de obtención de la ruta, lo que permite conocer la unidad máxima de transferencia (MTU, Maximun Transfer Unit) permitida por cada red en la ruta. Con este conocimiento, el nodo origen fragmentará, según se requiera, para cada dirección destino dada. Si no se ejecuta este algoritmo, el origen debe limitar todos los paquetes a 1.280 octetos, que debe ser la mínima MTU que permitan las redes.

La cabecera de fragmentación contiene los siguientes campos (Figura 15.12b):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Reservado (8 bits):** para usos futuros.
- **Desplazamiento del fragmento (13 bits):** indica donde se sitúa en el paquete original la carga útil de este fragmento. Se mide en unidades de 64 bits. Esto implica que los fragmentos (excepto el último) deben contener un campo de datos con una longitud múltiplo de 64 bits.
- **Reservado (2 bits):** reservado para usos futuros.
- **Indicador M (1 bit):** 1 = más fragmentos; 0 = último fragmento.
- **Identificación (32 bits):** utilizado para identificar de forma única el paquete original. El identificador debe ser único para la dirección origen, dirección destino y para el valor de la siguiente cabecera del paquete durante el tiempo que el paquete permanece en Internet.

El algoritmo de fragmentación es el mismo que el descrito en la Sección 15.1.

CABECERA DE ENCAMINAMIENTO

La cabecera de encaminamiento contiene una lista de uno o más nodos intermedios por los que se pasa en el camino del paquete a su destino. Todas las cabeceras de encaminamiento comienzan con un bloque de 32 bits consistente en 4 campos de 8 bits, seguido por datos de encaminamiento específicos al tipo de encaminamiento dado (Figura 15.12c). Los cuatro campos de 8 bits son los siguientes:

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que sigue inmediatamente a ésta.
- **Longitud de la cabecera de extensión (8 bits):** longitud de esta cabecera en unidades de 64 bits, sin incluir los primeros 64 bits.
- **Tipo de encaminamiento (8 bits):** identifica una variante particular de cabecera de encaminamiento. Si un dispositivo de encaminamiento no reconoce el valor del tipo de encaminamiento, debe descartar el paquete.
- **Segmentos que quedan (8 bits):** número de segmentos en la ruta que quedan; esto es, el número explícito de nodos intermedios en lista que se visitarán todavía antes de alcanzar el destino.

El único formato de cabecera de tipo encaminamiento explícito, definido en el RFC 2460, es el la cabecera de encaminamiento Tipo 0 (Figura 15.12d). Cuando se utiliza una cabecera de encaminamiento Tipo 0, el nodo origen no sitúa la dirección del último destino en la cabecera IPv6. En lugar de eso, esa dirección es la última de la lista en la cabecera de encaminamiento (Address[*n*], en la Figura 15.12d), y la cabecera IPv6 contiene la dirección destino del primer dispositivo de encaminamiento deseado en el camino. La cabecera de encaminamiento no se examina hasta que el paquete llega al nodo identificado por la cabecera IPv6. En ese punto, el paquete IPv6 y el contenido de la cabecera se actualizan y el paquete se reenvía. La actualización consiste en situar la siguiente dirección a visitar en la cabecera IPv6 y decrementar el campo segmentos que quedan en la cabecera de encaminamiento.

CABECERA DE OPCIONES PARA EL DESTINO

La cabecera de opciones para el destino lleva información opcional que, si está presente, se examina por el nodo destino del paquete. El formato de esta cabecera es el mismo que la cabecera de opciones salto-a-salto (Figura 15.12a).

15.5. MULTIDIFUSIÓN

Normalmente, una dirección IP hace referencia a un computador individual en una red particular. IP también permite direcciones que hacen referencia a un grupo de computadores en una o más redes. Tales direcciones se conocen como direcciones de multidifusión y el hecho de enviar un paquete desde un origen a los miembros de un grupo de multidifusión se conoce como multidifusión.

La multidifusión tiene una serie de aplicaciones prácticas. Por ejemplo:

- **Multimedia**: un grupo de usuarios se conectan a una transmisión de vídeo o audio desde una estación multimedia origen.
- **Teleconferencia**: un grupo de estaciones de trabajo forman un grupo de multidifusión de forma que una transmisión desde cualquier miembro del grupo se recibe por el resto de miembros del grupo.
- **Bases de datos**: todas las copias de un fichero o base de datos duplicados se actualizan al mismo tiempo.
- **Computación distribuida**: los resultados intermedios se envían a todos los participantes.
- **Grupo de trabajo en tiempo real**: los ficheros, gráficos y mensajes se intercambian entre todos los miembros activos en tiempo real.

La multidifusión realizada dentro del ámbito de un único segmento LAN es directa. El protocolo IEEE 802 y otros protocolos LAN incluyen direcciones que permiten la multidifusión a nivel MAC. Un paquete con una dirección multidifusión se transmite en un segmento LAN. Aquellas estaciones que son miembros del grupo de multidifusión correspondiente reconocen la dirección de multidifusión y aceptan el paquete. En este caso, sólo se transmite una copia del paquete. Esta técnica funciona debido a la naturaleza de difusión de una LAN: una transmisión desde cualquier estación se recibe por todas las estaciones en la LAN.

En un entorno de un conjunto de redes, la multidifusión es un poco más difícil de acometer. Para ver esto considere la configuración de la Figura 15.13; se tienen un determinado número de LAN interconectadas por dispositivos de encaminamiento. Los dispositivos de encaminamiento están conectados entre sí mediante un enlace de alta velocidad o a través de una red de área extensa (red N4). A cada enlace y red se le asocia un coste en cada dirección, indicado por el valor mostrado en dirección hacia el

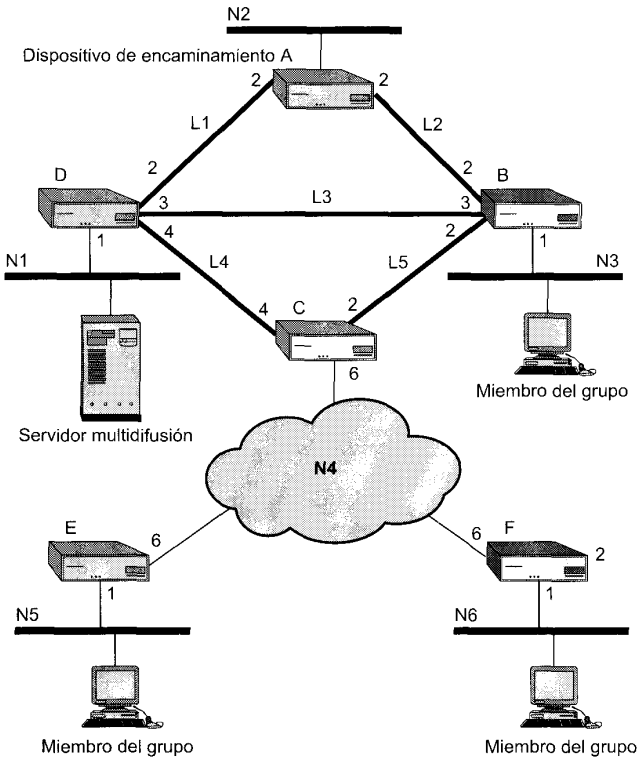


Figura 15.13. Ejemplo de configuración.

enlace o la red. Suponga que un servidor de multidifusión en la red N1 está transmitiendo paquetes a una dirección de multidifusión que representa las estaciones de trabajo en las redes N3, N4 y N6. Suponga que el servidor no conoce la localización de los miembros del grupo de multidifusión. Entonces una forma de asegurar que el paquete lo reciben todos los miembros del grupo es **difundir** una copia de cada paquete en cada red en la configuración sobre la ruta de menor coste para cada red. Por ejemplo, un paquete se mandaría a N3 y atravesaría N1, el enlace L3 y N3. El dispositivo de encaminamiento B es responsable de traducir la dirección multidifusión a nivel IP en una dirección de multidifusión a nivel MAC antes de transmitir la trama MAC en N3. La Tabla 15.4 resume el número de paquetes generados en los diferentes enlaces y redes para transmitir un paquete a un grupo multidifusión con este método. Se necesitan un total de 13 copias del paquete.

Suponga ahora que el sistema fuente conoce la localización de cada miembro del grupo de multidifusión. Esto es, la fuente tiene una tabla que traduce la dirección de multidifusión en una lista de redes que contienen a los miembros del grupo. En este caso, la fuente necesita solamente enviar los paquetes a aquellas redes que contienen los miembros del grupo.

Vamos a denominar a esta técnica como estrategia **monodistribución múltiple**. La Tabla 15.4 muestra que en este caso se necesitan 11 paquetes.

Ambas estrategias, difusión y monodistribución múltiple, son ineficientes ya que generan copias innecesarias del paquete origen. En una estrategia **multidifusión** verdadera se utiliza el siguiente método:

Tabla 15.4. Tráfico generado por varias estrategias de multidifusión

	Difusión					Monodifusión múltiple				Multidifusión
	S → N2	S → N3	S → N5	S → N6	Total	S → N3	S → N5	S → N6	Total	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3		1			1	1			1	1
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6				1	1			1	1	1
L1	1				1					
L2										
L3		1			1	1			1	1
L4			1	1	2		1	1	2	1
L5										
Total	2	3	4	4	13	3	4	4	11	8

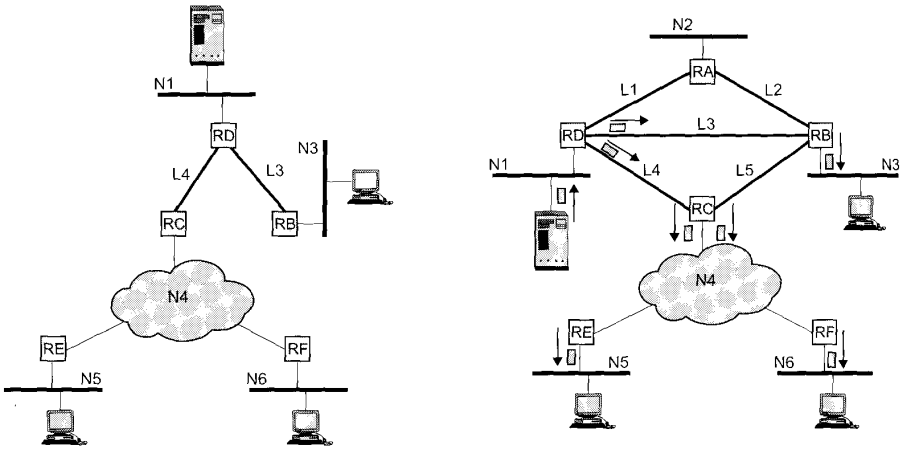
1. Se determina el camino de menor coste desde el origen a cada red que incluya miembros del grupo de multidifusión. Esto resulta en un árbol de expansión[4] de la configuración. Hay que darse cuenta que no es un árbol de expansión de la configuración completa. En su lugar, es un árbol de expansión que incluye sólo aquellas redes que contienen miembros del grupo.
2. La fuente transmite un único paquete a través del árbol de expansión.
3. El paquete sólo se duplica por los dispositivos de encaminamiento en los puntos de bifurcación en el árbol de expansión.

La Figura 15.14a muestra el árbol de expansión para la transmisión desde el origen al grupo de multidifusión, y la Figura 15.14b muestra este método en acción. El origen transmite un único paquete sobre N1 al dispositivo de encaminamiento D. D hace dos copias del paquete para transmitirlo sobre los enlaces L3 y L4. B recibe el paquete sobre L3 y lo transmite en N3, donde es recibido por los miembros del grupo de multidifusión en esa red. Mientras tanto, C recibe el paquete enviado en L4. Él debe entregar el paquete a E y F. Si N4 fuera una red de difusión (por ejemplo, una LAN IEEE 802), C sólo tendría que transmitir una copia del paquete para ambos dispositivos de encaminamiento. Si N4 es una red WAN de conmutación de paquetes, C debe hacer dos copias y direccionar uno a E y el otro a F. Cada uno de estos dispositivos de encaminamiento, de nuevo, retransmiten el paquete recibido en N5 y N6, respectivamente. Como muestra la Tabla 15.4, la técnica de multidifusión sólo requiere 8 copias del paquete.

REQUISITOS PARA LA MULTIDIFUSIÓN

En una transmisión ordinaria a un solo computador en un conjunto de redes, en la que cada datagrama tiene una red destino única, la tarea del dispositivo de encaminamiento es reenviar el datagrama por el camino más corto desde ese dispositivo de encaminamiento hasta la red destino. Con una transmisión multidifusión, el dispositivo de encaminamiento podría reenviar una o más copias de un datagrama que le llega. En nuestro ejemplo, los dispositivos de encaminamiento D y C deben reenviar dos copias de un único datagrama que les llega.

[4] El concepto del árbol de expansión fue introducido en nuestra discusión de los puentes en el Capítulo 13. Un árbol de expansión de un grafo consiste en todos los nodos del grafo más un subconjunto de enlaces (arcos) del grafo que proporciona conectividad (existe un camino entre cualquier par de nodos) sin lazos cerrados (existe sólo un camino entre cualquier par de nodos).



(a) Árbol de expansión desde la fuente al grupo multidifusión

(b) Paquetes generados por la transmisión multidifusión

Figura 15.14. Ejemplo de transmisión multidifusión.

De esta forma, es de esperar que la funcionalidad global del encaminamiento multidifusión es mucho más compleja que el encaminamiento a un solo destino. A continuación se da una lista de las funciones que se requieren:

1. Se necesita un convenio para identificar las direcciones de multidifusión. En IPv4 se reserva la clase D de direcciones para este propósito. Éstas son direcciones de 32 bits con los 4 bits más significativos puestos a un valor de 1110 seguidos por un identificador de grupo de 28 bits. En IPv6, una dirección de 128 bits de multidifusión consiste de un prefijo de 8 bits todos 1, un campo de indicadores de 4 bits, un campo de ámbito de 4 bits y un identificador de grupo de 112 bits. El campo de indicadores, actualmente, sólo indica si la dirección está asignada permanentemente o no. El campo de ámbito indica el ámbito de aplicabilidad de la dirección, un rango que va desde una única red a la red global.

2. Cada nodo (un dispositivo de encaminamiento o fuente participando en el algoritmo de encaminamiento) debe traducir una dirección IP multidifusión a la lista de redes que contienen los miembros de este grupo. Esta información permite al nodo construir el árbol de expansión de los caminos más cortos de todas las redes que contienen miembros del grupo.

3. Un dispositivo de encaminamiento debe traducir una dirección IP multidifusión a una dirección multidifusión para poder entregar un datagrama IP multidifusión en la red destino. Por ejemplo, en redes IEEE 802, la dirección a nivel MAC es de 48 bits. En ambos casos, si el bit más significativo es 1, entonces es una dirección de multidifusión. De esta forma, para una entrega multidifusión, el dispositivo de encaminamiento conectado a una red IEEE 802 debe traducir una dirección multidifusión IPv4 de 32 bits o IPv6 de 128 bits en una dirección multidifusión IEEE de 48 bits de nivel MAC.

4. Aunque algunas direcciones de multidifusión se pueden asignar permanentemente, el caso más general es que estas direcciones se generen dinámicamente y que los computadores individuales puedan unirse o abandonar los grupos multidifusión dinámicamente. Por lo tanto, se necesita un mecanismo por el que un computador individual informe al dispositivo de encaminamiento conectado en su misma red de una inclusión o exclusión de un grupo multidifusión.

5. Los dispositivos de encaminamiento deben de intercambiar dos tipos de información. Primero, los dispositivos de encaminamiento necesitan saber qué redes incluyen miembros de un grupo de multidifusión determinado. Segundo, los dispositivos de encaminamiento necesitan suficiente información para calcular los caminos más cortos a cada red que contiene miembros del grupo. Estos requisitos implican la necesidad de un protocolo de encaminamiento.
6. Se necesita un algoritmo de encaminamiento para calcular los caminos más cortos a todos los miembros del grupo.
7. Cada dispositivo de encaminamiento debe determinar los caminos de encaminamiento multidifusión sobre la base de las direcciones de la fuente y el destino.

El último punto es una consecuencia sutil de la utilización de las direcciones de multidifusión. Para ilustrar este punto, considere de nuevo la Figura 15.13. Si el servidor de multidifusión transmite un paquete ordinario dirigido a un computador en la red N5, el dispositivo de encaminamiento D envía el paquete a C, que reenvía el paquete a E. De forma similar, un paquete dirigido a un computador en la red N3, D lo envía a B. Pero ahora suponga que el servidor transmite un paquete con una dirección de multidifusión que incluye computadores en N3, N5 y N6. Como se ha discutido, D hace dos copias del paquete y envía una a B y otra a C. Hasta aquí todo bien. Pero, ¿qué hará C cuando reciba un paquete con una dirección multidifusión? C sabe que este paquete va dirigido a las redes N3, N5 y N6. Un esquema simple sería que C calcule los caminos más cortos a cada una de estas tres redes. Esto produce el árbol de expansión de caminos más cortos mostrado en la Figura 15.15. Como resultado C envía dos copias del paquete por la red N4, uno dirigido a la red N5 y otro para la red N6. Pero también envía una copia del paquete a B para su entrega en N3. De esta forma B recibirá dos copias del paquete, una de D y otra de C. Ésta no es claramente lo que intentaba hacer el computador en N1 cuando emitió el paquete.

Para evitar duplicidades innecesarias de paquetes, cada dispositivo de encaminamiento debe encaminar paquetes sobre la base de ambas, la fuente y el destino multidifusión. Cuando C recibe un paquete dirigido a un grupo de multidifusión desde una fuente en N1, él debe calcular el árbol de expansión con N1 como raíz (mostrado en la Figura 15.14a) y encaminar según este árbol de expansión.

PROTOCOLO DE GESTIÓN DE GRUPOS DE INTERNET (IGMP)

IGMP (del inglés, Internet Group Management Protocol), definido en el RFC 1112, se utiliza tanto por los dispositivos de encaminamiento como por los computadores para intercambiar información de miembros de grupos de multidifusión sobre una LAN. IGMP hace uso de la naturaleza de difusión de una LAN para proporcionar una técnica eficiente para el intercambio de información entre múltiples computadores y dispositivos de encaminamiento.

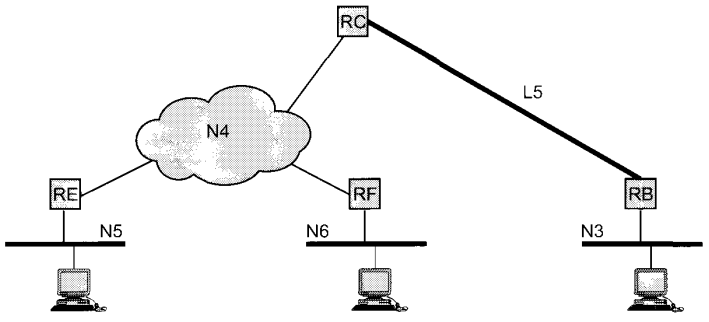


Figura 15.15. Árbol de expansión desde el dispositivo de encaminamiento C al grupo multidifusión.

Formato del mensaje IGMP

Todos los mensajes IGMP se transmiten en datagramas IP y tienen el formato que se muestra en la Figura 15.16. Los campos de los que consta son los siguientes:

- **Versión:** versión del protocolo, igual a 1.
- **Tipo:** existen dos tipos: el Tipo 1 especifica una petición solicitada por un dispositivo de encaminamiento de multidifusión. El Tipo 2 especifica un informe enviado por un computador.
- **Suma de comprobación:** un código de detección de errores calculado como la suma complemento a uno de todas las 4 palabras de 16 bits en este mensaje. Por motivos de cálculo, este campo se inicializa a sí mismo a un valor de todo cero. Es el mismo algoritmo de comprobación que el utilizado en IPv4.
- **Dirección de grupo:** valor cero en un mensaje de solicitud y una dirección de grupo válida en un mensaje de informe.

Funcionamiento de IGMP

El objetivo de que un computador utilice IGMP es hacerse conocer como un miembro de un grupo con una dirección de multidifusión dada a otros computadores en la LAN y a todos los dispositivos de encaminamiento en la LAN. Para unirse a un grupo, un computador envía un mensaje de informe, en el cual el campo de dirección de grupo es la dirección multidifusión del grupo. Este mensaje se envía en un datagrama IP con la misma dirección multidifusión destino. En otros palabras, el campo dirección de grupo del mensaje IGMP y el campo dirección destino de la cabecera del datagrama IP son el mismo. Todos los computadores que son miembros actuales de este grupo de multidifusión reciben el mensaje y tienen conocimiento del nuevo miembro del grupo. Cada dispositivo de encaminamiento conectado en la LAN debe atender a todas las direcciones IP de multidifusión para poder recibir todos los informes.

Para mantener una lista actual válida de las direcciones de grupos activos, un dispositivo de encaminamiento de multidifusión emite periódicamente mensajes de petición dentro de un datagrama IP con dirección de multidifusión *todos-los-computadores*. Cada computador que todavía quiere permanecer como miembro de uno o más grupos de multidifusión debe atender los datagramas con dirección todos-los-computadores. Cuando un computador de éstos recibe una solicitud debe responder con un mensaje de informe para cada grupo al cual reclama su pertenencia.

Hay que darse cuenta de que el dispositivo de encaminamiento de multidifusión no necesita conocer la identidad de cada computador en un grupo. En lugar de eso, necesita saber que existe al menos un miembro del grupo todavía activo. Por lo tanto, cada computador en un grupo que recibe una petición establece un temporizador con un retardo aleatorio. Cada computador que oye a otro computador reclamando la pertenencia a un grupo cancela su propio informe. Si no oye ningún informe y expira el temporizador, el computador envía un informe. Con este esquema, solamente un miembro de cada grupo proporciona un informe al dispositivo de encaminamiento de multidifusión.

Pertenencia a grupos en IPv6

IGMP se definió para operar con IPv4 y hace uso de direcciones de 32 bits. La misma funcionalidad se requiere para redes IPv6. En lugar de definir una versión separada de IGMP para IPv6, su función se ha

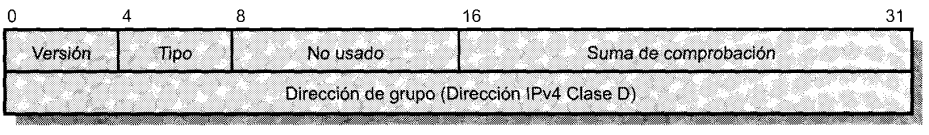


Figura 15.16. Formato del mensaje IGMP.

incorporado en la nueva versión del protocolo de mensajes de control de Internet (ICMPv6). ICMPv6 incluye toda la funcionalidad de ICMPv4 e IGMP. Para permitir la multidifusión, ICMPv6 incluye un mensaje de solicitud de pertenencia a grupo y un mensaje de informe de pertenencia a grupo, que se utiliza en la misma forma que IGMP. Además, existe un mensaje nuevo de terminación de la pertenencia a grupo, que permite que un computador anuncie que deja un grupo.

15.6. LECTURAS RECOMENDADAS Y PÁGINAS WEB

[MURP98] proporciona un tratamiento completo y claro de todos los tópicos tratados en este capítulo. En [COME95] y [STEV94] se puede encontrar un buen estudio sobre interconexión entre redes y sobre IPv4. [HUIT98] es una descripción técnica directa de varios RFC que integran juntos la especificación de IPv6; el libro proporciona una discusión del propósito de varias características y el funcionamiento del protocolo. [MILL98] trata cuestiones más prácticas y de implementación de IPv6. [KESH98] proporciona un repaso instructivo a la funcionalidad presente y futura de los dispositivos de encaminamiento.

BRAD96 Bradner, S., y Mankin, A. *IPng: Internet Protocol Next Generation.* Reading, MA: Addison-Wesley, 1996.

COME95 Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Englewood Cliffs, NJ: Prentice Hall, 1995.

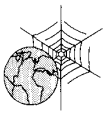
HUIT98 Huitema, C. *IPv6: The New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall, 1998.

KESH98 Keshav, S., y Sharma, R. «Issues and Trends in Router Design.» *IEEE Communications Magazine*, May 1998.

MILL98 Miller, S. *IPv6: The Next Generation Internet Protocol.* Bedford, MA: Digital Press, 1008.

MURH98 Murhammer, M., et. al. TCP/IP: *Tutorial and Technical Overview.* Upper Saddle River: NJ: Prentice Hall, 1998.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.



SITIOS WEB RECOMENDADOS

- **IPng:** información sobre IPv6 y temas relacionados.
- **Iniciativa de multidifusión IP:** un grupo de vendedores dedicado a la promoción de la multidifusión IP. Esta página web incluye artículos técnicos, información sobre vendedores y productos y el estado de la actividad de estandarización.

15.7. PROBLEMAS

15.1. En la discusión sobre IP, se mencionó que el *identificador*, el *indicador de no fragmentar* y el *tiempo de vida* se hallan presentes en la primitiva Send pero no en la primitiva Deliver ya que esos parámetros no son competencia de IP. Para cada una de estas primitivas indique si es competencia de la entidad IP en el origen, de la entidad IP en cada dispositivo de encaminamiento intermedio o de la entidad IP en el sistema final destino. Justifique su respuesta.

15.2. ¿Cuáles son los pros y los contras del reensamblado intermedio de un datagrama fragmentado frente al reensamblado en el destino final?

15.3. ¿Cuál es la información suplementaria de la cabecera en el protocolo IP?

15.4. Describa algunas circunstancias en las que sería deseable utilizar encaminamiento por la fuentes en lugar de dejar a los dispositivos de encaminamiento que realicen la decisión de encaminamiento.

15.5. A causa de la fragmentación, un datagrama IP puede llegar en varios trozos, no necesariamente en el orden adecuado. La entidad IP en el sistema final receptor debe acumular estos fragmentos hasta que se reconstruya el datagrama original.

a) Considere que la entidad IP crea una memoria temporal para reensamblar el campo de datos del datagrama original. Conforme se va realizando el reensamblado, la memoria temporal contendrá bloques de datos y zonas vacías («agujeros») entre los bloques de datos. Describa un algoritmo para reensamblar datagramas basado en este concepto.

b) Para el algoritmo de la parte (a) es necesario hacer un seguimiento a los agujeros. Describa un mecanismo sencillo para hacer esto.

15.6. Un datagrama de 4.480 octetos se va a transmitir y se necesita fragmentar ya que va a pasar por una red Ethernet con un campo máximo de carga útil de 1.500 octetos. Mostrar los valores de los campos longitud total, indicador de más, y desplazamiento de fragmento en cada uno de los fragmentos resultantes.

15.7. La suma de comprobación de IP necesita que se recalcule en los dispositivos de encaminamiento a causa de los cambios en la cabecera IP, como el que ocurre en el campo tiempo de vida. Es posible recalcular esta suma desde cero. Sugiera un procedimiento que suponga menos cálculos. *Sugerencia:* suponga que el valor en el octeto k es cambiado por Z = valor_nuevo − valor_viejo; considere el efecto de este cambio en la suma de comprobación.

15.8. Se va a segmentar un datagrama. ¿Qué opciones del campo de opción se necesitan copiar en la cabecera de cada segmento, y cuáles se necesitan copiar sólo en el primer segmento? Justificar el tratamiento de cada opción.

15.9. Un mensaje de la capa de transporte, que contiene 1.500 bits de datos y 160 bits de cabecera, se envía a la capa internet la cual incorpora otros 160 bits de cabecera. Esto se transmite a través de dos redes que utilizan cada una 24 bits de cabecera de paquete. La red destino tiene un tamaño de paquete máximo de 800 bits. ¿Cuantos bits, incluyendo cabeceras, se entregan al protocolo de la capa de red en el destino?

15.10. Se va a utilizar la arquitectura sugerida por la Figura 15.2 ¿Qué funciones se deberían añadir a los dispositivos de encaminamiento para aliviar algunos de los problemas causados por la desigualdad entre redes locales y de transporte a larga distancia?

15.11. ¿Debería existir una relación entre la interconexión entre redes y el encaminamiento interno de red? ¿Por qué sí, o por qué no?

15.12. Compare los campos individuales de la cabecera IPv4 con la cabecera IPv6. Compare las posibilidades proporcionadas por cada uno de los campos de IPv4 con los de IPv6.

15.13. Justifique el orden recomendado de las cabeceras de extensión de IPv6 (por ejemplo, ¿por qué es primera la cabecera de opciones salto-a-salto?, ¿por qué la cabecera de encaminamiento está antes que la cabecera de fragmentación?, y así hasta la cabecera final).

15.14. El estándar IPv6 afirma que si un paquete con una etiqueta de flujo distinta de cero llega a un dispositivo de encaminamiento y el dispositivo de encaminamiento no tiene información para esa etiqueta de flujo, el dispositivo de encaminamiento debería ignorar la etiqueta de flujo y reenviar el paquete.

a) ¿Cuáles son las desventajas de tratar este evento como un error, descartar el paquete y enviar un mensaje ICMP?

b) ¿Existen situaciones en las que encaminar el paquete como si su etiqueta de flujo fuera cero causará un resultado erróneo? Explíquelo.

15.15. El mecanismo de flujo de IPv6 supone que el estado asociado con una etiqueta de flujo dada se almacena en los dispositivos de encaminamiento, por lo tanto éstos saben cómo tratar los paquetes que llevan esa etiqueta de flujo. Un requisito del diseño es eliminar en los dispositivos de encaminamiento las etiquetas de flujo que no se van a utilizar más (etiquetas de flujo obsoletas).

a) Suponga que una fuente siempre envía un mensaje de control a todos los dispositivos de encaminamiento afectados suprimiendo una etiqueta de flujo cuando el origen acabe con ese flujo. En este caso, ¿cómo podría persistir una etiqueta de flujo antigua?

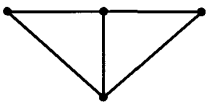
b) Sugiera mecanismos del origen y de los dispositivos de encaminamiento para superar el problema de las etiquetas de flujo antiguas.

15.16. La cuestión que se plantea es qué paquetes generados por un origen deberían llevar etiquetas de flujo IPv6 distintas de cero. Para algunas aplicaciones, la respuesta es obvia. Los intercambios pequeños de datos deberían tener una etiqueta de flujo cero, ya que no merece la pena crear un flujo para unos pocos paquetes. Los flujos en tiempo real deberían tener una etiqueta de flujo; estos flujos fueron la causa primera de que se crearan etiquetas de flujo. Una cuestión más difícil es qué hacer con entidades paritarias que están enviando una gran cantidad de tráfico con el mejor esfuerzo (por ejemplo, las conexiones TCP). Describa un caso para asignar una única etiqueta de flujo a cada conexión TCP de gran duración. Describa un caso para no hacer esto.

15.17. Las especificaciones originales de IPv6 combinaban los campos de etiqueta de flujo y prioridad en un solo campo de etiqueta de flujo de 28 bits. Esto permitía a los flujos redefinir la interpretación de los diferentes valores de prioridad. Sugiera una razón por la que la especificación final incluye un campo de prioridad en un campo distinto.

15.18. Para el encaminamiento IPv6 Tipo 0, especifique el algoritmo para actualizar las cabeceras IPv6 y de encaminamiento en los nodos intermedios.

15.19. Un grafo conectado podría tener más de un árbol de expansión. Encuentre todos los árboles de expansión de este grafo:



CAPÍTULO 16

Funcionamiento de la interconexión de redes

- Los protocolos de encaminamiento en un conjunto de redes funcionan de una forma similar a los que se utilizan en redes de conmutación de paquetes. Un protocolo de encaminamiento en un conjunto de redes se utiliza para intercambiar información sobre accesibilidad y retardos de tráfico, permitiendo a cada dispositivo de encaminamiento construir la tabla de encaminamiento del siguiente salto para los caminos a través del conjunto de redes. Normalmente, se utilizan protocolos de encaminamiento relativamente simples entre sistemas autónomos dentro de un conjunto de redes más grande y se utilizan protocolos de encaminamiento más complejos dentro de cada uno de los sistemas autónomos.
- La arquitectura de sistemas integrados es una respuesta a la creciente variedad y volumen de tráfico experimentado en Internet y las intranets. Proporciona un entorno de trabajo para el desarrollo de protocolos como RSVP para tratar tráfico multimedia/multidifusión y orientación a los fabricantes de dispositivos de encaminamiento en el desarrollo de técnicas eficientes para el tratamiento de cargas variadas.
- RSVP es un protocolo que permite a los sistemas finales reservar capacidad del conjunto de redes para el tráfico multidifusión o monodistribución. Los dispositivos de encaminamiento en la ruta multidifusión o monodistribución reservan espacio de la memoria temporal y capacidad del enlace para los flujos de paquetes que han reservado esa capacidad.
- Una arquitectura de servicios diferenciados se diseña para proporcionar una herramienta simple, fácil de utilizar y que genera poca información suplementaria para permitir un conjunto de servicios de red que se diferencian en función del rendimiento. Los servicios diferenciados se suministran mediante una etiqueta de 6 bits en la cabecera IP, que clasifica el tráfico en términos del tipo de servicio que dan los dispositivos de encaminamiento a ese tráfico.

A medida que Internet y las redes privadas crecen en tamaño, entra firmemente en escena un nuevo tipo de computador con nuevas demandas. Las aplicaciones clientes-servidor de gran volumen de tráfico están superando las conversaciones TELNET de bajo volumen de tráfico. A esto se ha unido más recientemente el tremendo volumen de tráfico de la Web, que cada vez supone un tráfico más intensivo debido a los gráficos. Actualmente las aplicaciones de voz y vídeo en tiempo real han incrementado esta carga.

Para tratar estas demandas, no es suficiente aumentar la capacidad de Internet. Se necesitan métodos efectivos y sensibles de gestión de tráfico y de control de la congestión. Históricamente, las redes basadas en IP han sido capaces de proporcionar un servicio simple de entrega del mejor esfuerzo a todas las aplicaciones que utilizan un conjunto de redes. Pero las necesidades de los usuarios han cambiado. Una compañía se ha podido gastar millones de dólares instalando una red basada en IP diseñada para transportar datos entre LAN pero encuentra que las nuevas aplicaciones en tiempo real, multimedia o de multidifusión no funcionan bien en esa configuración. El único esquema de interconexión diseñado para dar soporte desde el primer día al tráfico tradicional TCP y UDP y tráfico en tiempo real es ATM. Sin embargo, la confianza en ATM significa, o bien construir una segunda infraestructura de interconexión para el tráfico en tiempo real o reemplazar la configuración existente basada en IP por ATM, siendo ambas alternativas costosas.

De esta forma, existe una fuerte necesidad de ser capaz de soportar una gran diversidad de tráfico con una gran variedad de requisitos en cuanto a calidad del servicio (QoS, Quality-of-Service) dentro de una arquitectura TCP/IP. Este capítulo examina las funciones y servicios de interconexión de redes diseñados para satisfacer esta necesidad.

El capítulo empieza con la cuestión de los algoritmos de encaminamiento para la interconexión. A continuación, se examina la arquitectura de servicios integrados (ISA), que proporciona un entorno de

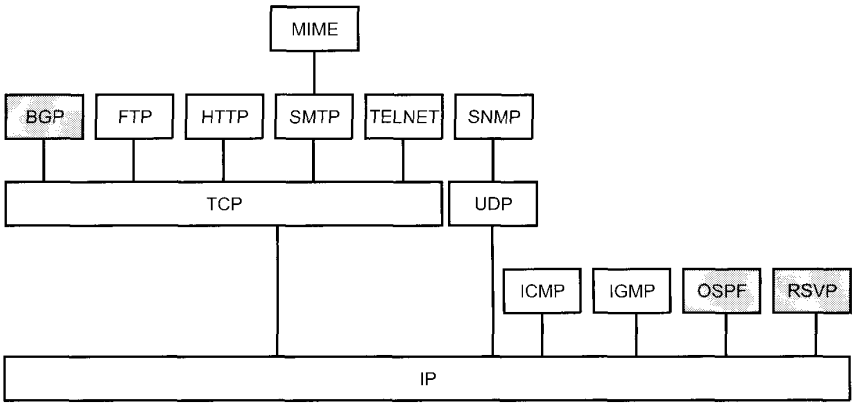


Figura 16.1. Protocolos de interconexión entre redes en su contexto.

trabajo para los servicios internet actuales y del futuro. A este punto le sigue un examen de uno de los protocolos más importantes que emergen en el contexto de ISA: RSVP. Finalmente se examina el concepto de servicios diferenciados.

La Figura 16.1 destaca la posición de los protocolos discutidos en este capítulo dentro de la arquitectura de protocolos TCP/IP.

16.1. PROTOCOLOS DE ENCAMINAMIENTO

En un conjunto de redes, los dispositivos de encaminamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Cada dispositivo de encaminamiento realiza la decisión de encaminamiento basándose en el conocimiento que se tiene sobre la topología y las condiciones del conjunto de redes. En un conjunto de redes sencillo, es posible utilizar un esquema de encaminamiento fijo. En conjuntos de redes más complejos, se necesita un grado de cooperación dinámica entre los dispositivos de encaminamiento. En particular, se deben evitar aquellas porciones de red que han sufrido un fallo y se deberían evitar aquellas porciones de red que sufren congestión. Para poder tomar estas decisiones de encaminamiento dinámicas, los dispositivos de encaminamiento deben intercambiar información de encaminamiento usando un protocolo de encaminamiento especial para ese propósito. La información que se necesita sobre el estado del conjunto de redes tiene que venir expresada en términos de qué redes son accesibles a través de qué dispositivos de encaminamiento y en términos de las características en retardo de varias rutas.

Al considerar las funciones de encaminamiento de los dispositivos de encaminamiento hay que distinguir dos conceptos importantes:

- **Información de encaminamiento:** información sobre la topología y el retardo del conjunto de las redes.
- **Algoritmo de encaminamiento:** algoritmo utilizado para la toma de decisiones de encaminamiento para un datagrama particular, basándose en la información de encaminamiento actual.

SISTEMAS AUTÓNOMOS

Para proceder con nuestra discusión sobre los protocolos de encaminamiento, necesitamos introducir el concepto de sistema autónomo. Un **sistema autónomo** (AS, Autonomous Systems) posee las siguientes características:

1. Un AS consta de un grupo de sistemas de encaminamiento intercambiando información a través de un protocolo de encaminamiento común.
2. Un AS es un conjunto de redes y dispositivos de encaminamiento gestionados por única organización.
3. Excepto en momentos de fallos, un AS está conectado (en un sentido teórico de grafo); esto es, existe un camino entre cualquier par de nodos.

Un **protocolo interior de dispositivo de encaminamiento** (IRP, Interior Router Protocol) pasa la información de encaminamiento entre los dispositivos de encaminamiento dentro de un sistema autónomo. El protocolo que se usa dentro de un sistema autónomo no necesita que esté implementado fuera del sistema. Esta flexibilidad permite que los IRP se hagan a medida para aplicaciones y requisitos específicos.

Podría ocurrir, sin embargo, que un conjunto de redes esté construido con más de un sistema autónomo. Por ejemplo, todas las LAN de un emplazamiento, como puede ser un complejo de oficinas o un campus, se unen por dispositivos de encaminamiento para formar un sistema autónomo. Este sistema se podría unir a otros sistemas autónomos a través de una red de área amplia. Es la situación que se muestra en la Figura 16.2. En este caso, los algoritmos y las tablas de encaminamiento usadas por los dispositivos de encaminamiento en los diferentes sistemas autónomos pueden ser diferentes. Sin embargo, los dispositivos de encaminamiento en un sistema autónomo necesitan al menos un nivel mínimo de información referente a las redes fuera del sistema autónomo a las que se puede acceder. El protocolo que se utiliza para pasar información de encaminamiento entre sistemas autónomos diferentes se conoce como **protocolo de dispositivo de encaminamiento exterior** (ERP, Exterior Router Protocol)[1].

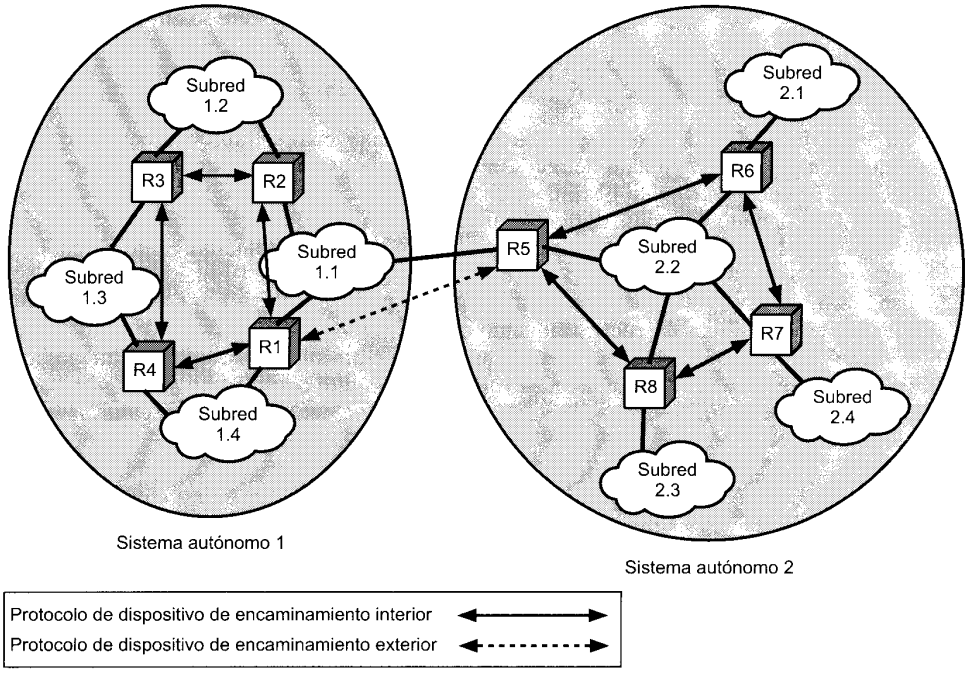


Figura 16.2. Aplicación de los protocolos de encaminamiento exterior e interior.

[1] En la Literatura, se utiliza a menudo los términos *protocolo de pasarela interior* (IGP, Interior Gateway Protocol) y *protocolo de pasarela exterior* (EGP, Exterior Gateway Protocolo) para designar al IPR y ERP. Sin embargo, ya que los términos IGP y EGP también hacen referencia a protocolos específicos, evitaremos su uso para definir conceptos generales.

En términos generales, los protocolos IRP y ERP tienen una característica de alguna forma diferente. Un protocolo IRP necesita construir un modelo más bien detallado de la interconexión de los dispositivos de encaminamiento dentro de un AS para poder calcular el camino con el menor coste desde un dispositivo de encaminamiento dado a cualquier red dentro del AS. Un protocolo ERP permite el intercambio de un resumen de información de alcanzabilidad entre AS administrados de forma separada. Normalmente, el uso de esta información de resumen significa que un protocolo ERP es más simple y utiliza menos información detallada que un protocolo IRP.

En el resto de esta sección, examinaremos el ejemplo que quizás sea el más importante de estos tipos de protocolos de encaminamiento.

PROTOCOLO DE PASARELA FRONTERA

El protocolo de pasarela frontera (BGP, Border Gateway Protocol) se desarrolló para su uso en conjunción con conjuntos de redes que emplean la arquitectura de protocolos TCP/IP, aunque los conceptos son aplicables a cualquier conjunto de redes. BGP se ha convertido en el protocolo de dispositivo de encaminamiento exterior estándar en Internet.

Funciones

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarelas en el estándar, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando conexiones TCP. El repertorio de mensajes se resume en la Tabla 16.1. La versión actual de BGP se conoce como BGP-4 (RFC 1771).

BGP supone tres procedimientos funcionales, que son:

- Adquisición de vecino.
- Detección de vecino alcanzable.
- Detección de red alcanzable.

Dos dispositivos de encaminamiento se consideran que son vecinos si están conectados a la misma subred. Si los dos dispositivos de encaminamiento están en sistemas autónomos diferentes, podrían desear intercambiar información de encaminamiento. Para este cometido, es necesario primero realizar la operación de **adquisición de vecino**. El término vecino se refiere a dos dispositivos de encaminamiento que comparten la misma red. En esencia, la adquisición de vecino ocurre cuando dos dispositivos de encaminamiento vecinos en diferentes sistemas autónomos se ponen de acuerdo en intercambiar regularmente información de encaminamiento. Se requiere un procedimiento formal de adquisición ya que uno de los dispositivos de encaminamiento puede no querer participar. Por ejemplo, el dispositivo de encaminamiento puede estar sobresaturado y no quiere ser responsable del tráfico que llega de fuera del sistema. En el proceso de adquisición de vecino, un dispositivo de encaminamiento envía un mensaje de

Tabla 16.1. Mensajes BGP-4.

Open	Utilizado para establecer una relación de vecindad con otro dispositivo de encaminamiento.
Update	Utilizado para (1) transmitir información a través de una única ruta y/o (2) enumerar rutas múltiples que se van a eliminar.
Keepalive	Utilizado para (1) confirmar una mensaje Open y (2) confirmar periódicamente la relación de vecindad.
Notification	Enviado cuando se detecta una condición de error.

petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no indica la cuestión de cómo puede un dispositivo de encaminamiento conocer la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones deben ser tratadas en el momento de establecer la configuración o por una intervención activa del gestor de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo de encaminamiento envía a otro un mensaje Open («abrir» relación). Si el dispositivo de encaminamiento destino acepta la solicitud, devuelve un mensaje «Keepalive» (la vecindad se «mantiene viva») como respuesta.

Una vez establecida la relación de vecino, se utiliza el procedimiento **detección de vecino alcanzable** para mantener la relación. Cada pareja necesita estar segura de que su pareja existe y está todavía comprometida con la relación de vecino. Para este propósito, periódicamente ambos dispositivos de encaminamiento se envían mensajes Keepalive.

El último procedimiento especificado por BGP es la detección de **red alcanzable**. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzar esa red. Siempre que se realiza un cambio en esta base de datos, el dispositivo de encaminamiento envía un mensaje Update por difusión a todos los otros dispositivos de encaminamiento que implementan BGP. Por medio de la difusión de estos mensajes Update, todos los dispositivos de encaminamiento de BGP pueden acumular y mantener información de encaminamiento.

Mensajes BGP

La Figura 16.3 muestra el formato de todos los mensajes BGP. Cada mensaje comienza con una cabecera de 19 octetos, y contiene tres campos, como se indica en la parte sombreada en la figura:

- **Marcador:** reservado para autenticación. El emisor puede insertar un valor en este campo que se usaría como parte de un mecanismo de autentificación para permitir al destino verificar la identidad del emisor.
- **Longitud:** longitud del mensaje en octetos.
- **Tipo:** tipo de mensaje: Open (abrir), Update (actualizar), Notification (notificar), Keepalive (continuar).

Para adquirir un vecino, un dispositivo de encaminamiento abre primero una conexión TCP al dispositivo de encaminamiento vecino de interés. Entonces envía un mensaje Open. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento. También incluye un parámetro temporizador de mantenimiento, que indica el número de segundos al que se establecerá el temporizador de mantenimiento y que propone el emisor. Si el destino está preparado para abrir una relación de vecindad, calcula un valor para el temporizador de mantenimiento, que es el valor mínimo de su tiempo de mantenimiento y el valor que introduce en su mensaje Open. El valor calculado representa el máximo número de segundos que puede transcurrir entre la recepción de mensajes Keepalive sucesivos y/o mensajes Update del emisor.

El mensaje Keepalive consta solamente de la cabecera. Cada dispositivo de encaminamiento emite estos mensajes bastante a menudo a cada una de sus parejas para prevenir que expire el temporizador de mantenimiento.

El mensaje Update facilita dos tipos de información:

- Información sobre una ruta particular a través del conjunto de redes. Esta información se puede incorporar a la base de datos de cada dispositivo de encaminamiento que la recibe.
- Una lista de rutas previamente anunciadas por este dispositivo de encaminamiento que van a ser eliminadas.

Un mensaje Update puede contener uno o ambos tipos de información. Consideremos primero el tipo de información 1. La información sobre una ruta particular a través de la red implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI, Network Layer Reachability

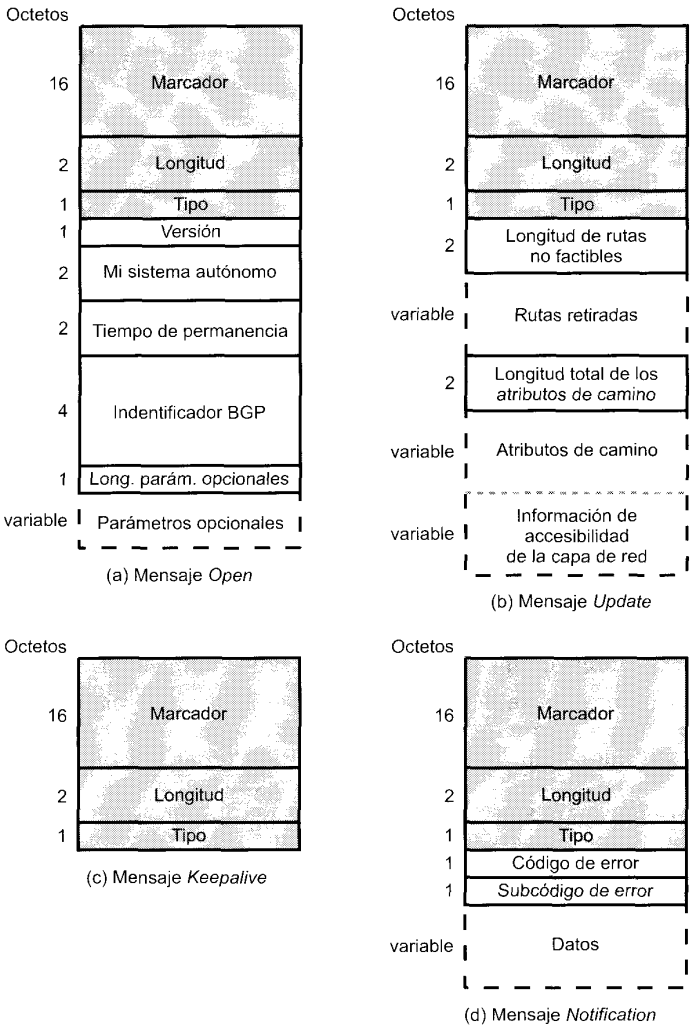


Figura 16.3. Formatos de mensaje BGP.

Information), campo de longitud de los atributos del camino total, y el campo de los atributos de camino. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de la dirección IP completa. Recuérdese que una dirección IP es una cantidad de 32 bits de la forma red, sistema final. El prefijo o la parte izquierda de esta cantidad identifica una red particular.

El campo atributos de camino contiene una lista de atributos que se aplican a esta ruta particular. Los atributos definidos son los siguientes:

- **Origen:** indica si la información fue generada por un protocolo de dispositivo de encaminamiento interior (por ejemplo, OSPF) o por un protocolo de dispositivo de encaminamiento exterior (en particular, BGP).

- **Camino_AS**: una lista de los AS que son atravesados por la ruta.
- **Siguiente_salto:** dirección IP del dispositivo de encaminamiento frontera que se debe usar como siguiente salto para alcanzar los destinos indicados en el campo NLRI.
- **Multi_exit_disc:** se usa para comunicar alguna información sobre rutas internas a un AS. Este atributo se describirá más adelante en esta sección.
- **Local_pref:** usado por un dispositivo de encaminamiento para informar a otros dispositivos de encaminamiento dentro del mismo AS de su grado de preferencia por una ruta particular. No tiene significado alguno para dispositivos de encaminamiento en otros AS.
- **Agregado_atómico**, **Agente_unión:** estos dos campos implementan el concepto de unión de rutas. En esencia, un conjunto de redes y su espacio de direcciones correspondiente se pueden organizar jerárquicamente, o como un árbol. En este caso, las direcciones de las redes se estructuran en dos o más partes. Todas las redes de un subárbol comparten una dirección internet parcial común. Usando esta dirección parcial común, la cantidad de información que se debe comunicar en NLRI se puede reducir significativamente.

El atributo Camino_AS sirve realmente para dos objetivos. Ya que indica los AS que debe atravesar un datagrama si sigue esta ruta, la información de Camino_AS habilita a un dispositivo de encaminamiento a que implemente un criterio de encaminamiento. Esto es, un dispositivo de encaminamiento puede decidir evitar un camino particular para evitar el paso por un AS particular. Por ejemplo, la información que es confidencial puede estar limitada a ciertos AS. O, un dispositivo de encaminamiento puede tener información sobre el rendimiento o calidad de una parte del conjunto de redes que está incluido en un AS lo que guía al dispositivo de encaminamiento para poder evitar ese AS. Algunos ejemplos de rendimiento o métrica de calidad son: velocidad del enlace, capacidad, tendencia a estar congestionado, y calidad global de funcionamiento. Otro criterio que se podría usar es minimizar el número de AS de tránsito.

El lector se podría preguntar por el objetivo del atributo Siguiente_salto. El dispositivo de encaminamiento que realiza la solicitud querrá conocer necesariamente qué redes se pueden alcanzar a través del dispositivo de encaminamiento que responde, pero ¿por qué proporcionar información de otros dispositivos de encaminamiento? Esta situación se explica mejor con la ayuda de la Figura 16.2. En este ejemplo, el dispositivo de encaminamiento R1 en el sistema autónomo 1 y el dispositivo de encaminamiento R5 en el sistema autónomo 2 implementan BGP y adquieren una relación de vecindad. R1 envía un mensaje Update a R5 indicando qué redes podría alcanzar y las distancias (saltos de red) implicadas. R1 también proporciona la misma información en representación de R2. Esto es, R1 le dice a R5 qué redes se pueden alcanzar vía R2. En este ejemplo, R2 no implementa BGP. Normalmente, la mayoría de los dispositivos de encaminamiento en un sistema autónomo no implementan BGP. Sólo unos pocos dispositivos de encaminamiento tendrán asignada la responsabilidad de comunicarse con otros dispositivos de encaminamiento en otros sistemas autónomos. Un punto final: R1 tiene la información necesaria sobre R2 ya que R1 y R2 comparten un protocolo de dispositivo de encaminamiento interior (IRP).

El segundo tipo de información de actualización es la retirada de una o más rutas. En cualquier caso, la ruta se identifica por la dirección IP de la red destino.

Finalmente, los mensajes de notificación se envían cuando se detecta una condición de error. Se puede informar de los siguientes errores:

- **Error en la cabecera del mensaje:** incluye errores de sintaxis y autentificación.
- **Error en mensaje Open:** incluye errores de sintaxis y opciones no reconocidas en un mensaje Open. Este mensaje también se puede utilizar para indicar que el tiempo de mantenimiento en el mensaje Open es inaceptable.
- **Error en el mensaje Update:** incluye errores de sintaxis y validación en un mensaje Update.
- **Tiempo de mantenimiento expirado:** si el dispositivo de encaminamiento que envía no ha recibido mensajes sucesivos Keepalive y/o Update y/o de Notificación durante el tiempo de mantenimiento, entonces se comunica este error y se cierra la conexión.

- **Error en la máquina de estados finitos:** incluye cualquier error de procedimiento.
- **Cese:** utilizado por un dispositivo de encaminamiento para cerrar una conexión con otro dispositivo de encaminamiento en ausencia de cualquier otro error.

Intercambio de información de encaminamiento BGP

La esencia de BGP es el intercambio de información de encaminamiento entre dispositivos de encaminamiento participantes en múltiples AS. Este proceso puede ser bastante complejo. A continuación, proporcionaremos un visión simplificada.

Consideremos el dispositivo de encaminamiento R1 en el sistema autónomo 1 (AS1), en la Figura 16.2. Para comenzar, un dispositivo de encaminamiento que implementa BGP implementará también un protocolo de dispositivo de encaminamiento interno como OSPF. Usando OSPF, R1 puede intercambiar información de encaminamiento con otros dispositivos de encaminamiento dentro de AS1 y construir un esquema de la topología de las redes y dispositivos de encaminamiento en AS1 para obtener una tabla de encaminamiento. A continuación, R1 puede emitir un mensaje Update a R5 en AS2. Este mensaje Update podría incluir lo siguiente:

- **Camino_AS:** la identidad de AS1.
- **Siguiente_salto:** la dirección IP de R1.
- **NLRI:** una lista de todas las redes en AS1.

Este mensaje informa a R5 que todas las redes indicadas en NLRI se alcanzan vía R1 y que el único sistema autónomo que hay que atravesar es AS1.

Supóngase ahora que R5 también tiene una relación de vecindad con otro dispositivo de encaminamiento, digamos R9 en AS3. R5 enviará la información que acaba de recibir de R1 a R9 en un mensaje Update nuevo. Este mensaje incluye lo siguiente:

- **Camino_AS:** la lista de identificadores {AS2, AS1}.
- **Siguiente_salto:** la dirección IP de R5.
- **NLRI:** una lista de todas las redes en AS1.

Este mensaje informa a R9 que todas las redes indicadas en NLRI se alcanzan vía R5 y que los sistemas autónomos que hay que atravesar son AS2 y AS1. R9 debe decidir si ésta es ahora su ruta preferida a las redes indicadas. R9 podría tener información de una ruta alternativa a alguna o a todas las redes que prefiere por razones de rendimiento o algún otro criterio de la métrica usada. Si R9 decide que la ruta suministrada por el mensaje de R5 es preferible, entonces incorpora la información de encaminamiento en su base de datos de encaminamiento y propaga la nueva información a sus vecinos. Este mensaje nuevo incluirá un campo Camino_AS del tipo {AS1, AS2, AS3}.

De esta forma, la información de encaminamiento actualizada se propaga a través de un conjunto de redes más grande que contendrá a su vez sistemas autónomos interconectados. El campo Camino_AS se usa para asegurar que el mensaje no circula indefinidamente: si se recibe un mensaje Update en un dispositivo de encaminamiento en un AS que está incluido en el campo Camino_AS, ese dispositivo de encaminamiento no enviará la información actualizada a otros dispositivos de encaminamiento, previniendo así que los mensajes entren en un bucle cerrado.

Los dispositivos de encaminamiento dentro de un AS, que son denominados vecinos internos, pueden intercambiar información BGP. En este caso, el dispositivo de encaminamiento origen no incorpora el identificador del AS común al campo Camino_AS. Cuando un dispositivo de encaminamiento ha seleccionado una ruta a un destino externo como preferida, transmite esta ruta a todos sus vecinos internos. Cada uno de estos dispositivos de encaminamiento decide entonces si la nueva ruta pasa a ser la preferida. En este caso, la ruta nueva se incorpora a su base de datos y envía un mensaje nuevo Update.

Cuando hay disponibles múltiples puntos de entrada a un AS, desde el punto de vista de un dispositivo de encaminamiento fronterizo en otro AS, el atributo Multi_Exit_Disc se usa para elegir uno de ellos. Este atributo contiene un número que refleja alguna métrica interna que indica como alcanzar el destino dentro de un AS. Por ejemplo, suponga que en la Figura 16.2 los dispositivos de encaminamiento R1 y R2 implementan BGP y que ambos tienen una relación de vecindad con R5. Cada uno envía un mensaje Update a R5 para la red 1.3 que incluye una métrica de encaminamiento utilizada internamente en AS1, tal como la métrica de encaminamiento asociada con el protocolo de encaminamiento interno OSPF. R5 podría usar entonces estas dos métricas nuevas como criterio para elegir entre los dos dispositivos de encaminamiento.

PROTOCOLO ABIERTO DEL PRIMER CAMINO MÁS CORTO (OSPF, OPEN SHORTEST PATH FIRST)

La historia de los protocolos de encaminamiento interior en Internet refleja lo que ocurrió con los protocolos de conmutación de paquetes en ARPANET. Recuérdese que ARPANET comenzó con un protocolo basado en el algoritmo Bellman-Ford. El protocolo resultante requería que cada nodo intercambiara con sus vecinos información sobre el retardo en las líneas. La información acerca de un cambio en las condiciones de la red se expandían gradualmente a través de la red. Una segunda generación de protocolos se basó en el algoritmo de Dijkstra y requería que cada nodo intercambiara información sobre el retardo del enlace con todos los otros nodos utilizando inundaciones. Se encontró que esta segunda técnica era más efectiva.

De igual forma, el protocolo de encaminamiento interior inicial en el conjunto de redes DARPA fue el Protocolo de Información de Encaminamiento (RIP, Routing Information Protocol), que era esencialmente el mismo protocolo que el protocolo ARPANET de la primera generación. Este protocolo requiere que cada dispositivo de encaminamiento transmita su tabla de encaminamiento completa. Aunque el algoritmo es sencillo y fácil de implementar, conforme se amplía el conjunto de redes, la actualización del encaminamiento se hace más grande y consume significativamente más ancho de banda de la red. De acuerdo a esto, OSPF opera de una forma similar al algoritmo de encaminamiento ARPANET revisado. OSPF utiliza lo que se conoce como un algoritmo de encaminamiento de estado del enlace. Cada dispositivo de encaminamiento mantiene las descripciones del estado de sus enlaces locales a las redes, y periódicamente transmite la información de estado actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento. Cada dispositivo de encaminamiento que recibe un paquete de actualización debe confirmarlo al emisor. Esta actualización produce un tráfico de encaminamiento mínimo ya que las descripciones de los enlaces son pequeñas y es raro que se tengan que enviar. El protocolo OSPF (RFC 2328) se usa de una forma generalizada como protocolo de dispositivo de encaminamiento interior en redes TCP/IP. OSPF calcula una ruta a través del conjunto de redes que suponga el menor coste de acuerdo a una métrica de coste configurable por usuario. El usuario puede configurar el coste para que exprese una función del retardo, la velocidad de transmisión, el coste en dólares, u otros factores. OSPF es capaz de equilibrar las cargas entre múltiples caminos de igual coste.

Cada dispositivo de encaminamiento mantiene una base de datos que refleja la topología conocida del sistema autónomo del que forma parte. Esta topología se expresa como un grafo dirigido. El grafo consta de:

- Vértices, o nodos, de dos tipos:
  - — dispositivo de encaminamiento
  - — red, que también puede ser de dos tipos:
    - *a*) de tránsito, si pueden transportar datos que no se han originado ni van dirigidos a un sistema final conectado a esta red.
    - *b*) terminal, si no es una red de tránsito.

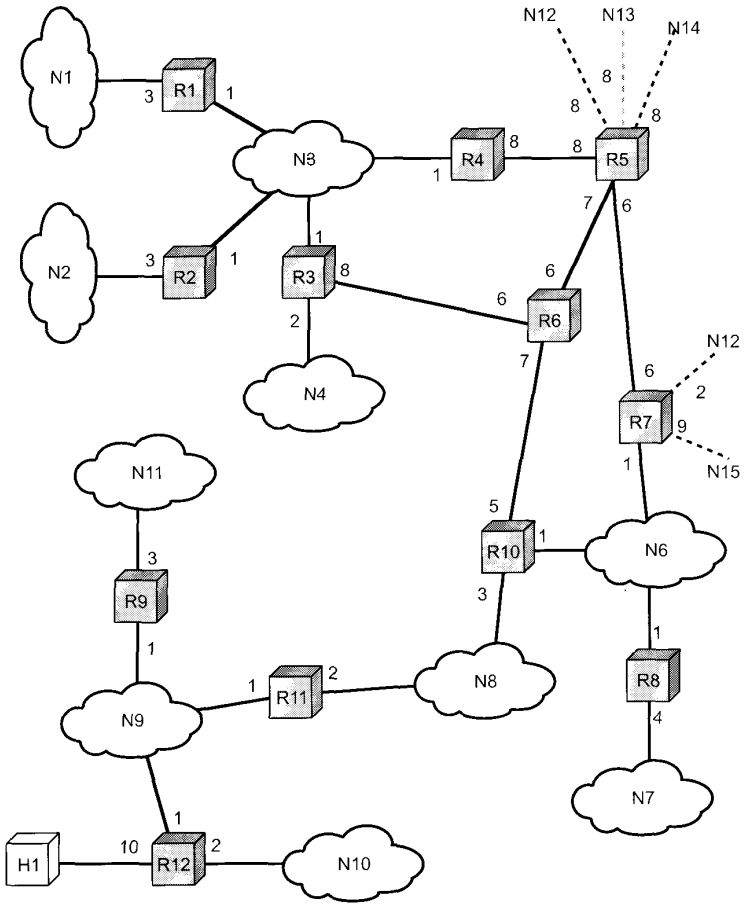


Figura 16.4. Un sistema autónomo sencillo.

- Arcos, de dos tipos:
  - — arcos del grafo que conectan dos vértices que son dispositivos de encaminamiento cuando los dispositivos de encaminamiento correspondientes están conectados el uno al otro por un enlace punto-a-punto directo.
  - — arcos del grafo que conectan un dispositivo de encaminamiento vértice a una red vértice cuando el dispositivo de encaminamiento está directamente conectado a la red.

La Figura 16.4 basada en una figura que se encuentra en el RFC 2328 muestra un ejemplo de un sistema autónomo, y la Figura 16.5 es el correspondiente grafo dirigido. La correspondencia es fácil:

- Dos dispositivos de encaminamiento unidos por un enlace punto-a-punto están representados en el grafo mediante una conexión directa por dos arcos, uno en cada dirección (por ejemplo, los dispositivos de encaminamiento 6 y 10).
- Cuando varios dispositivos de encaminamiento están conectados a una red (como una LAN o una red de conmutación de paquetes), el grafo dirigido muestra a todos los dispositivos de encamina-

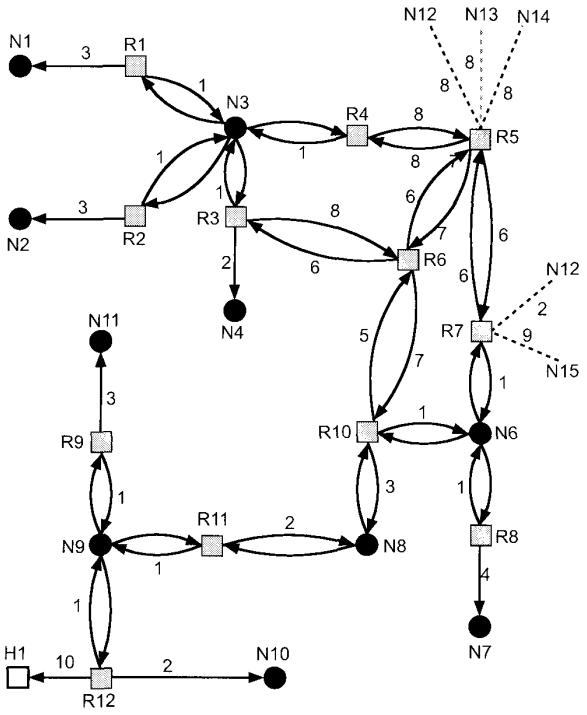


Figura 16.5. Grafo dirigido del sistema autónomo de la Figura 16.4.

miento conectados bidireccionalmente a la red vértice (por ejemplo, los dispositivos de encaminamiento 1, 2, 3 y 4 conectados a la red 3).

- Si un único dispositivo de encaminamiento está conectado a una red, la red aparecerá en el grafo como una red terminal (por ejemplo, la red 7).
- Un sistema final, denominado computador, se puede conectar directamente a un dispositivo de encaminamiento, en cuyo caso se dibuja en el grafo correspondiente (por ejemplo, el computador 1).
- Si un dispositivo de encaminamiento está conectado a otro sistema autónomo, entonces el coste del camino a cada una de las redes en el otro sistema se debe obtener mediante algún protocolo de encaminamiento exterior (ERP). Cada una de estas redes se representa en el grafo por una red terminal y un arco al dispositivo de encaminamiento con el coste conocido del camino (por ejemplo, las redes 12 a 15).

A cada lado de salida de cada interfaz de un dispositivo de encaminamiento se le asocia un coste. Este coste es configurable por el administrador del sistema. Los arcos en el grafo se etiquetan con el coste de la interfaz de salida del dispositivo de encaminamiento correspondiente. Los arcos que no tienen etiqueta tienen un coste 0. Obsérvese que los arcos que van de las redes a los dispositivos de encaminamiento tienen siempre coste 0.

La base de datos correspondiente al grafo dirigido se mantiene en cada dispositivo de encaminamiento. Se mantiene coherente con los mensajes de estado del enlace provenientes de otros dispositivos de encaminamiento en el conjunto de redes. Un dispositivo de encaminamiento calcula el camino de menor coste a todas las redes destino usando el algoritmo de Dijkstra (véase Apéndice 9A). El resultado para el dispositivo de encaminamiento 6 de la Figura 16.4 se muestra como un árbol en la Figura 16.6,

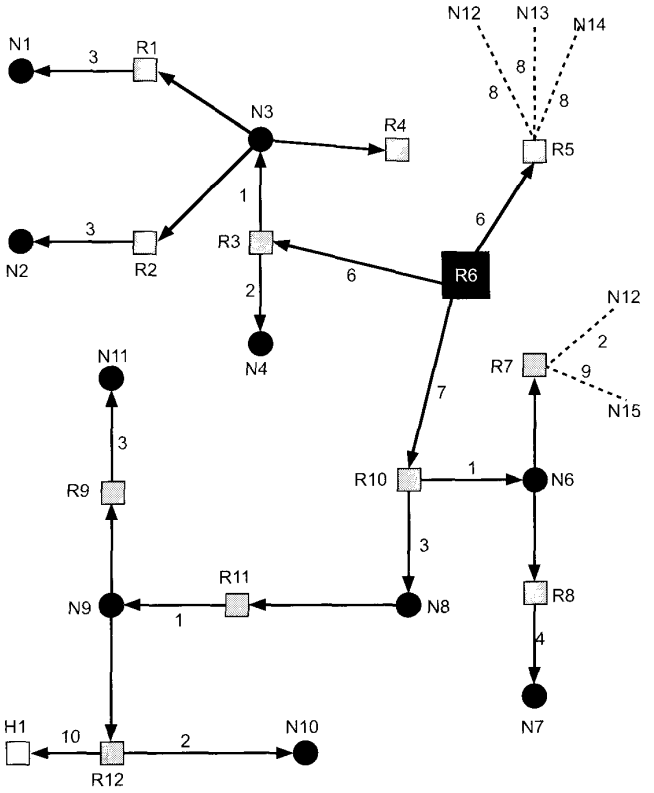


Figura 16.6. El árbol SPF para el dispositivo de encaminamiento R6.

con R6 como raíz del árbol. El árbol da la ruta completa a cualquier red o computador destino. Sin embargo, sólamente se usa el siguiente salto para el proceso de reenvío. La tabla de encaminamiento resultante para el dispositivo de encaminamiento se muestra en la Tabla 16.2. La tabla incluye elementos para los dispositivos de encaminamiento que informan de rutas externas (dispositivos de encaminamiento 5 y 7). Contiene elementos referentes a redes externas cuya identidad se conoce.

16.2. ARQUITECTURA DE SERVICIOS INTEGRADOS

Históricamente, las redes basadas en IP han sido capaces de proporcionar un servicio de entrega sencillo y de máximo esfuerzo a todas las aplicaciones que permitían estas redes. El servicio del mejor esfuerzo trata a todos los paquetes de igual forma, sin niveles de servicio, requerimientos, reservas o garantías. Aunque la cabecera de IPv4 está equipada con campos que pueden especificar nivel de precedencia y tipo de servicio, en general esta información se ha ignorado por los dispositivos de encaminamiento, tanto en la selección de los dispositivos de encaminamiento y en el tratamiento de los paquetes individuales. El estilo del mejor esfuerzo ha funcionado por lo general bien: los usuarios pueden tolerar algún retardo y la variabilidad en la velocidad de los datos («jitter») para el correo electrónico, la transferencia de ficheros o la navegación Web.

Tabla 16.2. Tabla de encaminamiento para R6.

Destino	Siguiente salto	Distancia
N1	R3	10
N2	R3	10
N3	R3	7
N4	R3	8
N6	R10	8
N7	R10	12
N8	R10	10
N9	R10	11
N10	R10	13
N11	R10	14
H1	R10	21
R5	R5	6
R7	R10	8
N12	R10	10
N13	R5	14
N14	R5	14
N15	R10	17

Pero las necesidades de los usuarios han cambiado. Una empresa puede haberse gastado millones de dólares instalando una red basada en IP diseñada para transportar datos entre LAN pero encuentra que las nuevas aplicaciones en tiempo real, multimedia o multidifusión no funcionan bien con esa configuración. Por ejemplo, la más ligera congestión puede transformar una llamada de teléfono por Internet en un galimatías. Para el tráfico sensible al retardo, la técnica del mejor esfuerzo sólo funciona bien cuando existen abundantes recursos de red desde un extremo de Internet al otro extremo. El único esquema de interconexión diseñado para dar soporte desde el primer día al tráfico tradicional TCP y UDP y al tráfico en tiempo real es ATM. Sin embargo, la confianza en ATM significa o bien construir una segunda infraestructura de interconexión para el tráfico en tiempo real o reemplazar la configuración existente basada en IP por ATM, las cuales son alternativas costosas.

De esta forma, existe una fuerte necesidad de ser capaz de soportar una gran variedad de tráfico con una gran diversidad de requisitos en cuanto a la calidad del servicio (QoS, del inglés, Quality-of-Service) dentro de una arquitectura TCP/IP. Un mecanismo de QoS traduce una petición de servicio (como una llamada de teléfono por Internet) en un conjunto de características de tráfico para ese servicio (como el rendimiento, el retardo, la variación de retardo, pérdidas y tasa de errores). El mecanismo de QoS debe ser capaz de medir estas características de tráfico y utilizar técnicas de encaminamiento y de tratamiento de colas para conseguirlas. Algunos mecanismos de QoS también tratan de obtener recursos de la red (capacidad y memoria de almacenamiento) suficientes para garantizar estas características. El requisito fundamental es incorporar una nueva funcionalidad a los dispositivos de encaminamiento y un medio para solicitar un servicio basado en QoS para un conjunto de redes. Para satisfacer este requisito la IETF está desarrollando un conjunto de estándares bajo el paraguas general de la Arquitectura de Servicios Integrados (ISA). ISA, pensado para proporcionar transporte de QoS sobre redes basadas en IP, se define en términos generales en el RFC 1633, mientras se desarrollan otra serie de documentos que cubren los detalles. Actualmente, una serie de vendedores han implementado partes de ISA en el software de los dispositivos de encaminamiento y de los sistemas finales.

Esta sección proporciona una visión general de ISA.

TRÁFICO EN INTERNET

El tráfico en una red o en un conjunto de redes se puede dividir en dos categorías generales: tráfico elástico y tráfico no elástico. Una consideración de sus diferentes necesidades clarifica la necesidad de una arquitectura de red mejorada.

Tráfico elástico

El tráfico elástico es aquel que se puede ajustar, sobre un gran rango, a cambios en el retardo y rendimiento a través de un conjunto de redes y aun así satisfacer las necesidades de sus aplicaciones. Éste es el tipo tradicional de tráfico admitido por las redes basadas en TCP/IP y es el tipo de tráfico para el cual se diseñaron las redes. Las aplicaciones que generan este tráfico normalmente utilizan a TCP o UDP como protocolo de la capa de transporte. En el caso de UDP, la aplicación utilizará tanta capacidad como haya disponible compatible con la velocidad de la aplicación que genera los datos. En el caso de TCP, la aplicación utilizará tanta capacidad como haya disponible hasta la máxima velocidad de datos que el receptor puede aceptar. También con TCP, el tráfico en las conexiones individuales se ajusta a la congestión reduciendo la velocidad a la que se envían los datos por la red; este caso se describe en el Capítulo 17.

Las aplicaciones que se pueden clasificar como elásticas incluyen las aplicaciones comunes que operan sobre TCP o UDP, entre ellas la transferencia de ficheros (FTP), el correo electrónico (SMTP), la conexión remota (TELNET), la gestión de red (SNMP) y el acceso a la información Web (HTTP). Sin embargo, existen diferencias entre las necesidades de estas aplicaciones. Por ejemplo:

- El correo electrónico es generalmente bastante insensible a los cambios en retardo.
- Cuando la transferencia de ficheros se hace en tiempo real, y es así normalmente, el usuario espera que el retardo sea proporcional al tamaño del fichero y, por tanto, es sensible a cambios en el rendimiento.
- Para la gestión de red, el retardo no es en general una preocupación seria. Sin embargo, si los fallos en un conjunto de redes se producen debido a la congestión, entonces la necesidad de que los mensajes SNMP se envíen con un retardo mínimo se incrementa con la congestión.
- Las aplicaciones interactivas, como la conexión remota y el acceso Web, son bastantes sensibles al retardo.

Es importante darse cuenta de que no es el retardo de cada paquete el valor que interesa. Como se indica en [CLAR95] la observación de retardos reales a través de Internet indica que no ocurren grandes rangos de variaciones. Debido a los mecanismos de control de congestión de TCP, cuando aparece congestión los retardos sólo se incrementan de forma moderada antes de que la velocidad de llegada de datos de las conexiones TCP disminuya. Por otro lado, la QoS percibida por el usuario se relaciona con el tiempo total transcurrido para transferir un elemento de la aplicación actual. Para una aplicación basada en TELNET en tiempo real, el elemento puede ser pulsar un tecla o una nueva línea. Para el acceso Web, el elemento puede ser una página Web, que puede ser tan pequeña como unos pocos kilobytes o puede ser sustancialmente más grande para una página rica en imágenes. Para una aplicación científica, el elemento podrían ser varios megabytes de datos.

Para los elementos muy pequeños, el tiempo total transcurrido está dominado por el tiempo de retardo a través del conjunto de redes. Sin embargo, para elementos más grandes, el tiempo total transcurrido está dictado por el rendimiento de la ventana deslizante de TCP y por lo tanto dominado por el rendimiento alcanzado en la conexión TCP. De esta forma, para transferencias grandes, el tiempo de transferencia es proporcional al tamaño del fichero y al grado al que la fuente reduce el envío debido a la congestión.

Debería quedar claro que aunque centremos nuestra atención en el tráfico elástico, es beneficioso un servicio de red basado en QoS. Sin este tipo de servicio, sólo se tendrían dispositivos de encaminamien-

to que tratan imparcialmente los paquetes IP que reciben, sin preocuparse del tipo de aplicación y de si los paquetes son parte de un elemento de transferencia más grande o de uno más pequeño. Bajo tales circunstancias, y si aparece congestión, no es probable que los recursos se asignen de tal forma que se satisfagan medianamente bien las necesidades de todas las aplicaciones.

Tráfico no elástico

El tráfico no elástico no se adapta fácilmente, si es que lo hace, a los cambios en el retardo y el rendimiento a través de un conjunto de redes. El principal ejemplo es el tráfico en tiempo real. Las necesidades del tráfico no elástico son algunas de las siguientes:

- **Rendimiento:** se puede requerir un valor mínimo del rendimiento. A diferencia de la mayoría del tráfico elástico, que puede continuar entregado datos con quizás un servicio degradado, muchas aplicaciones no elásticas requieren, de una forma absoluta, un rendimiento mínimo dado.
- **Retardo:** un ejemplo de aplicación sensible al retardo es el negocio de las acciones en bolsa; alguien que recibe constantemente un servicio tarde actuará constantemente tarde, y con una mayor desventaja.
- **Variación del retardo:** la magnitud de variación del retardo, llamada «*jitter*», es un factor crítico en las aplicaciones en tiempo real. Cuanto más grande es la variación del retardo permitida, más grande es el retardo real para entregar los datos y más grande es el tamaño de la memoria temporal necesaria para tratar el retardo en el receptor. Las aplicaciones interactivas en tiempo real, como es la teleconferencia, pueden requerir un límite superior en la variación del retardo.
- **Pérdida de paquetes:** las aplicaciones en tiempo real varían dependiendo de la cantidad de paquetes perdidos que pueden sufrir, si es que pueden sufrir pérdida de paquetes.

Estas necesidades son difíciles de satisfacer en un entorno con un retardo de tratamiento en cola variable y pérdidas debido a la congestión. Por lo tanto, el tráfico no elástico introduce dos nuevas necesidades en la arquitectura de interconexión. La primera, se necesitan medios para dar un tratamiento preferente a las aplicaciones con más necesidades de demanda.

Las aplicaciones deben ser capaces de indicar sus necesidades, bien antes de tiempo mediante algún tipo de función de solicitud de servicio, o sobre la marcha, por medio de campos en la cabecera del paquete IP. La primera propuesta permite una mayor flexibilidad a la hora de indicar las necesidades y permite a la red anticipar demandas y denegar nuevas solicitudes si los recursos solicitados no están disponibles. Esta propuesta implica el uso de algún tipo de protocolo de reserva de recursos.

La segunda necesidad para permitir tráfico no elástico en una arquitectura de interconexión es que el tráfico elástico debe seguirse permitiendo. Las aplicaciones no elásticas no dan marcha atrás y reducen la demanda cuando se enfrentan a la congestión, a diferencia de lo que hacen las aplicaciones basadas en TCP. Por lo tanto, en los periodos de congestión, el tráfico no elástico continuará suministrando una carga elevada y el tráfico elástico será retirado de la red. Un protocolo de reserva puede ayudar a controlar esta situación denegando las solicitudes de servicio que de otra forma dejarían muy pocos recursos disponibles para tratar el tráfico elástico actual.

ENFOQUE ISA

El propósito de ISA es habilitar el suministro de apoyo a QoS en un conjunto de redes basadas en IP. La cuestión de diseño central en ISA es cómo compartir la capacidad disponible en periodos de congestión.

Para un conjunto de redes basadas en IP que sólo proporcionan un servicio del mejor esfuerzo, las herramientas para controlar la congestión y proporcionar servicios son limitadas. En la práctica, los dispositivos de encaminamiento tienen dos mecanismos para actuar:

- **Algoritmos de encaminamiento:** la mayoría de los protocolos de encaminamiento en uso en las redes permiten elegir rutas que minimizan el retardo. Los dispositivos de encaminamiento intercambian información para hacerse una idea de los retardos a través del conjunto de redes. El encaminamiento de mínimo retardo ayuda a balancear la carga, y de esta forma, disminuir la congestión y ayudar a reducir los retardos vistos por la conexiones individuales TCP.
- **Descarte de paquetes:** cuando la memoria temporal de un dispositivo de encaminamiento se agota, éste descarta los paquetes. Normalmente, se descarta el paquete más reciente. El efecto de la pérdida de paquetes en una conexión TCP es que la entidad TCP que envía da marcha atrás y reduce su carga a la red, de esta forma alivia la congestión en la red.

Estas herramientas han funcionado razonablemente bien. Sin embargo, como muestran las discusiones de secciones anteriores, estas técnicas son inadecuadas para la variedad de tráfico venidero.

ISA es una arquitectura global dentro de la que se están desarrollando una serie de mejoras al tradicional mecanismo del máximo esfuerzo. En ISA, cada paquete IP se puede asociar con un flujo. El RFC 1633 define un flujo como una corriente distinguible de paquetes IP relacionados que provienen de una única actividad de usuario y requieren la misma QoS. Por ejemplo, un flujo puede estar compuesto de una conexión de transporte o una cadena de datos de vídeo distinguible por ISA. Un flujo se diferencia de una conexión TCP en dos cuestiones particulares: un flujo es unidireccional y puede haber más de un destino del flujo (multidifusión). Normalmente, un paquete IP se identifica como miembro de un flujo sobre la base de las direcciones IP origen y destino, los números de puerto y el tipo de protocolo. El identificador de flujo de la cabecera IPv6 no es necesariamente equivalente a un flujo ISA, pero en el futuro el identificador de flujo de IPv6 se podría utilizar en ISA.

ISA hace uso de las funciones siguientes para controlar la congestión y proporcionar transporte de QoS:

- **Control de admisión:** para el transporte QoS (además del transporte del mejor esfuerzo que se tiene por defecto) ISA requiere que se haga una reserva para un flujo nuevo. Si el dispositivo de encaminamiento determina colectivamente que no hay suficientes recursos para garantizar el QoS solicitado, entonces el flujo no se admite. El protocolo RSVP, que se discute en la Sección 16.3, se utiliza para hacer las reservas.
- **Algoritmo de encaminamiento:** la decisión de encaminamiento puede estar basada en una variedad de parámetros QoS, no solamente el retardo mínimo. Por ejemplo, el protocolo de encaminamiento OSPF, discutido en la Sección 16.1, puede seleccionar rutas basándose en QoS.
- **Disciplinas de atención en cola:** un elemento vital de ISA es una política de atención en cola efectiva que tenga en cuenta las diferentes necesidades de los diferentes flujos.
- **Política de descarte:** una política de atención en cola determina que paquete transmitir a continuación si existe un cierto número de ellos que están en la cola del mismo puerto de salida. Un elemento importante es un política de descarte para gestionar la congestión y satisfacer las QoS garantizadas.

COMPONENTES ISA

La Figura 16.7 es un diagrama general de la arquitectura de implementación para ISA dentro de un dispositivo de encaminamiento. Debajo de la línea horizontal gruesa se encuentran las funciones de reenvío del dispositivo de encaminamiento; éstas se ejecutan para cada paquete y por lo tanto deben de estar optimizadas. El resto de funciones, por encima de la línea, son funciones de respaldo que crean estructuras de datos utilizadas por las funciones de reenvío.

Las funciones de respaldo principales son las siguientes:

- **Protocolo de reserva:** este protocolo se utiliza para reservar recursos para flujos nuevos a un nivel dado de QoS. Se utiliza entre dispositivos de encaminamiento y entre dispositivos de encami-

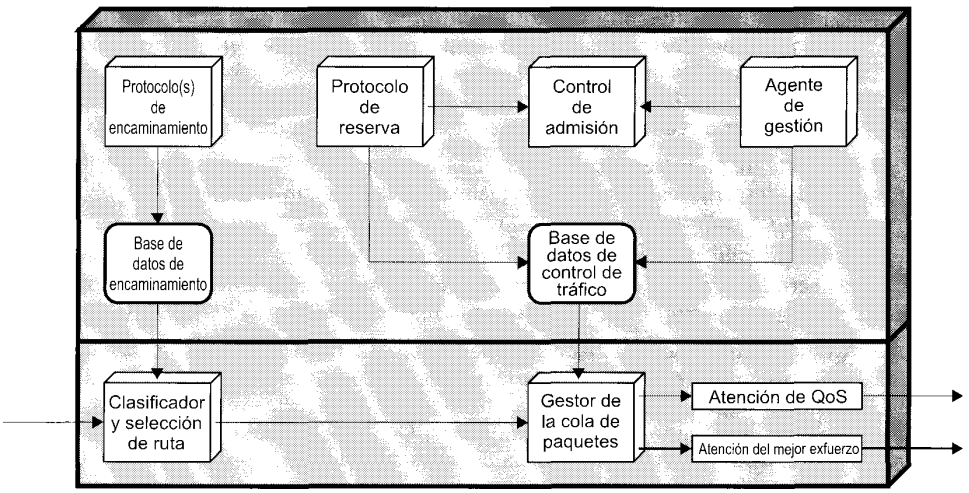


Figura 16.7. Arquitectura de servicios integrados implementada en un dispositivo de encaminamiento.

namiento y sistemas finales. El protocolo de reserva es responsable de mantener información de estado específica de un flujo en el sistema final y en los dispositivos de encaminamiento a lo largo del camino del flujo. Para este propósito se utiliza el protocolo RSVP. El protocolo de reserva actualiza la base de datos de control de tráfico utilizada por el gestor de la cola de salida de paquetes para determinar el servicio que se le proporciona a los paquetes de cada flujo.

- **Control de admisión:** cuando se solicita un flujo nuevo, el protocolo de reserva invoca la función de control de admisión. Esta función determina si hay disponibles recursos suficientes para este flujo al QoS solicitado. Esta determinación se basa en el nivel actual del compromiso con otras reservas y/o la carga actual de la red.
- **Agente de gestión:** un agente de gestión de red es capaz de modificar la base de datos de control de tráfico y dirigir el módulo de control de admisión para establecer políticas de control de admisión.
- **Protocolo de encaminamiento:** el protocolo de encaminamiento es responsable de mantener la base de datos de encaminamiento que da el siguiente salto para alcanzar cada dirección destino y cada flujo.

Estas funciones de respaldo dan apoyo a la tarea principal de un dispositivo de encaminamiento, que es reenviar paquetes. Las dos áreas funcionales principales que acompañan al reenvío son las siguientes:

- **Clasificador y selección de ruta:** para llevar a cabo el reenvío y el control de tráfico, los paquetes entrantes se tienen que clasificar en clases. Una clase puede corresponderse con un único flujo o con un conjunto de flujos que necesitan la misma QoS. Por ejemplo, los paquetes de todos los flujos de vídeo o los paquetes de todos los flujos atribuibles a una organización particular se pueden tratar de forma idéntica por motivos de asignación de recursos y disciplinas de tratamiento en cola. La selección de clase se hace en función de los campos de la cabecera IP. Basándose en la clase de un paquete y en su dirección IP destino, esta función determina la dirección del siguiente salto que va a hacer este paquete.
- **Gestor de la cola de salida:** esta función gestiona una o más colas de cada puerto de salida. Determina el orden en que se transmiten los paquetes en la cola de salida y selecciona los paquetes para descartarlos, si es necesario esto. Las decisiones se toman basándose en la clase del paquete, el contenido de la base de datos de control de tráfico y la actividad actual y pasada de este puerto

de salida. Parte de la tarea del gestor de la cola de salida es la de actuar como «policía» que es la función que determina si el tráfico de paquetes en un flujo dado excede la capacidad solicitada y, si es así, decidir cómo tratar el exceso de paquetes.

SERVICIOS ISA

El servicio ISA para un flujo de paquetes se define en dos niveles. Primero, se proporciona un número de categorías generales de servicios, cada una de ellas proporciona cierto tipo general de garantía de servicio. Segundo, dentro de cada categoría, el servicio que se le da a un flujo particular se especifica por los valores de ciertos parámetros; junto a esto, estos valores de denominan especificación de tráfico (TSpec). Actualmente se han definido tres categorías de servicio:

- Garantizado.
- Carga controlada.
- Mejor esfuerzo.

Una aplicación puede solicitar una reserva para un flujo con QoS garantizada o de carga controlada, con una TSpec que define la cantidad exacta del servicio solicitado. Si se acepta la reserva, entonces la TSpec forma parte del contrato entre el flujo de datos y el servicio. El servicio acepta proporcionar la QoS solicitada tanto tiempo como el tráfico del flujo de datos continúe siendo descrito de forma precisa por la TSpec. Los paquetes que no forman parte de un flujo reservado se les da por defecto un servicio del mejor esfuerzo.

Antes de repasar las categorías de servicio ISA, se debería definir un concepto general: la especificación de tráfico de cesta de testigos (token bucket). Ésta es una forma de caracterizar el tráfico y que posee tres ventajas en el contexto de ISA:

1. Muchas fuentes de tráfico se pueden definir fácilmente y de forma precisa por un esquema de cesta de testigos.
2. El esquema de cesta de testigos proporciona una descripción concisa de la carga que va a imponer un flujo, permitiendo al servicio determinar fácilmente la necesidad en recursos.
3. El esquema de cesta de testigos proporciona los parámetros de entrada a la función de actuar como «policía».

Una especificación de tráfico cesta de testigos consta de dos parámetros: una velocidad de relleno de testigos R y un tamaño de la cesta B. La velocidad de testigos R especifica la velocidad de datos sostenida constantemente, esto es, la velocidad media que se le puede proporcionar a un flujo durante un periodo de tiempo relativamente grande es R. El tamaño de la cesta B especifica la cantidad que la velocidad de datos puede superar a R durante periodos de tiempo cortos. La condición exacta es la siguiente: durante cualquier periodo de tiempo T, la cantidad de datos enviados no puede exceder a $RT + B$.

La Figura 16.8 ilustra este esquema y explica el uso del término *cesta*. La cesta representa un contador que indica el número permitido de octetos de datos IP que se pueden enviar en cualquier instante de tiempo. La cesta se llena con *testigos de octetos* a una velocidad de R (en otras palabras, el contador se incrementa R veces por segundo) hasta la capacidad de la cesta (hasta el valor máximo del contador). Los paquetes van llegando y se pasan a la cola para su procesamiento. Un paquete IP se procesa si hay suficientes testigos de octetos que igualen al tamaño de los datos IP. Si es así, se procesa el paquete y se quita el correspondiente número de testigos de la cesta. Si llega un paquete y hay insuficientes testigos disponibles, el paquete excede la TSpec para este flujo. El tratamiento que se le da a este paquete no está especificado en los documentos ISA; las acciones más comunes son relegar el paquete a un servicio del mejor esfuerzo, descartar el paquete o marcar el paquete de forma que puede ser descartado en el futuro.

Durante un periodo grande, la velocidad de datos IP permitidos por la cesta de testigos es R. Sin embargo, si existe un periodo de inactividad o relativamente lento, la capacidad de la cesta crece, de

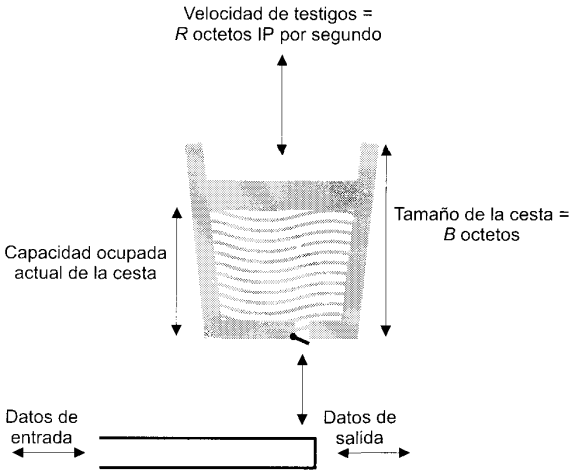


Figura 16.8. Esquema de cestas de testigos.

forma que como mucho unos B octetos adicionales se pueden aceptar por encima de la velocidad establecida. De esta forma, B es una medida de la longitud permitida para las ráfagas del flujo de datos.

Servicio garantizado

Los elementos claves del servicio garantizado son los siguientes:

- El servicio proporciona un nivel de capacidad o una velocidad de transmisión de datos segura.
- Existe una especificación de un límite superior para el retardo que se sufre en una cola a través de la red. Ésta se tiene que sumar al retardo de propagación, o latencia, para alcanzar el límite en el retardo total a través de la red.
- No existen pérdidas en la cola. Esto es, no se pueden perder paquetes por un desbordamiento de la memoria temporal: los paquetes se pueden perder por fallos en la red o por cambios en los caminos de encaminamiento.

Una de las categorías de aplicaciones que utiliza este servicio es aquella que necesita un límite superior en el retardo de forma que se puede utilizar una memoria temporal de retardos para reproducir en tiempo real los datos entrantes, y de esta forma no se tolera la pérdida de paquetes por la degradación en la calidad de la salida. Otro ejemplo son las aplicaciones con plazos en tiempo real estrictos.

El servicio garantizado es el servicio más demandado de los que proporciona ISA. Ya que el límite en el retardo es firme, éste se tiene que establecer a un valor grande para cubrir casos raros de grandes retardos en colas.

Carga controlada

Los elementos claves del servicio de carga controlada son los siguientes:

- El servicio aproxima estrictamente el comportamiento visible de las aplicaciones que reciben un servicio del mejor esfuerzo bajo condiciones de baja carga.
- No existe una especificación de un límite superior en el retardo de cola a través de la red. Sin embargo, el servicio asegura que un porcentaje elevado de paquetes no experimentarán retardos

que excedan el retardo de tránsito mínimo (es decir, el retardo debido al tiempo de propagación más el tiempo de procesamiento en los dispositivos de encaminamiento sin el retardo de cola).

- Un porcentaje muy alto de paquetes transmitidos son entregados satisfactoriamente (es decir, sin apenas pérdidas en cola).

Como se mencionó, el riesgo en un conjunto de redes que proporcionan QoS a aplicaciones en tiempo real es que se excluya el tráfico de mejor esfuerzo. Esto es así porque los tipos de aplicaciones del mejor esfuerzo utilizan TCP, que se decrementará cuando aparece la congestión o retardos. El servicio de carga controlada garantiza que la red reservará suficientes recursos de forma que una aplicación que reciba este servicio verá una red que responde como si las aplicaciones en tiempo real no estuvieran presentes y compitiendo por los recursos.

El servicio controlado es útil para las aplicaciones que se han referenciado como aplicaciones en tiempo real adaptativas [CLAR92]. Estas aplicaciones no requieren a un límite superior a priori en el retardo a través de la red. En su lugar, el receptor mide la variación del retardo experimentado por los paquetes entrantes y establece el punto de repetición al retardo mínimo que produce todavía una pérdida de velocidad de transmisión suficientemente pequeña (por ejemplo, el vídeo puede ser adaptativo a través de descartar una trama o retrasar el flujo de salida ligeramente; la voz puede ser adaptativa ajustando los periodos de silencio).

DISCIPLINAS DE ATENCIÓN EN COLA

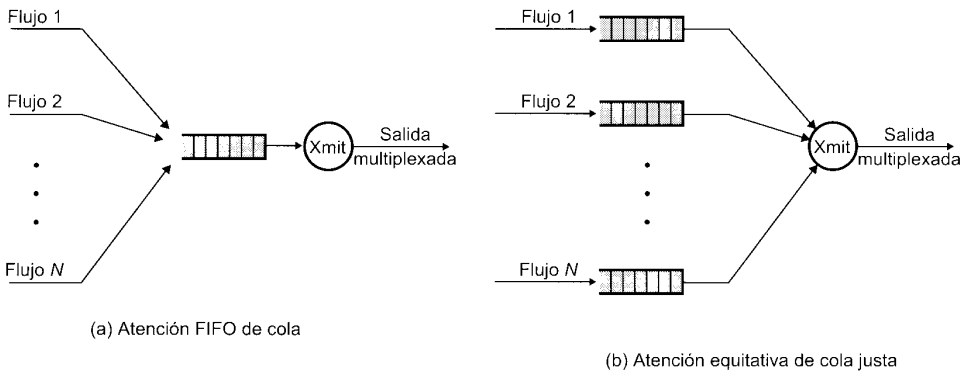
Un componente importante de una implementación ISA es la disciplina de atención de colas utilizada en los dispositivos de encaminamiento. Los dispositivos de encaminamiento han utilizado tradicionalmente la disciplina de atención en cola primero en llegar primero en salir (FIFO) en cada uno de los puertos de salida. En cada puerto de salida se mantiene un cola simple. Cuando llega un paquete y se encamina a un puerto de salida, éste se sitúa al final de la cola. Mientras la cola no esté vacía, el dispositivo de encaminamiento transmite paquetes de la cola, siendo el siguiente el más viejo.

La disciplina FIFO tiene varios inconvenientes:

- No se da ningún tratamiento especial a los paquetes de flujos que tienen una prioridad más alta o que son más sensible al retardo. Si hay cierto número de paquetes de diferentes flujos para reenviar, todos ellos se tratan estrictamente en el orden FIFO.
- Si hay un número de paquetes pequeños que se sitúan en cola después de un paquete grande, entonces la disciplina FIFO da lugar a en un retardo medio por paquete más grande que si los paquetes pequeños se transmiten antes que el grande. En general, los flujos con paquetes grandes obtienen un servicio mejor.
- Una conexión TCP «codiciosa» puede excluir a otras conexiones «altruistas». Si ocurre congestión y una conexión falla al retirarse, las otras conexiones en el camino de este segmento deben retirarse más de lo que deberían hacer en otras circunstancias.

Para resolver los inconvenientes de la disciplina FIFO se utiliza un tipo de esquema de atención equitativo de la cola, en el que un dispositivo de encaminamiento mantiene múltiples colas para cada puerto de salida (Figura 16.9). Con una atención equitativa de la cola y simple cada paquete de entrada se sitúa en una cola para su flujo. Las colas se atienden de una forma cíclica, tomando sucesivamente un paquete de cada cola no vacía. Las colas vacías no se atienden. Este esquema es equitativo en el sentido de que cada flujo consigue enviar exactamente un paquete por ciclo. Además, es también una forma de balancear la carga entre varios flujos. No hay ninguna ventaja para las conexiones «codiciosas. Un flujo codicioso encuentra que su cola se va haciendo más grande, incrementando el retardo, mientras que los otros flujos no se ven afectados por este comportamiento.

Algunos fabricantes han implementado una mejora de la atención equitativa de colas conocido como atención de colas equitativa ponderada (WFQ, Weighted Fair Queuing). De forma resumida, WFQ tiene



(a) Atención FIFO de cola

(b) Atención equitativa de cola justa

Figura 16.9. Atención equitativa en cola FIFO.

en cuenta la cantidad de tráfico en cada cola y asigna más capacidad a la colas más ocupadas sin dejar de atender a las colas menos ocupadas. Además WFQ puede tener en cuenta la cantidad de servicios solicitados por cada flujo de tráfico y ajustar la disciplina de atención en cola adecuadamente.

16.3. RESERVA DE RECURSOS: RSVP

Una tarea clave, tal vez la tarea crucial en una interconexión de redes, es la distribución de datos desde una fuente a uno o más destinos con la calidad del servicio (QoS) solicitada, como puede ser el rendimiento, retardo, variación del retardo, etc. Esta tarea resulta ser de una dificultad creciente en cualquier interconexión cuando se incrementan el número de usuarios, la velocidad de transmisión de las aplicaciones y la utilización de la multidifusión. Ya se ha visto que una herramienta para tratar una demanda elevada de tráfico es el encaminamiento dinámico. Un esquema de encaminamiento dinámico, soportado por protocolos como OSPF o BGP puede responder rápidamente a fallos en un conjunto de redes mediante el encaminamiento alrededor del punto que falla. Más importante incluso, un esquema de encaminamiento dinámico puede, hasta cierto punto, tratar la congestión, primero balanceando la carga de forma que se suaviza la carga a través del conjunto de redes, y segundo encaminando alrededor de las áreas en que se desarrolla la congestión utilizando un encaminamiento de menor coste. En el caso de multidifusión, los esquemas de encaminamiento dinámico se han complementado con capacidades de encaminamiento multidifusión que tienen en cuenta las ventajas de los caminos compartidos desde una fuente a los destinos multidifusión para minimizar el número de paquetes a duplicar.

Para satisfacer las necesidades crecientes en un conjunto de redes, no es suficiente reaccionar a la congestión. Además se necesitan herramientas que prevean la congestión permitiendo a las aplicaciones reservar recursos para una QoS dada. Las medidas preventivas pueden ser útiles en ambos tipos de transmisión, monodifusión y multidifusión. Para la monodifusión, dos aplicaciones se ponen de acuerdo en una calidad de servicio específica para una sesión y esperan que la función de interconexión soporte esa calidad de servicio. Si la función de interconexión está muy cargada, puede ocurrir que no se proporcione la QoS deseada y se distribuyan los paquetes a una QoS reducida. En este caso, las aplicaciones podrían preferir esperar antes de iniciar la sesión o al menos ser alertadas de la reducción potencial en la QoS. Una forma de tratar esta situación es hacer que la aplicación monodifusión reserve recursos para garantizarse una calidad de servicio determinada. Los dispositivos de encaminamiento a lo largo del camino posible pueden entonces preasignar recursos (espacio en las colas, capacidad de salida) para asegurar la QoS deseada. Si un dispositivo de encaminamiento no puede satisfacer la reserva de recursos debido a reservas vigentes hechas con anterioridad, entonces se informa a las aplicaciones de este hecho. Así, las aplicaciones podrían elegir entre intentarlo de nuevo a una reserva de QoS reducida o intentarlo más tarde.

La transmisión multidifusión presenta un caso mucho más apremiante para la implementación de la reserva de recursos. Un transmisión multidifusión puede generar una cantidad enorme de tráfico de interconexión si la aplicación es de gran volumen (por ejemplo, vídeo) o el grupo de multidifusión destino es grande y disperso, o ambas cosas al mismo tiempo. Lo que fuerza el caso de la reserva de recursos multidifusión es que mucha de la carga potencial generada por una fuente multidifusión se puede prever de forma fácil. Esto es así por dos razones:

1. Algunos de los miembros de un grupo multidifusión existente pueden que no necesiten la distribución desde una fuente determinada durante un periodo de tiempo dado. Por ejemplo, pueden haber dos «canales» (dos fuentes multidifusión) transmitiendo a un grupo multidifusión particular al mismo tiempo. Un destino multidifusión podría querer «sintonizar» sólo uno de los canales en un momento dado.
2. Algunos miembros de un grupo sólo podrían ser capaces de gestionar una porción de la transmisión de la fuente. Por ejemplo, una fuente de vídeo puede transmitir un flujo de vídeo que consta de dos componentes: una componente básica que proporciona una calidad de imagen reducida y una componente mejorada. Algunos receptores pueden que no tengan la potencia de procesamiento para tratar la componente mejorada o pueden estar conectados a la función de interconexión a través de una red o enlace que no tiene la capacidad para la señal completa.

En consecuencia, la utilización de la reserva de recursos puede habilitar a los dispositivos de encaminamiento a decidir con antelación si pueden satisfacer las necesidades de transporte de una transmisión multidifusión a todos los destinos multidifusión indicados y reservar si es posible los recursos apropiados.

La reserva de recursos en un conjunto de redes se diferencia del tipo de reserva de recursos que se pueden implementar en una red orientada a conexión, como es ATM o la retransmisión de tramas. Un esquema de reserva de recursos en un conjunto de redes debe interaccionar con una estrategia de encaminamiento dinámica que permita cambiar la ruta seguida por los paquetes de una transmisión dada. Cuando la ruta cambia, las reservas de recursos deben cambiar. Para tratar esta situación dinámica se utiliza el concepto de estado flexible («soft»). Un estado flexible es simplemente un conjunto de información de estado en un dispositivo de encaminamiento que expira a menos que la entidad que solicita el estado la refresque regularmente. Si la ruta de una transmisión dada cambia, algunos estados flexibles expiran y la reserva de recursos invocará los estados flexibles apropiados a los dispositivos de encaminamiento a lo largo de la ruta. Así, el sistema final que solicita recursos debe renovar periódicamente sus solicitudes durante el curso de la transmisión de una aplicación.

Centramos ahora nuestra atención en el protocolo que se ha desarrollado para llevar a cabo la reserva de recursos en un entorno de un conjunto de redes: el protocolo de reserva de recursos RSVP (Resource ReSerVation Protocol) definido en el RFC 2205.

CARACTERÍSTICAS Y METAS DE RSVP

Las metas de diseño que guiaron el desarrollo de las especificaciones de RSVP son las siguientes [ZHAN95]:

1. Proporcionar la capacidad de hacer reservas a receptores heterogéneos diseñados específicamente para sus propias necesidades. Como se ha mencionado, algunos miembros de un grupo multidifusión pueden ser capaces de manejar o pueden que quieran manejar sólo una parte de la transmisión multidifusión, como puede ser la componente de baja resolución de una señal de vídeo. Se debe permitir diferenciar reservas de recursos entre los miembros del mismo grupo multidifusión.
2. Tratar elegantemente los cambios en la pertenencia a un grupo multidifusión. La pertenencia a un grupo puede ser dinámica. De esta forma, la reserva debe ser dinámica y, de nuevo, esto sugiere que son necesarias las reservas dinámicas separadas para cada miembro del grupo multidifusión.

3. Especificar necesidades de recursos de tal forma que el total de los recursos reservados para un grupo de multidifusión refleje realmente los recursos necesarios. El encaminamiento multidifusión tiene lugar sobre un árbol de forma que la duplicación de paquetes se minimice. Por lo tanto, cuando se reservan recursos para miembros individuales de un grupo, estas reservas se tienen que agregar para tener en cuenta los segmentos de caminos comunes por las rutas a los diferentes miembros del grupo.
4. Permitir a los receptores seleccionar una fuente entre varias fuentes que transmiten a un grupo multidifusión. Ésta es la capacidad de cambiar de canal descrita antes.
5. Tratar elegantemente los cambios en las rutas, restablecer automáticamente la reserva de recursos a lo largo de un camino nuevo mientras los recursos adecuados estén disponibles.
6. Controlar la información suplementaria del protocolo. Justo cuando las reservas de recursos se agregan para tener ventaja de los segmentos de caminos comunes entre receptores multidifusión los mensajes RSVP de solicitud de reserva se deben de agregar para minimizar la cantidad de tráfico RSVP en el conjunto de redes.
7. Ser independiente del protocolo de encaminamiento. RSVP no es un protocolo de encaminamiento, su tarea es establecer y mantener las reservas de recursos sobre un camino o un árbol de distribución, independientemente de cómo se creó el camino o el árbol.

Basándose en estas metas de diseño, el RFC 2205 especifica las características siguientes de RSVP:

- **Monodifusión y multidifusión:** RSVP hace reservas para ambos tipos de transmisión, adaptando dinámicamente a los cambios en las pertenencias a grupos así como en los cambios de rutas y reservando recursos basándose en las necesidades individuales de los miembros de multidifusión.
- **Simplex:** RSVP hace reservas para flujos de datos unidireccionales. El intercambio de datos entre dos sistemas finales requiere reservas separadas en las dos direcciones.
- **Reserva iniciada por el receptor:** el receptor de un flujo de datos inicia y mantiene la reserva de recursos para ese flujo.
- **Mantenimiento de estado flexible en el conjunto de redes:** RSVP mantiene un estado flexible en los dispositivos de encaminamiento intermedios y deja la responsabilidad de mantener estos estados de reserva a los usuarios finales.
- **Suministro de diferentes estilos de reserva:** éstos permiten a los usuarios de RSVP especificar cómo las reservas para el mismo grupo multidifusión se deberían agregar en los conmutadores intermedios. Esta característica habilita un uso más eficiente de los recursos del conjunto de redes.
- **Operación transparente a través de dispositivos de encaminamiento no RSVP:** ya que la reserva y RSVP son independientes del protocolo de encaminamiento, no existen conflictos fundamentales en un ambiente mixto en el que algunos dispositivos de encaminamiento no utilizan RSVP. Estos dispositivos de encaminamiento simplemente utilizarán la técnica de transporte del mejor esfuerzo.
- **Soporte a IPv4 e IPv6:** RSVP puede hacer uso del campo «Tipo de Servicio» en la cabecera IPv4 y del campo «Etiqueta de Flujo» de la cabecera IPv6.

Merece la pena profundizar en dos de estas características de diseño: la reserva iniciada por el receptor y el estado flexible.

Reserva iniciada por el receptor

Los intentos previos realizados sobre reserva de recursos, y el enfoque tomado en las redes ATM y retransmisión de tramas, eran para que la fuente de un flujo de datos solicitara un conjunto dado de recursos. En un ambiente estrictamente monodistribución, este enfoque es razonable. Una aplicación que transmite es capaz de transmitir datos a una cierta velocidad de transmisión y tiene una calidad de

servicio dada dentro del esquema de transmisión. Sin embargo, esta propuesta es inadecuada para la multidifusión. Si el flujo de transmisión de una fuente se puede dividir en componentes, subflujos, entonces algunos de los miembros de multidifusión podrían requerir sólo un único subflujo. Si hay múltiples fuentes transmitiendo a un grupo de multidifusión, entonces un receptor particular de este grupo podría querer seleccionar sólo una o un subconjunto de fuentes para recibir la información de ellas. Finalmente, las necesidades en QoS de los diferentes receptores pueden diferir dependiendo de la salida del equipo, la potencia de procesamiento y la velocidad del enlace del receptor.

Por lo tanto, tiene sentido que sean los receptores y no las fuentes los que hagan la reserva de recursos. Una fuente necesita proporcionar a los dispositivos de encaminamiento las características del tráfico de la transmisión (velocidad de transmisión, variabilidad), pero son los receptores lo que deben especificar la QoS deseada. Los dispositivos de encaminamiento pueden entonces agregar las reservas de recursos de multidifusión para aprovecharse de los segmentos de caminos compartidos a lo largo del árbol de distribución.

Estado flexible

RSVP hace uso del concepto de estado flexible. Este concepto fue introducido por primera vez por David Clark en [CLAR88], y merece la pena destacar su descripción[2]:

> Mientras que el datagrama ha sido muy útil a la hora de resolver las metas más importantes de Internet, las metas de la gestión y responsabilidad de los recursos han demostrado que son difíciles de alcanzar. La mayoría de los datagramas son parte de alguna secuencia de paquetes desde un origen a un destino, en vez de ser unidades aisladas del nivel de aplicación. Sin embargo, las pasarelas no pueden ver directamente la existencia de esta secuencia ya que se ven forzadas a tratar cada paquete aisladamente. Por lo tanto, las decisiones de gestión de recursos o la contabilidad deben hacerse en cada paquete separadamente.
>
> Esto sugiere que debería existir un bloque de construcción mejor que el datagrama para la siguiente generación de arquitectura. La característica general de este bloque de construcción es que identificaría una secuencia de paquetes viajando desde un origen a un destino. He utilizado el término flujo para caracterizar este bloque de construcción. Sería necesario que las pasarelas tuvieran un estado de flujo para poder recordar la naturaleza de los flujos que pasan a través de ellas, pero la información de estado no debería ser crítica a la hora de mantener el tipo de servicio descrito asociado con el flujo. En su lugar, ese tipo de servicio se debería forzar por los sistemas finales, que periódicamente enviarían mensajes para asegurar que el tipo de servicio se está asociando con el flujo correctamente. De esta forma, la información de estado asociada con el flujo se podría perder en una caída sin interrumpir permanentemente las características del servicio que está siendo utilizado.

En esencia, un esquema orientado a conexión hace uso de un enfoque de estado rígido («hard»), en el que la naturaleza de las conexiones a lo largo de una ruta fija está definida por la información de estado en los nodos de conmutación intermedios. RSVP hace uso de un enfoque de estado flexible, o no orientado a conexión, en el que el estado de reserva es información almacenada temporalmente en los dispositivos de encaminamiento que están instalados y se refresca periódicamente por los sistemas finales. Si un estado no se refresca dentro del límite de tiempo requerido el dispositivo de encaminamiento descarta el estado. Si se prefiere una nueva ruta para un flujo dado, el sistema final proporciona la reserva a los dispositivos de encaminamiento nuevos en la ruta.

FLUJOS DE DATOS

La base del funcionamiento de RSVP la forman tres conceptos relacionados con los flujos de datos: sesión, especificación de flujo y especificación de filtro.

---

[2] *Pasarela* es el termino utilizado para designar al *dispositivo de encaminamiento* en la mayoría de los primeros RFC en la literatura de TCP/IP; y todavía se utiliza ocasionalmente (por ejemplo, Protocolo de Pasarela Frontera).

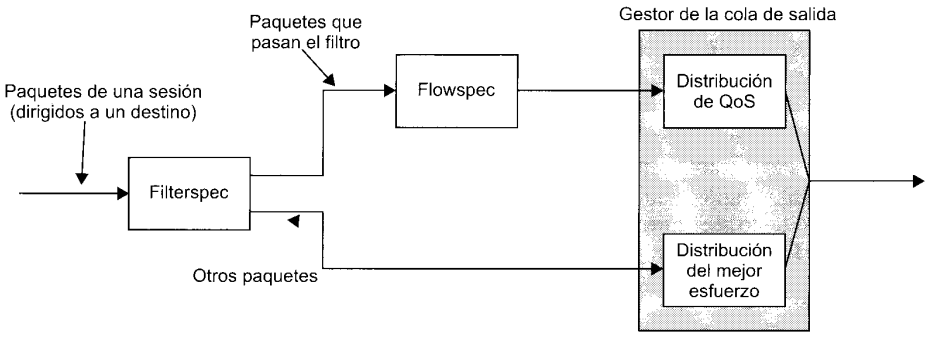


Figura 16.10. Tratamiento de los paquetes de una sesión en un dispositivo de encaminamiento.

Una **sesión** es un flujo de datos identificado por su destino. Una vez que se ha hecho la reserva en un dispositivo de encaminamiento por un destino particular, el dispositivo de encaminamiento considera esto como una sesión y asigna recursos durante la vida de esta sesión.

Se llama **descriptor de flujo** a una solicitud de reserva emitida por un sistema final destino y consta de una **especificación de flujo** (flowspec) y un **filtro de flujo** (filterspec). La especificación de flujo indica una calidad de servicio deseada y se utiliza para establecer parámetros en el gestor de salida de paquetes de un nodo. Esto es, el dispositivo de encaminamiento transmitirá los paquetes con un conjunto dado de preferencias basándose en la especificación de flujo actual. La especificación de filtro define un conjunto de paquetes para los que se solicita la reserva. Así, la especificación de filtro y la sesión definen el conjunto de paquetes, o flujo, que van a recibir la QoS deseada. Cualquier otro paquete que va dirigido al mismo destino se trata como tráfico del mejor esfuerzo.

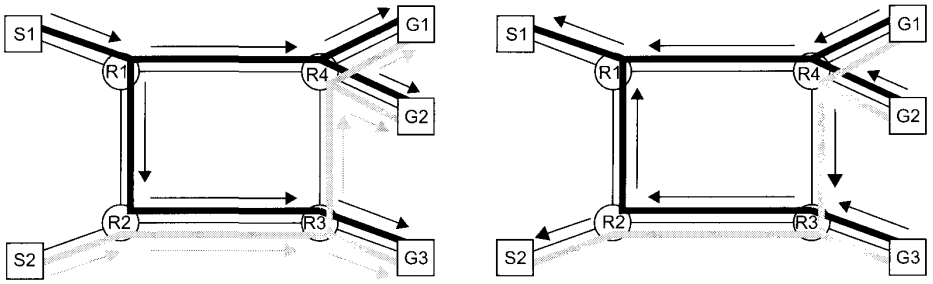
El contenido de la especificación de flujo está más allá del ámbito de RSVP, que simplemente es un portador de solicitudes. En general, la especificación de flujo contiene una clase de servicio, una Rspec (R de reserva, especificación de reserva) y una Tspec (T de tráfico, especificación de tráfico). La clase de servicio es un identificador de un tipo de servicio que se está solicitando. Los otros dos parámetros son conjuntos de valores numéricos. El parámetro Rspec define la calidad de servicio deseada y el parámetro Tspec describe el flujo de datos. Los contenidos de Rspec y Tspec son opacos a RSVP.

En principio, la especificación de filtro puede designar un subconjunto arbitrario de los paquetes de una sesión (es decir, los paquetes que llegan con el destino especificado por esta sesión). Por ejemplo, la especificación de filtro podría especificar solamente fuentes específicas, o protocolos origen específicos, o en general, solamente paquetes que coinciden en ciertos campos en cualquiera de las cabeceras de protocolo en el paquete.

La Figura 16.10 indica la relación entre sesión, especificación de flujo y especificación de filtro. Cada paquete de entrada es parte de, como mucho, una sesión y se trata de acuerdo al flujo lógico indicado en la figura para esa sesión. Si un paquete no pertenece a ninguna sesión se le da un servicio de distribución del mejor esfuerzo.

FUNCIONAMIENTO DE RSVP

Una gran parte de la complejidad de RSVP tiene que ver con el tratamiento de la transmisión multidifusión. La transmisión monodifusión se trata como un caso especial. En la Figura 16.11a se muestra un ejemplo de configuración multidifusión. Esta configuración implica a cuatro dispositivos de encaminamiento. El enlace entre cualquier par de dispositivos de encaminamiento, indicado por una línea delgada negra, puede ser un enlace punto-a-punto o una red. Hay tres computadores, G1, G2 y G3, que son miembros de un grupo multidifusión y pueden recibir datagramas con la correspondiente dirección



(a) Distribución de datos a un grupo de multidifusión (b) Mensajes Resv fusionados

Figura 16.11. Funcionamiento RSVP.

destino de multidifusión. Hay dos computadores, S1 y S2, que transmiten datos a esta dirección de multidifusión. Las líneas negras gruesas indican el árbol de encaminamiento para la fuente S1 y este grupo multidifusión, y la línea gris gruesa indica el árbol de encaminamiento para S2 y este mismo grupo. Las flechas indican la transmisión de paquetes desde S1 (negras) y S2 (grises).

Podemos ver que los cuatro dispositivos de encaminamiento necesitan estar seguros de las reservas de recursos de cada destino multidifusión. Así, las solicitudes de reserva desde los destinos deben propagarse hacia atrás a través de los árboles de encaminamiento hacia cada computador potencial.

MECANISMOS DEL PROTOCOLO RSVP

RSVP utiliza dos tipos de mensajes básicos: Resv y Path. Los mensajes Resv se originan en los receptores de un grupo de multidifusión y se propagan hacia arriba a través del árbol de distribución siendo fusionados y empaquetados cuando es apropiado en cada nodo a lo largo del camino. Estos mensajes crean estados flexibles dentro de los dispositivos de encaminamiento del árbol de distribución que define los recursos reservados para esta sesión (esta dirección multidifusión). Finalmente, los mensajes fusionados Resv llegan a los computadores origen para establecer los parámetros de control de tráfico apropiados para el primer salto. La Figura 16.11b indica el flujo de los mensajes Resv. Hay que notar que los mensajes se fusionan de forma que sólo un único mensaje viaja hacia arriba a lo largo de cualquier rama de los árboles de distribución combinados. Sin embargo, estos mensajes se deben repetir periódicamente para mantener los estados flexibles.

El mensaje Path se utiliza para proporcionar información de encaminamiento hacia arriba. En todos los protocolos de encaminamiento multidifusión actualmente en uso sólo se mantiene una ruta hacia abajo, en la forma de un árbol de distribución. Sin embargo, los mensajes Resv se deben propagar hacia arriba a través de todos los dispositivos de encaminamiento intermedios y hacia todos los computadores origen. En ausencia de información de encaminamiento inversa a partir de los protocolos de encaminamiento, RSVP proporciona esto con los mensajes Path. Cada computador que desea participar como origen en un grupo multidifusión emite un mensaje Path que se transmite a través del árbol de distribución a todos los destinos multidifusión. A lo largo del camino, cada dispositivo de encaminamiento y cada computador destino crea un estado de camino que indica el salto inverso que hay que utilizar para ese origen. La Figura 16.11a indica los caminos seguidos por estos mensajes, que son los mismos que siguen los paquetes de datos.

Desde la perspectiva de un computador, el funcionamiento del protocolo se puede describir como sigue:

a) Un receptor se une a un grupo multidifusión enviando un mensaje de unión IGMP a un dispositivo de encaminamiento vecino.

b) Un origen potencial emite un mensaje Path a la dirección de grupo multidifusión.

c) Un receptor recibe un mensaje Path identificando al origen.

d) Ahora el receptor tiene información del camino inverso, puede empezar a enviar mensajes Resv, especificando los descriptores de flujo deseados.

e) Los mensajes Resv se propagan a través de las redes interconectadas y se entregan al origen.

f) El origen comienza a enviar paquetes de datos.

g) El receptor comienza a recibir paquetes de datos.

Los pasos a y b pueden producirse en cualquier orden.

16.4. SERVICIOS DIFERENCIADOS (DS)

La Arquitectura de Servicios Integrados (ISA) y RSVP están pensadas para permitir ofrecer calidad de servicios (QoS) en Internet y en redes privadas. Aunque ISA en general y RSVP en particular son herramientas útiles para este propósito, estas características son relativamente complejas de implementar. Además, puede que no se pueda escalar bien para tratar grandes volúmenes de tráfico debido a la cantidad de señales de control necesarias para coordinar la oferta de QoS integradas y debido al mantenimiento de la información de estado necesaria en los dispositivos de encaminamiento.

A medida que la carga en Internet crece, así como la variedad de aplicaciones, existe una necesidad inmediata de proporcionar niveles diferenciados de QoS a diferentes flujos de tráfico. La arquitectura de servicios diferenciados (DS) (RFC 2475) está diseñada para proporcionar una herramienta simple, fácil de implementar y con poca información suplementaria que permita un rango de servicios de red que están diferenciados sobre la base del rendimiento.

Varias características claves de DS contribuyen a su eficiencia y facilitan su implementación:

- Los paquetes IPv4 se etiquetan para un tratamiento de QoS diferenciado utilizando el octeto de tipo de Servicio de IPv4 (Figura 15.4) o el octeto de Clase de Tráfico de IPv6 (Figura 15.11). De esta forma, no se necesitan cambios en IP.
- Antes de utilizar DS se establece un acuerdo de nivel de servicio (SLA, Servicce Layer Agreement) entre el proveedor de servios (dominio de Internet) y el cliente. Esto evita la necesidad de incorporar los mecanismos DS en las aplicaciones. Así, no se necesita modificar las aplicaciones existentes para utilizar DS.
- DS proporciona un mecanismo de agregación integrado. Todo el tráfico con el mismo octeto DS se trata por el mismo servicio de red. Por ejemplo, múltiples conexiones de voz no se tratan de forma individual sino en conjunto. Esto permite escalar de forma apropiada redes y cargas de tráfico grandes.
- DS se implementa en dispositivos de encaminamiento individuales por medio de la atención en cola y el encaminamiento basándose en el octeto DS. Los dispositivos de encaminamiento tratan cada paquete individualmente y no tienen que guardar información de estado sobre flujos de paquetes.

Aunque DS está pensado para proporcionar un servicio simple basándose en mecanismos relativamente simples, el conjunto de RFC relacionados con DS es relativamente complejo. La Tabla 16.3 resume algunos de los términos claves obtenidos de estas especificaciones.

SERVICIOS

El tipo de servicio de DS se proporciona dentro de un domino DS, que se define como una porción continua de Internet sobre la que se administra un conjunto consistente de políticas DS. Normalmente,

Tabla 16.3. Terminología de los Servicios Diferenciados.

Agregados de comportamiento	Un conjunto de paquetes con el mismo código DS cruzando un enlace en una dirección particular.
Clasificador	Paquetes seleccionados basándose en el campo DS (clasificador BA) o en campos múltiples dentro de la cabecera del paquete (clasificador MF).
Nodo frontera DS	Un nodo DS que conecta un dominio DS a otro nodo en otro dominio.
Código DS	Un valor específico de la porción DSCP de 6 bits del campo DS de 8 bits en la cabecera IP.
Dominio DS	Un conjunto continuo (conectados) de nodos, capaces de implementar servicios diferenciados, que operan con un conjunto común de políticas de suministro de servicios y definiciones de comportamiento en cada salto.
Nodo interior DS	Un nodo DS que no es un nodo frontera DS.
Nodo DS	Un nodo que suministra servicios diferenciados. Normalmente, un nodo DS es un dispositivo de encaminamiento. Un computador que proporciona servicios diferenciados para sus aplicaciones también es un nodo DS.
Descarte	El proceso de descartar paquetes basándose en reglas específicas; también llamadas políticas.
Marcado	El proceso de fijar el código DS en un paquete. Los paquetes se pueden marcar en el inicio o pueden ser remarcados por un nodo DS en la ruta.
Medición	El proceso de medir las propiedades temporales (por ejemplo, la velocidad de transferencia) del flujo de paquetes por un medidor. El estado instantáneo de ese proceso podría afectar las funciones de marcado, modelado y de descarte.
Comportamiento en cada salto (PHB)	El comportamiento de reenvío observable desde fuera aplicado en un nodo a un agregado de comportamientos.
Acuerdo de nivel de servicio (SLA)	Un contrato de servicio entre un cliente y un proveedor de servicios.
Modelado	El proceso de retrasar paquetes en un flujo de paquetes para ver si se ajusta a algún perfil de tráfico predefinidos.
Acondicionamiento de tráfico	Funciones de control implementadas para forzar reglas especificadas en un TCA, que incluye medición, marcado, modelado y descarte.
Acuerdo de acondicionamiento de tráfico (TCA)	Un acuerdo que especifica reglas de clasificación y reglas de acondicionamiento de tráfico que se aplican a los paquetes seleccionados por el clasificador.

un domino DS debería estar bajo el control de una única entidad administrativa. Los servicios proporcionados a través de un domino DS se definen en el acuerdo de nivel de servicio (SLA), que es el contrato de servicio entre el cliente y el proveedor de servicios que especifica el servicio de reenvío que recibirá el cliente para varias clases de paquetes. Un cliente podría ser una organización u otro dominio DS. Una vez que se establece el SLA, el cliente emite paquetes con el octeto DS marcado para indicar la clase de paquete. El proveedor de servicios debe asegurar que el cliente obtiene al menos la QoS acordada para cada clase de paquete. Para proporcionar esa QoS el proveedor de servicios debe configurar las políticas de reenvío apropiadas en cada dispositivo de encaminamiento (basándose en el valor del octeto DS) y debe medir el rendimiento que se está proporcionando a cada clase sobre una base de salida.

Si un cliente envía un paquete dirigido para varios destinos dentro del domino DS, entonces se espera que el dominio DS proporcione el servicio acordado. Si el destino está más allá del dominio DS del cliente, entonces el dominio DS intentará reenviar los paquetes a través de otros dominios, solicitando el servicio más apropiado que se parezca al servicio solicitado.

Un documento preliminar sobre el entorno de trabajo DS indica los siguientes parámetros detallados de funcionamiento que se podrían incluir en una SLA:

- Parámetros detallados de prestaciones del servicio, tal como rendimiento esperado, probabilidad de descarte y latencia.
- Restricciones en los puntos de entrada y salida a través de los que se suministra el servicio, indicando el ámbito del servicio.
- Perfiles de tráfico a los que se ha de adherir para recibir el servicio solicitado, como, por ejemplo, los parámetros de la cesta de testigos.
- Disposición del tráfico enviado en exceso del perfil especificado.

Este documento de trabajo proporciona también algunos ejemplos de servicios que se podrían suministrar:

1. El tráfico ofrecido en el nivel de servicio A será distribuido con una latencia baja.
2. El tráfico ofrecido en el nivel de servicio B será distribuido con una tasa de pérdida baja.
3. El noventa por ciento del perfil de tráfico distribuido en el nivel de servicio C no experimentará más de 50 ms de latencia.
4. El noventa y cinco por ciento del perfil de tráfico distribuido en el nivel de servicio D será distribuido.
5. El tráfico ofrecido en el nivel de servicio E tendrá asignado el doble de ancho de banda que el tráfico ofrecido en el nivel de servicio F.
6. El tráfico con precedencia de descarte X tiene una probabilidad mayor de distribución que el tráfico con precedencia de descarte Y.

Los primeros dos ejemplos son cualitativos y son sólo válidos al hacer la comparación con otro tipo de tráfico, como el tráfico por defecto que obtiene un servicio del mejor esfuerzo. Los dos ejemplos siguientes son cuantitativos y proporcionan una garantía específica que puede ser verificada mediante la medida del servicio real sin comparar con otros servicios ofrecidos al mismo tiempo. Los dos ejemplos finales son una mezcla de cualitativo y cuantitativo.

OCTETO DS

Los paquetes se etiquetan para el servicio que los trata por medio del octeto DS, que se sitúa en el campo Tipo de Servicio de la cabecera IPv4 o en el campo Clase de Tráfico de la cabecera IPv6. El RFC 2474 define el octeto DS como aquél con el siguiente formato: los 6 bits a la izquierda forman el código DS y los dos bits a la derecha no se utilizan actualmente. El código DS es la etiqueta DS utilizada para clasificar los paquetes para los servicios diferenciados.

Con un código de 6 bits, existen en principio 64 clases de tráfico diferentes que se podrían definir. Estos 64 códigos se agrupan en tres conjuntos de códigos como se indica a continuación:

- Los códigos de la forma xxxxx0, donde x es 0 o 1, están reservados para una asignación estándar.
- Los códigos de la forma xxxx11 están reservados para un uso experimental o local.
- Los códigos de la forma xxxx01 están también reservados para un uso experimental o local, pero se podrían asignar para estándares futuros actuando según se necesite.

En el RFC 2474 se hacen varias asignaciones dentro del primer grupo. El código 000000 es la clase de paquete por defecto. La clase por defecto es el comportamiento de reenvío del mejor esfuerzo en los dispositivos de encaminamiento existentes. Tales paquetes se reenvían en el orden en el que son recibidos tan pronto como la capacidad del enlace esté disponible. Si hay disponibles para transmitir otros paquetes de una prioridad más alta en otras clases DS, se les da precedencia sobre los paquetes del mejor esfuerzo.

Los códigos de la forma xxx000 están reservados para proporcionar compatibilidad hacia atrás con el servicio de precedencia de IPv4. Para explicar esta necesidad, necesitamos realizar una explicación del servicio de precedencia IPv4. El campo Tipo de Servicio (TOS, Type Of Service) de IPv4 incluye dos subcampos, un campo de precedencia de 3 bits y un subcampo de TOS de 4 bits. Estos subcampos sirven funciones complementarias. El subcampo TOS proporciona una guía a la entidad IP (en el origen o en el dispositivo de encaminamiento) para seleccionar el siguiente salto para el datagrama, y el subcampo precedencia proporciona una guía sobre la asignación relativa de los recursos del dispositivo de encaminamiento para el datagrama.

El campo de precedencia se establece para indicar el grado de urgencia o prioridad que se le va a asociar a un datagrama. Si el dispositivo de encaminamiento permite el subcampo de precedencia, se *tienen tres enfoques para responder*:

- **Selección de ruta:** se puede seleccionar una ruta particular si el dispositivo de encaminamiento tiene una cola pequeña para esa ruta o si el siguiente salto para esa ruta permite la precedencia o prioridad de red (por ejemplo, una red de paso de testigo permite prioridad).
- **Servicio de red:** si la red en el siguiente salto permite precedencia se invoca ese servicio.
- **Disciplina de atención en cola:** un dispositivo de encaminamiento puede utilizar precedencia para influir en cómo se tratan la colas. Por ejemplo, un dispositivo de encaminamiento puede dar un tratamiento preferencial en la colas a datagramas con una precedencia más alta.

Los requerimientos del RFC 1812, para los dispositivos de encaminamiento con IP Versión 4, proporcionan recomendaciones para la disciplina de atención en colas que se engloban en dos categorías:

- **Servicio de cola**
  - — Los dispositivos de encaminamiento deberían implementar un servicio de cola ordenado por precedencia. Un servicio de cola ordenado por precedencia significa que cuando se selecciona un paquete para su salida en un enlace (lógico), se envía el paquete con la precedencia más alta que ha sido situado en cola para ese enlace.
  - — Cualquier dispositivo de encaminamiento PODRÍA implementar otros criterios basados en procedimientos de gestión del rendimiento que resulten en algo diferente a la ordenación de precedencia estricta, pero DEBE ser configurable para suprimirlos (es decir, utilización de la ordenación estricta).
- **Control de congestión.** Cuando un dispositivo de encaminamiento recibe un paquete cuando ya ha superado su capacidad de almacenamiento debe descartarlo, o descartar a otro paquete o a otros paquetes.
  - — Un dispositivo de encaminamiento PODRÍA descartar el paquete justo cuando lo recibe; esto es lo más simple pero no es la mejor política.
  - — Idealmente, el dispositivo de encaminamiento seleccionaría el paquete de uno de las sesiones que están abusando más del enlace, dado que la política aplicable de QoS permite esto. Una política recomendable en un entorno de datagramas utilizando colas FIFO es descartar un paquete seleccionado aleatoriamente de la cola. Un algoritmo equivalente en dispositivos de encaminamiento que utilicen colas justas es descartar de la cola más larga. Un dispositivo de encaminamiento PODRÍA utilizar estos algoritmos para determinar qué paquete descarta.
  - — Si se implementa un servicio de cola con ordenación de precedencia y está habilitada, el dispositivo de encaminamiento NO DEBE descartar paquetes cuya precedencia IP es más alta que un paquete que no se descarta.
  - — Un dispositivo de encaminamiento PODRÍA proteger paquetes cuya cabecera IP solicita la máxima seguridad TOS, excepto en el caso en que lo que se hace viole reglas previas.

— Un dispositivo de encaminamiento PODRÍA proteger paquetes IP fragmentados, basándose en la teoría de que descartando un fragmento de un datagrama podría incrementar la congestión debido a que la fuente debería retransmitir todos los fragmentos del paquete.

— Para ayudar a prevenir las perturbaciones en el encaminamiento o la interrupción de las funciones de gestión, el dispositivo de encaminamiento PODRÍA proteger para que no se descarten los paquetes utilizados para el control de la congestión, control de enlace o gestión de red. Los dispositivos de encaminamiento dedicados (es decir, dispositivos de encaminamiento que no son computadores de propósito general, servidores de terminales, etc.) pueden alcanzar una aproximación a esta regla protegiendo los paquetes cuya fuente o destino es el propio dispositivo de encaminamiento.

Los códigos DS de la forma xxx000 deberían proporcionar un servicio que como mínimo es equivalente a la funcionalidad de precedencia de IPv4.

CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS DS

La Figura 16.12 muestra el tipo de configuración prevista en los documentos DS. Un dominio DS consta de un conjunto de dispositivos de encaminamiento contiguos, esto es, es posible ir desde cualquier dispositivo de encaminamiento en el dominio a cualquier otro dispositivo de encaminamiento en el dominio a través de un camino que no incluye dispositivos de encaminamiento de fuera del dominio. Dentro de un dominio, la interpretación de los códigos DS es uniforme, de forma que se suministra un servicio uniforme y consistente.

Los dispositivos de encaminamiento en un dominio DS pueden ser nodos fronteras o nodo interiores. Normalmente, los nodos interiores implementan mecanismos simples para tratar los paquetes basándose en los valores de su código DS. Esto incluye la disciplina para atender la cola para dar un tratamiento preferencial dependiendo del valor del código y de la reglas de descarte de paquetes que dictan qué

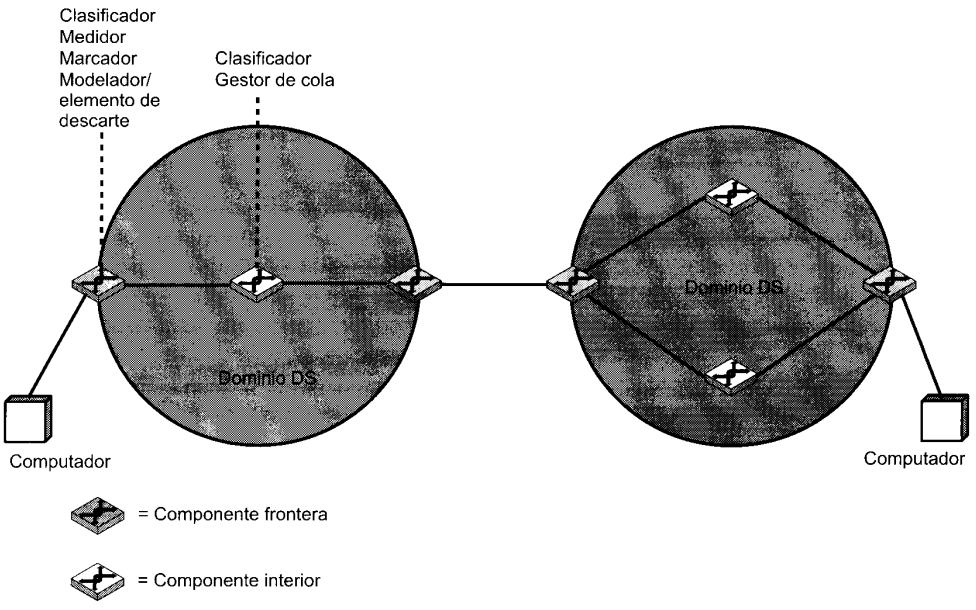


Figura 16.12. Dominios DS.

paquetes se deberían descartar primero, en el caso de que se saturase la memoria temporal. Las especificaciones de DS indican, el tratamiento de reenvío proporcionado en un dispositivo de encaminamiento como un comportamiento por saltos (PHB, Per-Hop Behavior). Este PHB debe estar disponible en todos los dispositivos de encaminamiento y normalmente el PHB es la única parte de DS implementado en los dispositivos de encaminamiento interiores.

Los nodos fronteras incluyen mecanismos PHB pero también incluyen mecanismos más sofisticados de acondicionamiento del tráfico necesarios para proporcionar el servicio deseado. Así, los dispositivos de encaminamiento interiores tienen una funcionalidad mínima y un intercambio mínimo de información suplementaria al proporcionar el servicio DS, mientras que la mayor parte de la complejidad está en los nodos frontera. La función de un nodo frontera también la puede suministrar un computador del dominio en beneficio de las aplicaciones de ese computador.

La función de acondicionamiento del tráfico consta de cinco elementos:

- **Clasificador:** separa los paquetes enviados en clases diferentes. Esto es la base del suministro de servicios diferenciados. Un clasificador podría separar el tráfico sobre la base del código DS (comportamiento del clasificador de agregados) o sobre la base de campos múltiples dentro de la cabecera del paquete o incluso de los datos del paquete (clasificador múltiple).
- **Medidor:** mide el tráfico enviado que se ajusta a un perfil. El medidor determina si una clase de flujo de paquetes dada está dentro o excede el nivel de servicio garantizado para esa clase.
- **Marcador:** controla el tráfico mediante el remarcado de los paquetes con un código diferente según se necesite. Esto se podría hacer a aquellos paquetes que excedan el perfil, por ejemplo, si se garantiza un rendimiento dado para una clase de servicio particular, cualquier paquete en esta clase que exceda el rendimiento en algún intervalo de tiempo definido se puede remarcar para tratarse por medio del mejor esfuerzo. También es posible necesitar el remarcado en el límite entre dos dominios DS. Por ejemplo, si una clase de tráfico dada va a recibir la prioridad más alta, y ésta es el valor 3 en un dominio y 7 en el dominio siguiente, los paquetes con una prioridad que viajan desde el primer dominio al segundo se remarcan con prioridad 7 cuando entran en el segundo dominio.
- **Modelador:** controla el tráfico retardando paquetes tanto como sea necesario para que el flujo de paquetes en una clase dada no exceda la velocidad de transferencia especificada en el perfil para esa clase.
- **Elemento de descarte:** descarta paquetes cuando la velocidad de transferencia de paquetes de una clase dada excede la especificada en el perfil de esa clase.

La Figura 16.13 muestra la relación entre los elementos de acondicionamiento del tráfico. Después de la clasificación de un flujo, se mide su consumo de recursos. La función de medida mide el volumen de paquetes en un intervalo de tiempo dado para determinar el cumplimiento del flujo con el acuerdo de tráfico. Si el computador tiene un comportamiento de transmisión a ráfagas, puede que no sea suficiente

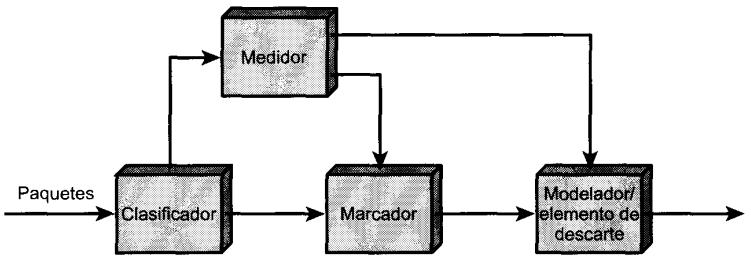


Figura 16.13. Acondicionamiento de tráfico DS.

la simple velocidad de transmisión de datos o de paquetes para capturar las características de tráfico deseadas. Un ejemplo de la forma de definir un perfil de tráfico para tener en cuenta la velocidad de transferencia y el comportamiento de transmisión a ráfagas es el esquema de cesta de testigos, como el que se muestra en la Figura 16.8.

Se pueden seguir varias alternativas si un flujo de tráfico excede algún perfil. Los paquetes individuales que exceden el perfil pueden ser remarcados con un tratamiento de calidad inferior y permitirles el paso en el dominio DS. Un modelador de tráfico puede acoger una ráfaga de en memoria temporal y liberar los paquetes lentamente durante un periodo de tiempo grande. Un elemento de descarte puede eliminar paquetes si la memoria temporal utilizada para liberar lentamente los paquetes se satura.

16.5. LECTURAS RECOMENDADAS Y PÁGINAS WEB

En [HUIT95] se proporciona un tratamiento detallado de OSPF y de otros algoritmos de encaminamiento; estos temas también se tratan en [STEE95] y en [PERL92].

[XIAO99] contiene una descripción general y un entorno de trabajo general de la QoS en Internet así como de los servicios integrados y diferenciados. [CLAR92] y [CLAR95] proporcionan un estudio valioso de las cuestiones implicadas en la asignación de servicios internet para aplicaciones en tiempo real y elásticas, respectivamente. [SHEN95] es un análisis potente de la base lógica de la arquitectura de internet basada en QoS. [ZHAN95] es un estudio general de las disciplinas de tratamiento de colas que se pueden utilizar en una ISA, incluyendo un análisis de FQ y WFQ.

[ZHAN93] presenta una buena descripción general de la filosofía y la funcionalidad de RSVP, escrito por sus diseñadores. [WHIT97] contiene un estudio general de ISA y RSVP.

[WEIS98] es un estudio instructivo de los servicios diferenciados, mientras que [KUMA98] revisa los servicios diferenciados y los mecanismos de dispositivo de encaminamiento de apoyo pero va más allá que los RFC actuales.

CLAR92 Clark, D.; Shenker, S.; y Zhang, L. «Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism» *Proceedings, SIGCOMM '92,* August 1992.

CLAR95 Clark, D. *Adding Service Discrimination to the Internet.* MIT Laboratory for Computer Science Technical Report, September 1995. Available at http://anawww.lcs.mit.edu/anaWeb/papers.html.

HUIT95 Huitema, C. *Routing in the Internet.* Englewood Cliffs, NJ: Prentice Hall, 1995.

KUMA98 Kumar, V.; Lakshman, T.; y Stiliadis, D. «Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet.» *IEEE Communications Magazine*, May 1998.

PERL92 Perlman, R. *Interconnections: Bridges and Routers.* MA: Addison-Wesley, 1992.

SHEN95 Shenker, S. «Fundamental Desing Issues for the Future Internet.» *IEEE Journal on Selected Areas in Communications*, September 1995.

STEE95 Steenstrup, M. *Routing in Communications Networks.* Englewood Cliffs, NJ: Prentice Hall, 1995.

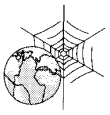
WEIS98 Weiss, W. «QoS with Differentiated Services.» *Bell Labs Technical Journal*, October-December 1998.

WHIT97 White, P., y Crowcroft, J. «The Integrated Services in the Internet: State of the Art.» *Proceedings of the IEEE*, December 1997.

XIAO99 Xiao, X., y Ni, L. «Internet QoS: A Big Picture.» *IEEE Network*, March/April 1999.

ZHAN93 Zhang, L.; Deering, S.; Estrim, D.; Shenker, S.; y Zappala, D. «RSVP: A New Resource ReSerVation Protocol.» *IEEE Network*, September 1993.

ZHAN95 Zhang, H. «Service Disciplines for Guaranteed Performance Service in Packet-Swirching Networks.» *Proceeedings of the IEEE*, October 1995.



SITIOS WEB RECOMENDADOS

- **Proyecto RSVP:** página Web para el desarrollo de RSVP.

16.6. PROBLEMAS

16.1. ¿Debería el encaminamiento en una interconexión de redes preocuparse del encaminamiento interno de una red? ¿Por qué o por qué no?

16.2. Cuando existen múltiples rutas de igual coste a un destino, OSPF puede distribuir el tráfico de igual forma entre las rutas. Esto se llama *balanceamiento de carga*. ¿Qué efectos tiene este balanceamiento de carga en el protocolo de la capa de transporte, como es TCP?

16.3. El esquema de cubo de testigos establece un límite en la duración del tiempo en el que el tráfico puede transmitirse a la velocidad de transmisión máxima. Si definimos la cesta de testigos por un tamaño de cesta de B octetos y una tasa de llegada de testigos de R octetos/segundo y si la velocidad de transferencia máxima de salida es M octetos/segundo.

a) Obtener una fórmula para S, la longitud de la ráfaga a velocidad máxima. Esto es, ¿durante cuánto tiempo puede un flujo transmitir a la velocidad máxima de salida cuando está gobernado por una cesta de testigos?

b) ¿Cuál es el valor de S para $b = 250$ Kb, $r = 2$ MB/s y $M = 25$ MB/s?

(*Sugerencia:* La fórmula de S no es tan fácil como pudiera parecer, ya que llegan más testigos mientras la ráfaga se está enviando.)

16.4. En RSVP, los números de puerto de UDP/TCP se utilizan para clasificar paquetes, por lo que cada dispositivo de encaminamiento debe se capaz de analizar estos campos. Esta necesidad trae problemas en las siguientes áreas:

a) Procesamiento de la cabecera IPv6.

b) Seguridad a nivel IP.

Indicar la naturaleza del problema en cada área y sugerir una solución.

CAPÍTULO 17

Protocolos de transporte

- El protocolo de transporte proporciona un servicio de transferencia de datos extremo-a-extremo que aísla a las capas superiores de los detalles de la red o redes subyacentes. Un protocolo de la capa de transporte puede ser orientado a conexión, como es TCP, o no orientado a conexión, como es UDP.
- Si la red subyacente o el servicio de interconexión es no seguro, como en el caso de IP, el protocolo de transporte orientado a conexión resulta ser muy complejo. La causa básica de esta complejidad es la necesidad de tratar con retardos variables y relativamente grandes que se producen entre los sistemas finales. Estos retardos complican las técnicas del control de flujo y el control de errores.
- TCP utiliza una técnica de control de flujo y error basada en créditos que es en cierta forma diferente del control de flujo de la ventana deslizante utilizada en X.25 y HDLC. La esencia está en que TCP separa las confirmaciones de la gestión del tamaño de la ventana deslizante.
- Aunque el mecanismo basado en créditos de TCP se diseñó para el control de flujo extremo-a-extremo, también se utiliza para ayudar al control de la congestión en la interconexión de redes. Cuando una entidad TCP detecta la presencia de congestión en el conjunto de redes, reduce el flujo de datos que envía al conjunto de redes hasta que detecta un alivio en la congestión.

En una arquitectura de protocolos, el protocolo de transporte se sitúa encima de la capa de red o de interconexión que proporciona los servicios relacionados con la red, y justo debajo de las aplicaciones o protocolos de capas superiores. El protocolo de la capa transporte proporciona servicios a los usuarios del servicio de transporte (TS, Transport Service), como son FTP, SMTP y TELNET. La entidad local de transporte se comunica con alguna otra entidad de transporte remota utilizando los servicios de algún protocolo inferior, como puede ser el Protocolo Internet. El servicio general proporcionado por un protocolo de transporte es el transporte de datos extremo-a-extremo de forma que aísla al usuario TS de los detalles de los sistemas de comunicaciones subyacentes.

Comenzaremos analizando los mecanismos de protocolo que se requieren para proporcionar los servicios anteriormente citados. Se encuentra que la mayor parte de la complejidad está relacionada con los servicios orientados a conexión. Como cabría esperar, cuantos menos servicios proporciona la red, más trabajo debe hacer el protocolo de transporte. El resto del capítulo trata sobre los dos protocolos de transporte más usados: el protocolo de control de la transmisión (TCP, Transmission Control Protocol) y el protocolo datagrama de usuario (UDP, User Datagram Protocol). La Figura 17.1 destaca la posición de estos protocolos dentro del conjunto de protocolos TCP/IP.

17.1. MECANISMOS DEL PROTOCOLO DE LA CAPA DE TRANSPORTE ORIENTADO A CONEXIÓN

Son posibles dos tipos básicos de servicio: orientado a conexión y no orientado a conexión o servicio datagrama. Un servicio orientado a conexión proporciona el establecimiento, mantenimiento y cierre de una conexión lógica entre usuarios TS. Éste ha sido el tipo de servicio de protocolo más común disponible hasta ahora y tiene una gran variedad de aplicaciones. El servicio orientado a conexión implica generalmente que el servicio es seguro. Esta sección estudia los mecanismos del protocolo de transporte necesarios para permitir un servicio orientado a conexión.

Un protocolo de transporte con todas las características de orientado a conexión, como es TCP, es muy complejo. Por motivos de claridad presentamos los mecanismos del protocolo de transporte de una forma que sigue su evolución. Empezaremos con los servicios de red que facilitan el funcionamiento del

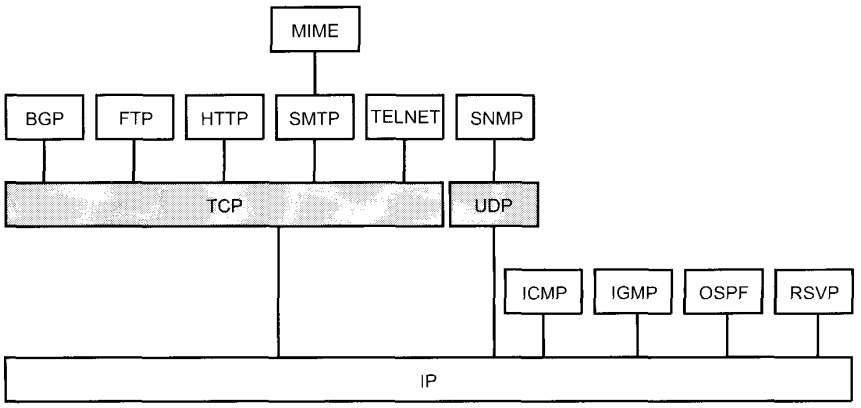


Figura 17.1. Protocolos del nivel de transporte en su contexto.

protocolo de transporte y que garantizan el transporte de todas las unidades de datos de transporte en orden y definen los mecanismos requeridos. Después examinaremos los mecanismos de transporte necesarios para tratar con un servicio de red no seguro. Toda esta discusión se aplica en general a los protocolos de la capa de transporte. En la Sección 17.2, aplicaremos los conceptos desarrollados para describir TCP.

SERVICIO DE RED DE SECUENCIAMIENTO SEGURO

Supongamos que el servicio de red acepta mensajes con un tamaño arbitrario y los envía en secuencia al destino con una seguridad virtual del 100%. Ejemplos de estas redes son:

- Una red de conmutación de paquetes altamente segura con una interfaz X.25
- Una red de retransmisión de tramas (*frame relay*) utilizando el protocolo de control LAPF.
- Una LAN IEEE 802.3 utilizando el servicio LLC orientado a conexión.

En todos los casos, el protocolo de transporte se utiliza como un protocolo extremo-a-extremo entre dos sistemas finales conectados en la misma red, en vez de hacerlo a través de un conjunto de redes. La suposición de servicios de red seguros con secuenciamiento permiten el uso de un protocolo de transporte bastante sencillo. Hay cuatro cuestiones a considerar.

- Direccionamiento.
- Multiplexación.
- Control de flujo.
- Establecimiento/cierre de la conexión.

Direccionamiento

La cuestión sobre direccionamiento es simplemente ésta: un usuario de una entidad de transporte dada desea, o bien, establecer una conexión o bien realizar una transferencia de datos sin establecer una conexión con un usuario de otra entidad de transporte. El usuario destino debe ser especificado mediante la información completa siguiente:

- Identificación de usuario.
- Identificación de la entidad de transporte.

- Dirección de la estación.
- Número de red.

El protocolo de transporte debe ser capaz de extraer la información indicada anteriormente de la dirección del usuario TS. Normalmente, la dirección de usuario se especifica como (*estación, puerto*). La variable puerto representa un usuario TS particular en la estación especificada. En general, habrá una sola entidad de transporte en cada estación, por lo tanto no es necesario una identificación de entidad. Si están presentes más de una entidad de transporte, normalmente, hay una de cada tipo. En este último caso, la dirección debería incluir una indicación del tipo de protocolo de transporte (por ejemplo, TCP, UDP). En el caso de una red única, *estación* identifica un dispositivo de red conectado a la misma. En el caso de un conjunto de redes, *estación* es una dirección internet global. En TCP, la combinación del puerto y la estación se refiere como un conector.

Ya que el encaminamiento no es una cuestión de la capa de transporte, éste simplemente pasa el campo *estación* de la dirección hacía el servicio de red. El campo *puerto* se incluye en la cabecera de transporte y será utilizado en el destino por el protocolo de transporte destino.

Queda todavía una cuestión por estudiar. ¿Cómo puede el usuario TS que inicia la comunicación conocer la dirección destino del usuario de transporte? Existen dos estrategias estáticas y dos dinámicas que se explican por sí mismas:

1. El usuario TS debe conocer la dirección si desea un tiempo de respuesta más rápido. Ésta es básicamente una función de la configuración del sistema. Por ejemplo, un proceso puede estar ejecutándose pero sólo incumbe a un número limitado de usuarios TS, como, por ejemplo, un proceso que recoge estadísticas sobre prestaciones. De vez en cuando, una rutina de gestión de la red central se conecta al proceso para obtener las estadísticas. En general, estos procesos no son, o no deberían ser, conocidos para poder ser accedidos por todos.
2. A algunos servicios usados comúnmente se le asignan direcciones bien conocidas. Por ejemplo, servicios de tiempo compartido y procesadores de textos.
3. Proporcionando un servidor de nombres. El usuario TS requiere un servicio mediante algún nombre genérico o un nombre global. Esta petición se envía a un servidor de nombres, que realiza una búsqueda en una tabla y devuelve una dirección. La entidad de transporte procede entonces con la conexión. Este servicio es útil para aplicaciones comunes que cambian su localización de una vez a otra. Por ejemplo, un proceso de entrada de datos se podría cambiar de una estación a otra en una red local para balancear la carga.
4. En algunos casos, el usuario destino es un proceso que se genera cuando se le requiere para una conexión. El usuario que inicia la comunicación puede enviar una petición a un proceso a una dirección bien conocida. El usuario en esa dirección es un proceso privilegiado del sistema que generará el nuevo proceso y devolverá una dirección. Por ejemplo, un programador ha desarrollado una aplicación privada (por ejemplo, un programa de simulación) que se ejecutará en un computador central remoto pero que se invoca desde un minicomputador local. Se puede mandar una petición a un proceso de gestión de trabajos remoto que lanza el proceso de simulación.

Multiplexación

El concepto de multiplexación, se discutió en términos generales en la Sección 2.1. Con respecto a la interfaz entre el protocolo de transporte y el protocolo de la capa superior, el protocolo de transporte implementa una función de multiplexación/demultiplexación. Esto es, usuarios múltiples emplean el mismo protocolo de transporte, y se distinguen unos de otros por números de puerto o puntos de acceso al servicio.

La entidad de transporte también podría implementar una función de multiplexación con respecto a los servicios de red que él usa. Hay que recordar que definimos una multiplexación hacia arriba como la

multiplexación de múltiples conexiones en una única conexión de la capa inferior, y multiplexación hacia abajo como la división de una única conexión entre múltiples conexiones de la capa inferior.

Consideremos, por ejemplo, una entidad de transporte haciendo uso de un servicio X.25. ¿Por qué una entidad de transporte debería utilizar multiplexación hacia arriba? Después de todo, hay 4.095 circuitos virtuales disponibles. En un caso típico, esto es más que suficiente para gestionar todos los usuarios TS activos. Sin embargo, la mayoría de las redes X.25 basan parte del cobro que realizan en el tiempo de conexión, ya que cada circuito virtual consume algunos recursos de memoria temporal del nodo. Así, si un único circuito virtual proporciona el rendimiento suficiente para múltiples usuarios TS, se justifica utilizar multiplexación hacia arriba.

Por otra parte, la multiplexación hacia abajo se podría usar para mejorar el rendimiento. Por ejemplo, cada circuito virtual X.25 está restringido a un número de secuencia de 3 o 7 bits. Para redes de alta velocidad o de gran retardo sería necesario utilizar un espacio de secuenciamiento más grande. Por supuesto, el rendimiento sólo se puede incrementar hasta cierto límite. Si sólo existe un único enlace estación-nodo sobre el cual se multiplexan todos los circuitos virtuales, el rendimiento de una conexión de transporte no puede exceder la velocidad de transmisión de datos del enlace.

Control de flujo

Mientras que el control de flujo es un mecanismo relativamente sencillo en la capa de enlace, en la capa de transporte es un mecanismo bastante complejo por dos razones principales:

- El retardo de transmisión entre entidades de transporte es generalmente grande comparado con el tiempo de transmisión real. Esto significa que hay un retardo considerable en la comunicación de la información de control de flujo.
- Ya que la capa de transporte opera sobre una red o un conjunto de redes, la cantidad de retardo en la transmisión puede ser muy variable. Esto hace difícil utilizar de forma efectivo el mecanismo de temporizadores para la retransmisión de los datos perdidos.

En general existen dos razones por las que una entidad de transporte debería moderar la tasa de transmisiones de segmentos a través de una conexión desde otra entidad de transporte:

- El usuario de la entidad de transporte receptora no puede mantener el flujo de datos.
- La propia entidad de transporte receptora no puede mantener el flujo de segmentos.

¿Cómo se manifiestan tales problemas? Presumiblemente una entidad de transporte tiene una cierta capacidad de memoria temporal. Los segmentos que llegan se almacenan en las memorias temporales. Cada segmento almacenado se procesa (por ejemplo, se examina la cabecera de transporte) y los datos se envían al usuario. Cualquier de los dos problemas mencionados antes causarán que las memorias temporales se saturen. De esta manera, la entidad de transporte necesita tomar medidas para detener o disminuir el flujo de segmentos para evitar la saturación de las memorias temporales. Este requerimiento no es tan fácil de cumplir a causa de las molestias que causa el intervalo de tiempo entre la emisión y la recepción. Volveremos a este punto un poco más adelante. Primero, presentamos cuatro formas de hacer frente al requisito de control de flujo. La entidad de transporte receptora puede:

1. No hacer nada.
2. Rechazar la aceptación de más segmentos del servicio de red.
3. Usar un protocolo fijo de ventana deslizante.
4. Usar un esquema de créditos.

La alternativa 1 significa que se descartan los segmentos que llegan una vez agotados las memorias temporales. La entidad de transporte emisora, viendo que no recibe una confirmación, los retransmitirá. Esto es bochornoso, ya que la ventaja de una red segura es que uno nunca tiene que retransmitir. Además, ¡el efecto de esta técnica es acrecentar el problema! El emisor incrementa sus envíos para incluir los segmentos nuevos además de los originalmente retransmitidos.

La segunda alternativa es un mecanismo de presión hacia atrás que se basa en el servicio de red para realizar esta tarea. Cuando las memorias temporales de una entidad de transporte están llenas, esta entidad rechaza datos adicionales del servicio de red. Esto dispara un mecanismo de control de flujo que estrangula el servicio de red en el extremo emisor. Este servicio, por el contrario, rechaza segmentos adicionales de su entidad de transporte. Debería quedar claro que este mecanismo es poco riguroso y tosco. Por ejemplo, cuando conexiones múltiples de transporte están multiplexadas en una única conexión de red (circuito virtual), el control de flujo se ejerce sólo en el agregado de todas las conexiones de transporte.

La tercera estrategia es familiar al lector debido a la discusión sobre los protocolos de la capa de enlace de datos. Recuerde que los ingredientes claves son:

- El uso de números de secuencia en las unidades de datos.
- El uso de una ventana de tamaño fijo.
- El uso de confirmaciones para desplazar la ventana.

Con un servicio de red seguro, la técnica de ventana deslizante funcionaría realmente bien. Por ejemplo, considere un protocolo con un tamaño de ventana de 7. Siempre que el emisor recibe una confirmación de un segmento particular, es autorizado automáticamente a enviar los siete segmentos siguientes (por supuesto, algunos podrían haber sido ya enviados). Ahora, cuando el receptor puede admitir otros 7 nuevos segmentos, puede retener las confirmaciones de los segmentos que lleguen para evitar la saturación. La entidad de transporte emisora puede enviar como mucho 7 segmentos adicionales y a continuación parar el envío. Como el servicio de red subyacente es seguro, los temporizadores del emisor no expirarán y no retransmitirán ninguno. Así, en este punto, una entidad de transporte emisora podría haber transmitido cierto número de segmentos y para las cuales no ha recibido las confirmaciones. Ya que trabajamos con una red segura, la entidad de transporte emisora puede suponer que los segmentos han llegado y que la falta de confirmaciones se debe a una táctica de control de flujo. Esta táctica no funcionará bien en una red no segura, ya que la entidad de transporte emisora no sabría si la falta de confirmaciones es debido al control de flujo o a la pérdida de un segmento.

La cuarta alternativa, un esquema de créditos, proporciona al receptor un mayor grado de control sobre el flujo de datos. Aunque no es estrictamente necesario con un servicio de red seguro, un esquema de créditos da lugar a un flujo más suave. Además, como veremos, es un esquema más efectivo con un servicio de red no seguro.

El esquema de créditos desliga las confirmaciones del control de flujo. En los protocolos de ventana deslizante fija, tales como X.25, los dos conceptos son sinónimos. En un esquema de créditos, un segmento puede ser confirmado sin obtener un nuevo crédito, y viceversa. En el esquema de créditos, cada octeto individual de datos que se transmite se considera que tiene un número de secuencia. Además de los datos, cada segmento transmitido incluye en su cabecera tres campos relacionados con el control de flujo: un número de secuencia, un número de confirmación y la ventana. Cuando una entidad de transporte envía un segmento, incluye el número de secuencia del primer octeto en el campo de datos del segmento. Una entidad de transporte confirma un segmento recibido con un segmento de vuelta que incluye ($AN = i$, $W = j$), con la siguiente interpretación:

- Se confirman todos lo octetos con número de secuencia hasta $SN = i - 1$; el siguiente octeto esperado tiene número de secuencia i.
- Se concede permiso para enviar una ventana adicional de $W = j$ octetos de datos; esto es, los j octetos correspondientes a los números de secuencia i hasta $i + j - 1$.

La Figura 17.2 ilustra el protocolo (comparar con la Figura 7.4). Por simplicidad, se muestra el flujo de datos en un solo sentido y se supone que en cada segmento se envían 200 octetos. Inicialmente, a través del proceso de establecimiento de la conexión, los números de secuencia de emisión y recepción están sincronizados y A obtiene una asignación inicial de 1.400 octetos, comenzando con el octeto número 1001. Después de enviar 600 octetos en tres segmentos, A ha reducido su ventana a un tamaño de

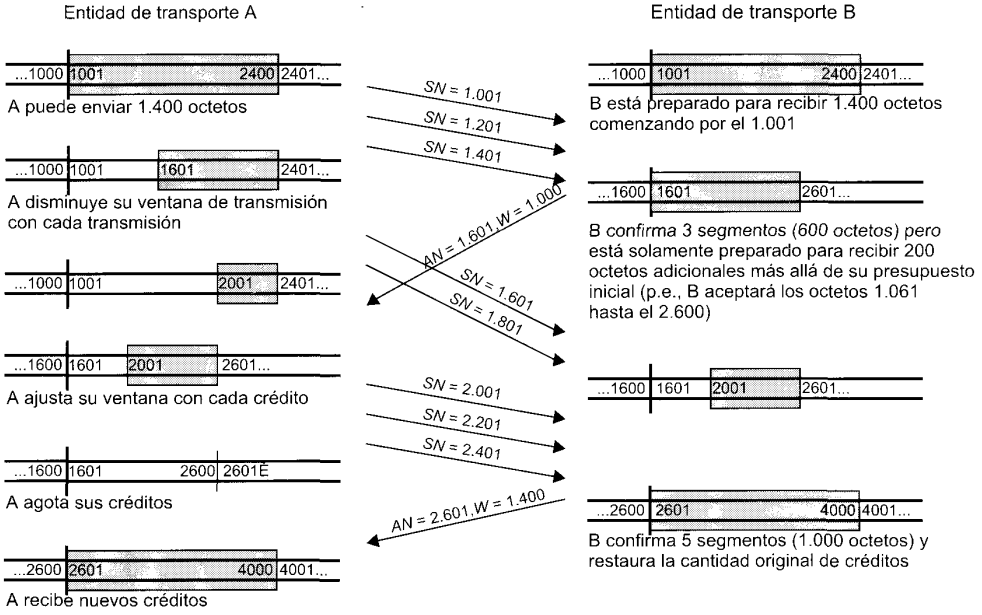


Figura 17.2. Ejemplo del mecanismo de asignación de créditos de TCP.

800 octetos (números de 1601 a 2400). Tras la recepción de estos segmentos, B confirma la recepción de todos los octetos hasta el 1600 y emite un crédito de 1.000 octetos. Esto significa que A puede enviar los octetos 1601 al 2600 (5 segmentos). Sin embargo, para cuando A recibe el mensaje de B, A ya ha enviado dos segmentos, que contienen los octetos 1601 al 2000 (lo cual estaba permitido bajo la asignación inicial). Así, los créditos restantes de A en este punto se reducen a 400 octetos (2 segmentos). Conforme avanza el intercambio, A avanza el borde final de su ventana cada vez que transmite, y avanza el borde de la cabecera de la ventana cada vez que obtiene un crédito.

La Figura 17.3 muestra una perspectiva del mecanismo desde el lado del emisor y del receptor (comparar con la Figura 7.3). Normalmente, ambos lados tienen ambas perspectivas ya que los datos se pueden intercambiar en ambas direcciones. Hay que notar que el receptor no está obligado a confirmar inmediatamente los segmentos que llegan, sino que puede esperar y emitir una confirmación conjunta para un número determinado de segmentos.

El receptor necesita adoptar algunos criterios sobre la cantidad de datos que va a permitir que el emisor transmita. La opción conservadora es solamente permitir nuevos segmentos hasta el límite del espacio de memoria temporal disponible. Si esta fuera la política en la Figura 17.2, el primer mensaje de crédito implica que B tiene 1.000 octetos libre en su memoria temporal, y el segundo mensaje, que B tiene 1.000 octetos disponibles.

Un esquema de control de flujo conservador puede limitar el rendimiento de la conexión de transporte en situaciones de gran retardo. El receptor podría incrementar potencialmente el rendimiento mediante la asignación de una forma optimista de los créditos de espacio que no tiene. Por ejemplo, si la memoria temporal del receptor está llena pero él anticipa que puede librar espacio de dos segmentos dentro del tiempo de propagación de ida y vuelta, podría enviar inmediatamente un crédito de 1.000 octetos. Si el receptor puede ir al paso del emisor, este esquema podría incrementar el rendimiento y evitar perjuicios. Sin embargo, si el emisor es más rápido que el receptor, algunos segmentos podrían ser descartados, necesitando una retransmisión. Ya que las retransmisiones no son necesarias con un

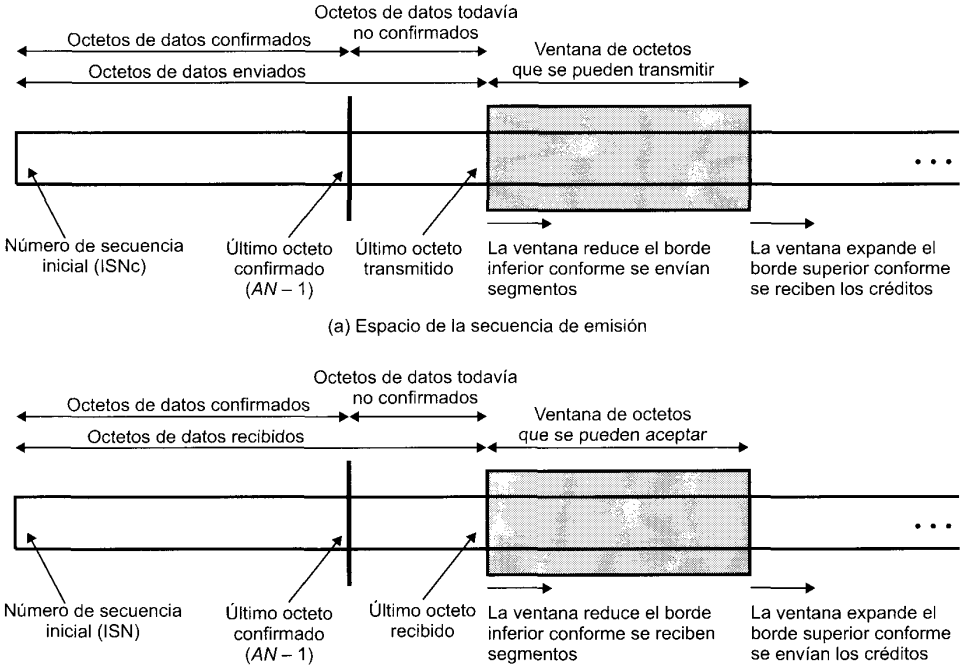


Figura 17.3. Perspectivas del control de flujo emisor y receptor.

servicio de red seguro (en ausencia de congestión en el conjunto de redes), un esquema de control de flujo optimista complicará el protocolo.

Establecimiento y cierre de la conexión

Incluso con servicios de red seguros, existe la necesidad de procedimientos de establecimiento y cierre de conexión para ofrecer un servicio orientado a conexión. El establecimiento de la conexión cumple tres objetivos principales:

- Permite a cada extremo asegurarse de que el otro existe.
- Permite la negociación de parámetros opcionales (por ejemplo, el tamaño del segmento, tamaño máximo de la ventana, calidad de servicio).
- Pone en marcha la reserva de recursos de la entidad de transporte (por ejemplo, espacio de memoria, entradas en la tabla de conexiones).

El establecimiento de la conexión es por mutuo acuerdo y se puede llevar a cabo mediante un conjunto sencillo de órdenes de usuario y segmentos de control, como se muestra en el diagrama de estados de la Figura 17.4. Para comenzar, un usuario TS está en un estado CERRADO (por ejemplo, no tiene conexiones de transporte abiertas). El usuario TS puede indicar que esperará pasivamente hasta que reciba una petición con una orden *Passive Open*. Esto es lo que podría hacer un programa servidor, tal como una aplicación en tiempo compartido o una aplicación de transferencia de ficheros. El usuario TS podría cambiar de idea enviando una orden *Close*. Después de haberse emitido la orden *Passive Open*, la entidad de transporte crea un objeto de conexión de algún tipo (por ejemplo, una entrada en una tabla) que está en el estado PREPARADO.

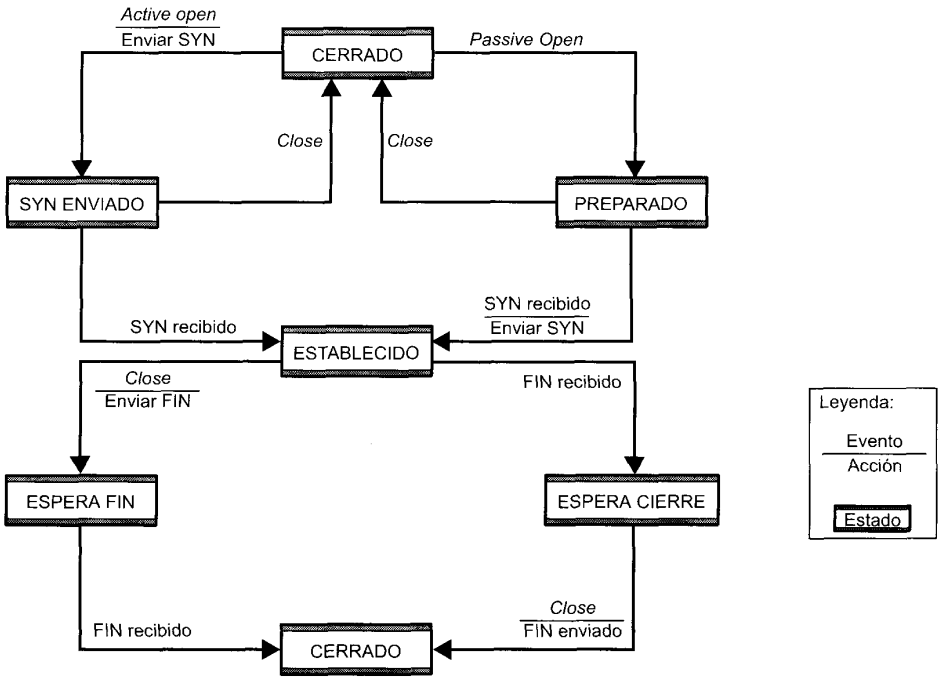


Figura 17.4. Diagrama de estados de una conexión sencilla.

Desde el estado CERRADO, el usuario TS puede abrir una conexión emitiendo una orden *Active Open*, que da instrucciones a la entidad de transporte para que intente realizar el establecimiento de una conexión con el usuario designado, esto hace que la entidad de transporte envíe un segmento SYN (para sincronizar). El segmento se lleva a la entidad de transporte receptora y es interpretado como una petición de conexión a un puerto particular. Si la entidad de transporte destino está en el estado PREPARADO para ese puerto entonces se establece una conexión por medio de las acciones siguientes que realiza la entidad de transporte:

- Informa al usuario TS que una conexión está abierta.
- Envía un SYN como confirmación a la entidad de transporte remota.
- Sitúa el objeto de conexión en el estado ESTABLECIDO (establecido).

Cuando el correspondiente SYN se recibe en la entidad de transporte que inició el proceso, ella también puede pasar la conexión al estado ESTABLECIDO. La conexión se aborta prematuramente si cualquier usuario TS emite una orden *Close*.

La Figura 17.5 muestra la robustez de este protocolo. Cualquier lado puede iniciar la conexión. Además, si ambos lados inician la conexión en instantes próximos, ésta se establece sin confusión. Esto es así, ya que el segmento SYN funciona como petición de conexión y como confirmación de la conexión.

El lector se preguntará qué ocurre si llega un SYN en un momento en el que el usuario TS solicitado está desocupado (no atiende a llamadas). Se pueden seguir tres caminos:

- La entidad de transporte puede rechazar la petición enviando un segmento RST (reiniciar) a la otra entidad de transporte.
- La petición se puede poner en cola hasta que el usuario TS emita una orden *Open*.

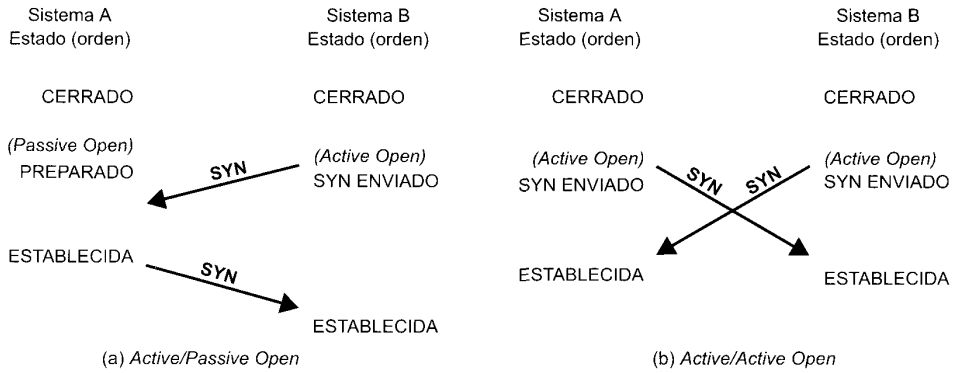


Figura 17.5. Escenarios de establecimiento de conexión.

- La entidad de transporte puede interrumpir, o informar de cualquier otra manera, al usuario de la existencia de una petición pendiente.

Notar que si se utiliza este último mecanismo, no es estrictamente necesario una orden *Passive Open*, que podría ser reemplazado por una orden *Accept*, que se utiliza como una señal del usuario utilizada para indicarle a la entidad de transporte que acepta la conexión.

El cierre de la conexión se trata de manera similar. Cualquier lado, o ambos, pueden iniciar el cierre. La conexión se cierra por mutuo acuerdo. Esta estrategia permite un cierre abrupto u ordenado. Para conseguir este último, una conexión que está en el estado ESPERA CIERRE debe continuar aceptando segmentos de datos hasta que se reciba un segmento FIN.

La Figura 17.4 también define el procedimiento para un cierre ordenado. Primero consideremos el lado que inicia el proceso de cierre:

1. En respuesta a una primitiva *Close* del usuario TS, se envía un segmento FIN al otro extremo de la conexión, solicitando el cierre.
2. Habiendo enviado FIN, la entidad de transporte sitúa la conexión en el estado ESPERA FIN. En este estado, la entidad de transporte debe continuar aceptando datos del otro extremo y pasarlos a su usuario.
3. Cuando se recibe como respuesta un FIN, la entidad de transporte informa a su usuario y cierra la conexión.

Desde el punto de vista del extremo que no inicia el cierre:

1. Cuando se recibe un segmento FIN, la entidad de transporte informa a su usuario de la petición de cierre y sitúa la conexión en el estado ESPERA CIERRA. En este estado, la entidad de transporte debe continuar aceptando datos de su usuario y transmitirlos en segmentos de datos al otro extremo.
2. Cuando el usuario emite una primitiva *Close*, la entidad de transporte envía un segmento FIN de respuesta al otro extremo y cierra la conexión.

Este procedimiento asegura que ambos extremos han recibido todos los datos pendientes y que ambos están de acuerdo en terminar la conexión antes del cierre real.

SERVICIO DE RED NO SEGURO

El caso más difícil para un protocolo de transporte es aquel en que se ofrece un servicio de red no seguro. Ejemplos de tales redes son:

- Una interconexión de redes utilizando IP.
- Una red *frame relay* utilizando sólamente el núcleo del protocolo LAPF.
- Una LAN IEEE 802.3 usando un servicio no orientado a conexión LLC sin confirmaciones.

El problema no es sólo que los segmentos pueden perderse ocasionalmente, sino que los segmentos pueden llegar fuera de secuencia debido al retardo de tránsito variable. Como veremos, se requiere un elaborado mecanismo para tratar con estas dos deficiencias interrelacionadas de la red. También veremos que aparece un modelo desalentador. La combinación de inseguridad y no secuenciamiento crea problemas con todos los mecanismos que hemos discutido hasta ahora. Generalmente, la solución a cada problema produce nuevos problemas. Aunque hay problemas que tienen que ser resueltos por los protocolos en todas las capas, parece que hay más dificultades con un protocolo de transporte orientado a conexión que con cualquier otro tipo de protocolo.

Hay seis cuestiones que han de ser tratadas:

- Transporte en orden.
- Estrategia de retransmisión.
- Detección de duplicados.
- Control de flujo.
- Establecimiento de la conexión.
- Cierre de la conexión.
- Recuperación de las caídas.

Transporte en orden

Con un servicio de red no seguro, es posible que los segmentos, incluso si todos llegan, lo hagan en forma desordenada. La solución a este problema es numerar los segmentos secuencialmente. Ya hemos visto que para los protocolos de control del enlace de datos, tales como HDLC o X.25, cada unidad de datos (trama, paquete) se numera secuencialmente siendo cada número de secuencia sucesivo, uno más que el número de secuencia anterior. Este esquema se utiliza en algunos protocolos de transporte, tales como en los protocolos de transporte de ISO. Sin embargo, TCP usa un esquema algo diferente en el que cada octeto de datos que se transmite está implícitamente numerado. Así, el primer segmento podría tener el número de secuencia 0. Si ese segmento contiene 1.000 octetos de datos, el segundo segmento tendría el número de secuencia 1.000, y así a sucesivamente. Por simplicidad en la discusión de esta sección, supondremos que el número de secuencia de cada segmento sucesivo es 200 más que el del segmento previo; esto es, cada segmento contiene exactamente 200 octetos de datos.

Estrategia de retransmisión

Existen dos eventos que requieren la retransmisión de un segmento. Primero, el segmento se puede dañar en el camino pero sin embargo llega a su destino. Si se incluye en el segmento una secuencia de comprobación de trama, la entidad de transporte receptora puede detectar el error y descartar el segmento. La segunda contingencia es que el segmento no llega al destino. En cualquier caso, la entidad de transporte emisora no sabe que la transmisión del segmento se realizó sin éxito. Para cubrir esta contingencia, se requiere que se use un esquema de confirmaciones positivas: El receptor debe confirmar cada recepción de un segmento con éxito devolviendo un segmento que contiene un número de confirmación. Por razones de eficiencia no se requiere una confirmación por cada segmento. En su lugar, se utiliza una confirmación acumulativa, como se ha visto ya varias veces en este libro. Así, el receptor puede recibir los segmentos numerados como 1, 201 y 401, pero sólo envía la confirmación $AN = 601$ de vuelta. El emisor debe interpretar $AN = 601$ que significa que el segmento con $SN = 401$ y los anteriores se han recibido con éxito.

Tabla 17.1. Temporizadores del protocolo de transporte.

Temporizador de retransmisión	Para retransmitir una segmento no confirmado.
Temporizador de reconexión	Tiempo mínimo entre el cierre de una conexión y el establecimiento de otra con la misma dirección destino.
Temporizador de ventana	Tiempo máximo entre segmentos ACK/CREDIT.
Temporizador de retransmisión de SYN	Tiempo entre intentos de establecer una conexión.
Temporizador de persistencia	Abortar una conexión cuando no se confirman segmentos.
Temporizador de inactividad	Abortar una conexión cuando no se reciben segmentos.

Si un segmento no llega con éxito, no se enviará un ACK y se tiene que producir la retransmisión. Para poder tratar esta situación tiene que haber un temporizador asociado con cada segmento que se envía. Si el temporizador expira antes de que se confirme, el emisor debe retransmitirlo.

Así la inclusión de temporizadores soluciona el problema. El problema siguiente es: ¿Qué valor se debe establecerse en el temporizador? Hay dos estrategias que se sugieren a sí mismas. Se podría utilizar un temporizador con valor fijo, basándose en el conocimiento del comportamiento típico de la red. Esta estrategia tiene la debilidad de no saber adaptarse a las condiciones cambiantes de la red. Si el valor es muy pequeño, habrá muchas retransmisiones innecesarias, desperdiciando la capacidad de la red. Si el valor es muy grande, el protocolo será muy lento en dar respuesta a la pérdida de un segmento. El temporizador se debe fijar a un valor un poco mayor que el retardo de ida y vuelta (enviar un segmento, recibir un ACK). Por supuesto, este retardo es variable incluso para una carga constate de la red. Y lo que es peor, la estadística del retardo variará con condiciones de red variables.

La otra estrategia es utilizar un esquema adaptativo, que también tiene sus propios problemas. Supongamos que la entidad de transporte registra el tiempo que se tarda en confirmar los segmentos de datos y fija los temporizadores de retransmisión de acuerdo a la media de los retardos observados. No es posible fiarse de este valor por tres razones:

- La entidad par puede que no confirme inmediatamente un segmento. Cabe recordar que le hemos dado el privilegio de confirmaciones acumulativas.
- Si un segmento tiene que ser retransmitido, el emisor no puede saber si el ACK recibido es la respuesta a la transmisión inicial o a la retransmisión.
- Las condiciones de la red pueden cambiar rápidamente.

Cada uno de estos problemas es la causa de alguna complicación adicional del algoritmo de transporte, pero el problema no admite una solución completa. Siempre habrá alguna incertidumbre con respecto al mejor valor para el temporizador de retransmisión.

Por cierto, el temporizador de retransmisión es sólo uno de una serie de temporizadores necesarios para el funcionamiento correcto del protocolo de transporte. Éstos se listan en la Tabla 17.1, junto a una breve explicación.

Detección de duplicados

Si un segmento se pierde y después se retransmite, no se producirá confusión. Sin embargo, si se pierde un ACK, se retransmitirán uno o más segmentos y, si llegan correctamente, se tendrán duplicados del segmento recibido previamente. Así, el receptor debe ser capaz de reconocer duplicados. El hecho de

que cada segmento lleve un número de secuencia ayuda pero, de cualquier forma, la detección de duplicados no es una tarea fácil. Existen dos casos:

- Se recibe un duplicado antes del cierre de la conexión.
- Se recibe un duplicado después de que se ha cerrado la conexión.

Hay que notar que se ha dicho «un» duplicado y no «el» duplicado. Desde el punto de vista del emisor, el segmento retransmitido es el duplicado. Sin embargo, el segmento retransmitido podría llegar antes que el segmento original, en cuyo caso el receptor ve el segmento original como el duplicado. En cualquier caso, se necesitan dos tácticas para tratar el caso de que un duplicado se reciba antes de cerrar la conexión.

- El receptor debe asumir que su confirmación se perdió y por lo tanto debe confirmar el duplicado. Consecuentemente, el emisor debe no confundirse si recibe múltiples ACK de un mismo segmento.
- El espacio de números de secuencia debe ser lo suficientemente grande para no agotarse en menos tiempo que la vida máxima posible de un segmento.

La Figura 17.6 ilustra la razón del porqué del último requisito. En este ejemplo, el espacio de secuencia es de longitud 1.600; esto es, después de $SN = 1.600$, los números de secuencia vuelven a empezar con $SN = 1$. Por simplicidad, suponemos que se utiliza un protocolo tipo ventana deslizante con un tamaño de ventana de 600. Supongamos que A ha transmitido los segmentos de datos con $SN = 1$, 201

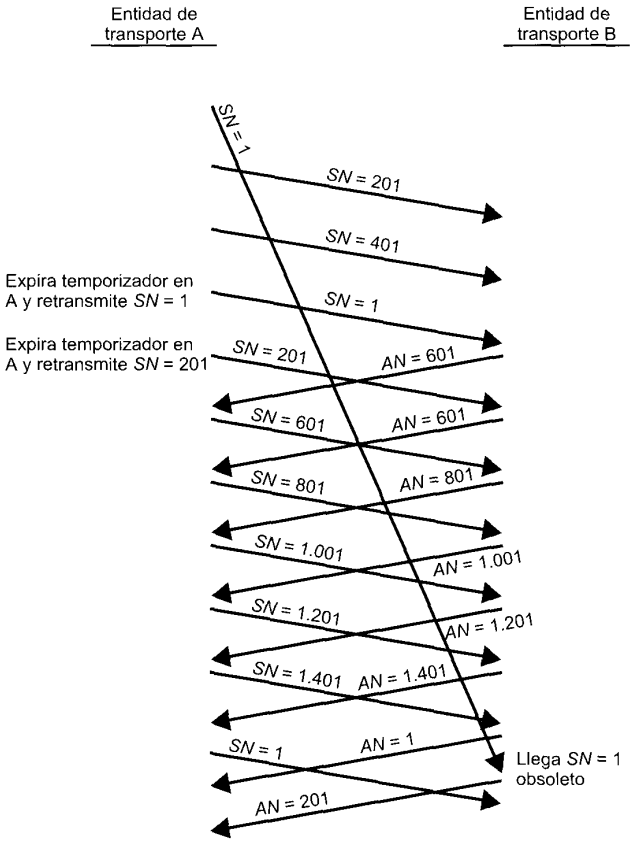


Figura 17.6. Ejemplo de una detección incorrecta de duplicados.

y 401 y que no confirmaciones. Al cabo del tiempo, se produce una expiración y retransmite el segmento $SN = 1$. B ha recibido dos segmentos con $SN = 201$ y 401, pero $SN = 1$ se ha retrasado en el camino. Así, de esta forma B no envía ninguna confirmación. Cuando llega el duplicado del segmento $SN = 1$, B confirma el 1, 201 y el 401 con $AN = 601$. Mientras tanto, en A se produce otra expiración y retransmite el $SN = 201$, que es confirmado por B con otro $AN = 601$. Las cosas parecen que se han arreglado solas y la transferencia de datos continúa. Cuando el espacio de secuencia se agota A vuelve a comenzar con el número de secuencia $SN = 1$ y continúa. Desafortunadamente, el segmento obsoleto $SN = 1$ hace una aparición tardía y es aceptado por B antes de que el nuevo segmento $SN = 1$ llegue.

Debería quedar claro que la aparición fuera de tiempo de un segmento antiguo no habría causado dificultades si los números de secuencia no hubieran dado la vuelta. El problema es: ¿Qué tamaño debe de tener el espacio de secuencia? Esto depende, entre otras cosa, de si la red fuerza un tiempo de vida del paquete y la tasa a la que los segmentos se retransmiten. Afortunadamente, la incorporación de un único bit al campo de números de secuencia dobla el espacio de secuencia de forma que es fácil seleccionar un tamaño seguro.

Control de flujo

El mecanismo de control de flujo por medio de la asignación de créditos descrito antes es bastante robusto en presencia de un servicio de red no seguro y requiere pocas mejoras. Como se ha mencionado, un segmento que contiene ($AN = i$, $W = j$) acepta todos los octetos con número hasta $i - 1$ y concede créditos para j octetos adicionales empezando por el octeto i. El mecanismo de asignación de créditos es bastante flexible. Por ejemplo, considere que el último mensaje emitido por B fue ($AN = i$, $W = j$) y que el último octeto de datos recibido por B fue el octeto número $i - 1$. Entonces:

- B emite ($AN = i$, $W = k$) para incrementar o decrementar los créditos en una cantidad $k (k > j)$ cuando no han llegado datos adicionales.
- B emite ($AN = i + m$, $W = j - m$) para confirmar un segmento nuevo conteniendo m octetos de datos ($m < j$) sin conceder créditos adicionales.

La pérdida de un segmento ACK/CREDIT tiene poco impacto en el funcionamiento del esquema. Las confirmaciones futuras resincronizarán el protocolo. Además, si no hay nuevas confirmaciones en camino, en el emisor expirará un temporizador y se retransmitirá un segmento de datos, lo que dispara una nueva confirmación. Considere la situación en la cual B envía ($AN = i$, $W = 0$), cerrando temporalmente la ventana. Con posterioridad, B envía ($AN = i$, $W = j$), pero este segmento se pierde. A está esperando la oportunidad de enviar datos y B piensa que ha concedido esa oportunidad. Para superar este problema, se puede utilizar un temporizador de ventana. Este temporizador se reinicializa cada vez que se envía un segmento (todos los segmentos contienen los campos AN y W). Si el temporizador expira alguna vez, se le requiere a la entidad de transporte que envíe un segmento, incluso si el nuevo duplica uno anterior. Esto rompe la parálisis y le asegura al otro extremo que la entidad de transporte está todavía viva.

Establecimiento de la conexión

Como con otros mecanismos de protocolo, el establecimiento de la conexión debe tener en cuenta la falta de seguridad del servicio de red. Recuérdese que el establecimiento de la conexión requiere el intercambio de SYN, un procedimiento llamado a veces «diálogo» en dos sentidos. Supongamos que A emite un SYN a B. El espera un SYN de vuelta, confirmando la conexión. Pueden ocurrir dos cosas mal: el SYN de A se puede perder o la respuesta de B se puede perder. Ambos casos se pueden tratar mediante el uso de un temporizador de retransmisión de SYN. Después que A emite un SYN, lo volverá a emitir cuando el temporizador expire.

Esto puede ocasionar, potencialmente, la aparición de SYN duplicados. Si el SYN de A se pierde no habrá duplicados. Si la respuesta de B se pierde, entonces B podría recibir dos SYN de A. Además, si la

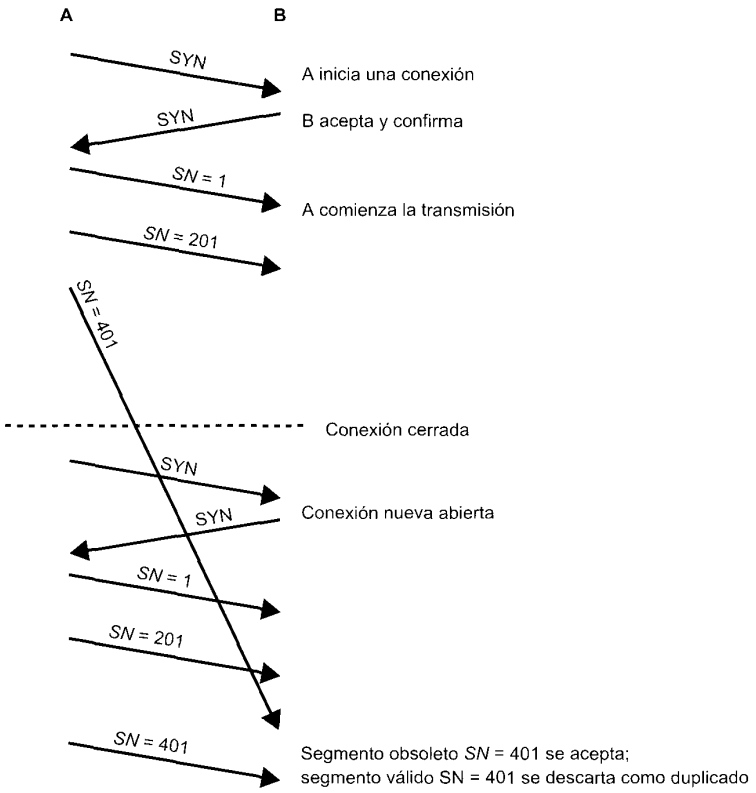


Figura 17.7. El diálogo en dos sentidos; problema con un segmento de datos obsoleto.

respuesta de B no se pierde, si no que simplemente se retrasa, A podría recibir dos SYN de respuesta. Todo esto significa que A y B deben simplemente ignorar los SYN duplicados una vez que la conexión se ha establecido.

Existen otros problemas que hay que tratar. Al igual que un SYN retrasado o una respuesta perdida puede producir un SYN duplicado, un segmento de datos retrasado o una confirmación perdida puede dar lugar a la duplicidad de segmentos de datos, como se ha visto en la Figura 17.6. Estos segmentos retrasados o duplicados pueden interferir con el establecimiento de conexión, como se ilustra en la Figura 17.7. Suponemos que con cada nueva conexión, cada entidad del protocolo de transporte inicia la numeración de sus segmentos de datos con el número de secuencia 1. En la figura, una copia duplicada del segmento *SN* = 401 de una conexión antigua llega durante el tiempo en que la nueva conexión está establecida, y es entregada a la entidad B antes que el segmento de datos legítimo número *SN* = 401. Una forma de abordar este problema es empezar cada nueva conexión con un número de secuencia diferente, elegido lejos del último número de secuencia de la conexión más reciente. Para este propósito, la petición de conexión es de la forma SYN *i*, donde *i* es el número de secuencia del primer segmento de datos que será enviado en esta conexión.

Ahora, consideremos que un SYN *i* duplicado sobrevive hasta pasado el cierre de la conexión. La Figura 17.8 muestra el problema que se puede plantear. Un SYN *i* obsoleto llega a B después de que la conexión ha terminado. B supone que ésta es una petición nueva y responde con SYN *j*. Mientras tanto, A ha decidido abrir una nueva conexión con B y envía SYN *k*. B descarta este último como uno dupli-

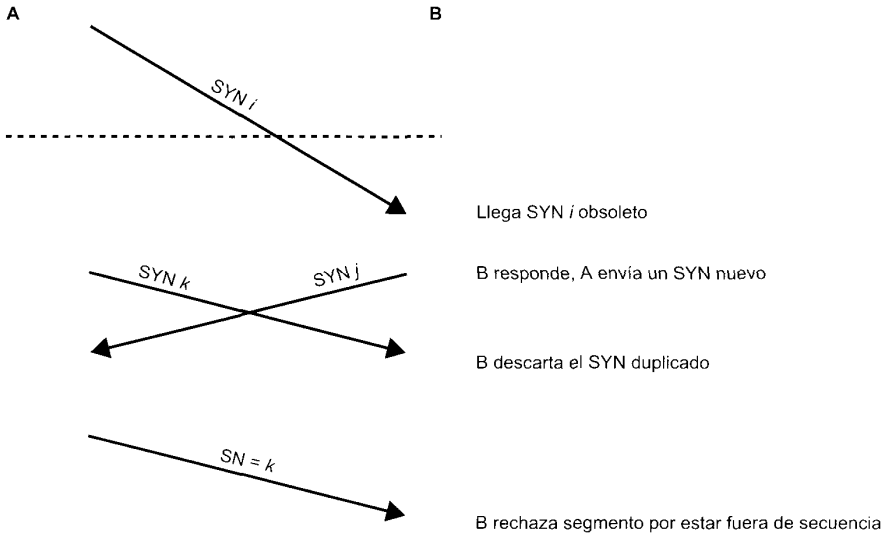


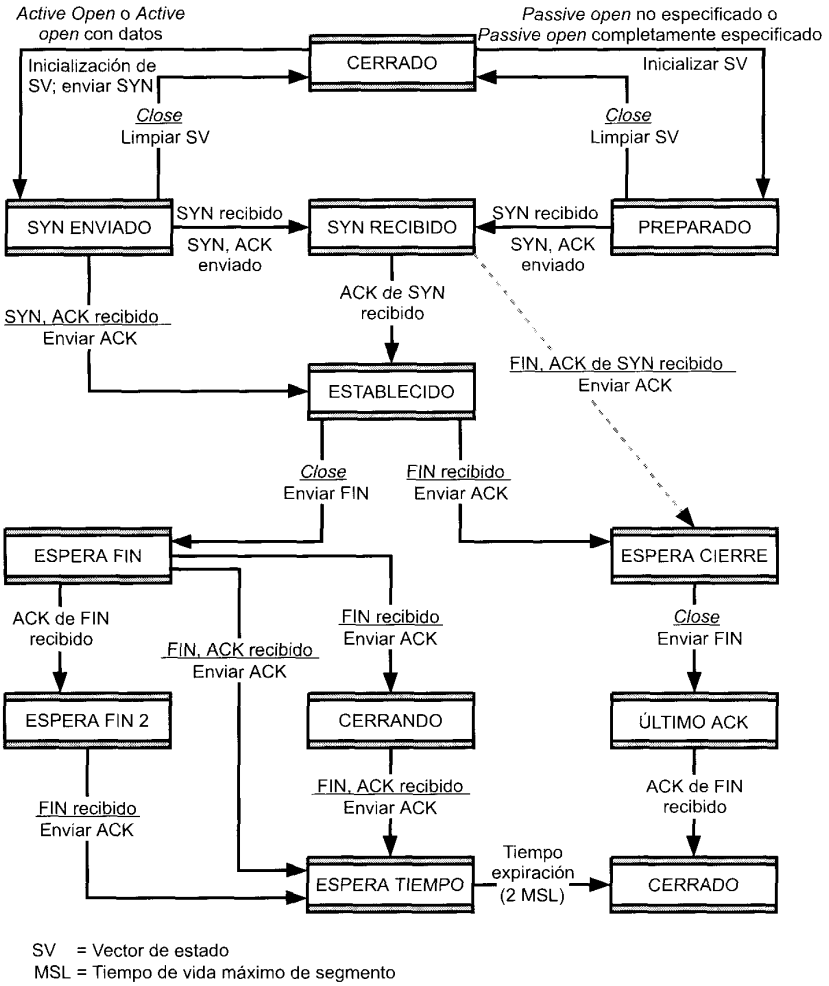
Figura 17.8. El diálogo en dos sentidos; problemas con segmentos SYN obsoletos.

cado. Ahora, ambos lados han transmitido y recibido un segmento SYN, y por lo tanto piensan que existe una conexión válida. Sin embargo, A inicia la transferencia de datos con un segmento numerado con *k*. B rechaza el segmento por estar fuera de secuencia.

La solución de este problema es que cada lado confirme explícitamente el SYN y número de secuencia del otro. El procedimiento es conocido como diálogo en tres direcciones. El diagrama de estados de conexión revisado, que es uno de los empleados por TCP, se muestra en la parte superior de la Figura 17.9. Se ha incluido un nuevo estado (SYN RECIBIDO). En este estado, la entidad de transporte se muestra indecisa durante el proceso de abrir una conexión para asegurar que cualquier SYN que ha sido enviado ha sido también confirmado antes de que la conexión se declare abierta. Además del nuevo estado, hay un nuevo segmento de control (RST) para reinicializar al otro lado cuando se detecta un SYN duplicado.

La Figura 17.10 ilustra las operaciones típicas del diálogo en tres direcciones. En la Figura 17.10a la entidad de transporte A inicia la conexión. El SYN de A incluye el número de secuencia de envío, *i*. El SYN de respuesta confirma el número e incluye el número de secuencia para el otro extremo. A confirma el SYN/ACK en su primer segmento de datos. La Figura 17.10b muestra la situación en la que un SYN *i* obsoleto llega a B después de cerrar la conexión relevante. B supone que es una petición nueva y responde con SYN *j*, $AN = i$. Cuando A recibe este mensaje, se da cuenta que él no ha solicitado una conexión y por lo tanto envía un RST, $AN = j$. Hay que notar que la porción $AN = j$ del mensaje RST es esencial para que un RST duplicado obsoleto no cancele un establecimiento de conexión legítimo. La Figura 17.10c muestra un caso en que un SYN/ACK obsoleto llega en medio del establecimiento de una nueva conexión. Debido al uso de números de secuencia en las confirmaciones, este evento no causa perjuicio.

Por simplicidad, la parte superior de la Figura 17.9 no incluye transiciones en las que se envía RST. La regla básica es: Enviar un RST si el estado de la conexión no es todavía ABIERTO y se recibe un ACK inválido (uno que no referencia a algo que ha sido enviado). El lector debería intentar varias combinaciones de eventos para ver que este procedimiento de establecimiento de conexión funciona ante cualquier combinación de segmentos obsoletos o perdidos.



SV = Vector de estado
MSL = Tiempo de vida máximo de segmento

Figura 17.9. Diagrama de estado de una entidad TCP.

Cierre de la conexión

El diagrama de estados de la Figura 17.4 define el uso de un diálogo en dos sentidos simple para el establecimiento de la conexión, que ha resultado insatisfactorio con servicios de red no seguros. De igual forma, el diálogo en dos sentidos definido en ese diagrama para el cierre de conexión es inadecuado para un servicio de red no seguro. El siguiente escenario podría ser causado por un desorden de los segmentos. Una entidad de transporte en el estado ESPERA CIERRE envía su último segmento de datos, seguido por un segmento FIN, pero el segmento FIN llega al otro extremo antes que el último segmento de datos. La entidad de transporte receptora aceptará ese FIN, cerrará la conexión y perderá al último segmento de datos. Para evitar este problema, se puede asociar un número de secuencia con FIN, que puede ser el siguiente número de secuencia después del último octeto de los datos transmitidos. Con este refinamiento, la entidad de transporte receptora, después de recibir un FIN, esperará si es necesario a los datos que lleguen tarde antes de cerrar la conexión.

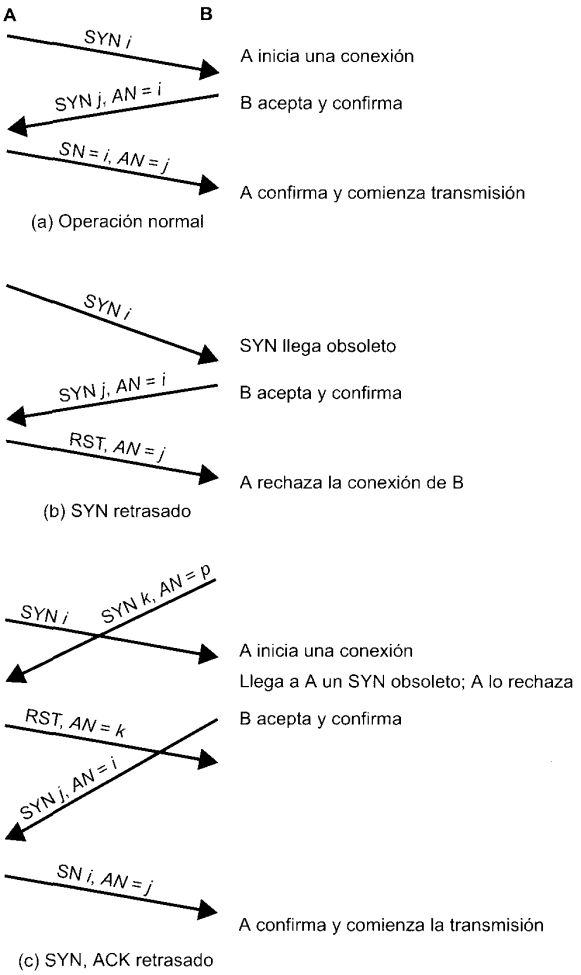


Figura 17.10. Ejemplo de diálogo en tres sentidos.

Un problema más serio es la potencial pérdida de segmentos y la presencia potencial de segmentos obsoletos. La Figura 17.9 muestra que el procedimiento de cierre adopta una solución similar que la usada para el establecimiento de la conexión. Cada extremo debe explícitamente confirmar el segmento FIN del otro usando un ACK con número de secuencia del FIN a confirmar. Para realizar un cierre ordenado, una entidad de transporte requiere lo siguiente:

- Debe enviar un FIN i y recibir un $AN = i$.
- Debe recibir un FIN j y enviar un $AN = j$.
- Debe esperar un intervalo igual a dos veces el máximo del tiempo de vida esperado de un segmento.

Recuperación de caídas

Cuando el sistema sobre el que una entidad de transporte se está ejecutando falla y consecuentemente rearranca, la información de estado de todas las conexiones se pierden. Las conexiones afectadas llegan

a estar «medio abiertas» ya que el lado que no se vio afectado por la caída no se ha dado cuenta todavía del problema.

El lado todavía activo de la conexión medio abierta puede cerrar la conexión usando un temporizador de renuncia. Este temporizador mide el tiempo máximo que la máquina de transporte continuará esperando una confirmación (u otra respuesta apropiada) de un segmento transmitido después de que el segmento ha sido retransmitido el máximo número de veces. Cuando el temporizador expira, la entidad de transporte supone que la otra entidad de transporte o que la red que interviene ha fallado, cierra la conexión e indica un cierre no normal al usuario TS.

En el caso que una entidad de transporte se cancele y rearranque rápidamente, la conexión medio abierta se puede terminar más rápidamente mediante el uso del segmento RST. El lado que falla devuelve un RST *i* por cada segmento *i* que recibe. Cuando el RST *i* se recibe en el otro extremo, se debe comprobar su validez basándose en el número de secuencia *i*, ya que el RST podría ser en respuesta a un segmento obsoleto. Si el reinicio es válido, la entidad de transporte ejecuta un cierre no normal.

Estas medidas clarifican la situación a nivel de transporte. La decisión de reabrir la conexión se deja al usuario TS. El problema es de sincronización. Cuando ocurrió la caída, podría haber uno o más segmentos enviados en ambas direcciones. El usuario TS en el lado que no se cayó sabe cuántos datos ha recibido, pero el otro usuario no, si la información de estado se ha perdido. Así, existe el peligro de que algunos datos de usuario se pierdan o se dupliquen.

17.2. TCP

El conjunto de protocolos TCP/IP incluye dos protocolos en la capa de transporte: el protocolo de control de la transmisión, (TCP, Transmission Control Protocol), que es un protocolo orientado a conexión, y el protocolo datagrama de usuario, (UDP, User Datagram Protocol), que es no orientado a conexión. En esta sección examinaremos el protocolo TCP (especificado en el RFC 793), primero los servicios que ofrece al usuario TS y luego los detalles internos del protocolo.

SERVICIOS TCP

TCP está diseñado para proporcionar una comunicación segura entre pares de procesos (usuarios TCP) a través de una gran variedad de redes seguras e inseguras así como sobre un conjunto de redes interconectadas. TCP suministra dos facilidades útiles para etiquetar datos: cargar y urgente:

- **Cargar flujo de datos:** normalmente, TCP decide cuando se han acumulado suficientes datos para formar un segmento para su transmisión. El usuario TCP puede requerir que TCP transmita todos los datos pendientes a los que incluye una etiqueta con un indicador de carga. En el extremo receptor, TCP entregará los datos al usuario en la misma forma. Un usuario puede requerir esto si en los datos se detecta una interrupción lógica.
- **Indicación de datos urgentes:** esta posibilidad proporciona un medio para informar al usuario TCP destino que en el flujo de datos entrantes existen datos significativos o «urgentes». Es responsabilidad de usuario destino realizar la acción apropiada.

Como con IP, los servicios suministrados por TCP se definen en términos de primitivas y parámetros (véase Figura 15.5). Los servicios proporcionados por TCP son considerablemente más ricos que los proporcionados por IP y, por tanto, el conjunto de primitivas y parámetros es más complejo. La Tabla 17.2 lista las primitivas de petición de servicio TCP, que son emitidas por el usuario TCP a TCP, y la Tabla 17.3 lista las primitivas respuesta de servicio TCP, emitidas por TCP a un usuario TCP local. La Tabla 17.4 proporciona una breve definición de los parámetros relacionados. Se han incorporado varios comentarios. Las dos órdenes de establecimiento pasivo indican el deseo del usuario TCP de aceptar una petición de conexión. El establecimiento activo con datos permite al usuario comenzar transmitiendo datos con el establecimiento de la conexión.

Tabla 17.2. Primitivas de solicitud de servicio TCP.

Primitiva	Parámetros	Descripción
Passive open no especificado	puerto-origen, [tiempo-expiración], [acción-tiempo-expiración], [precedencia], [rango-de-seguridad]	Preparado para intentos de conexión con una seguridad y precedencia especificadas desde cualquier destino remoto.
Passive open completamente especificado	puerto-origen, puerto-destino, dirección-destino, [tiempo-expiración], [acción-tiempo-expiración], [precedencia], [rango-de-seguridad]	Preparado para intentos de conexión con una seguridad y precedencia especificadas desde destino remoto especificado.
Active open	puerto-origen, puerto-destino, dirección-destino, [tiempo-expiración], [acción-tiempo-expiración], [precedencia], [seguridad]	Solicita una conexión con una seguridad y precedencia particulares al destino especificado.
Active open con datos	puerto-origen, puerto-destino, dirección-destino, [tiempo-expiración], [acción-tiempo-expiración], [precedencia], [seguridad], datos, longitud-datos, indicador-PUSH, indicador-URGENT	Solicita una conexión con una seguridad y precedencia particulares al destino especificado y transmite datos con la solicitud.
Send	nombre-conexión-local, datos, longitud-datos, indicador-PUSH, indicador-URGENT, [tiempo-expiración], [acción-tiempo-expiración]	Transfiere datos a través de la conexión indicada.
Allocate	nombre-conexión-local, longitud-datos	Emite un incremento de asignación de créditos para recibir datos en TCP.
Close	nombre-conexión-local	Cierra la conexión ordenadamente
Abort	nombre-conexión-local	Cierra la conexión abruptamente
Status	nombre-conexión-local	Pregunta el estado de la conexión

Nota: Los paréntesis cuadrados indican parámetros opcionales.

FORMATO DE LA CABECERA TCP

TCP utiliza un único tipo de unidad de datos de protocolo, llamado segmento TCP. La cabecera se muestra en la Figura 17.11. Ya que la cabecera debe servir para implementar todos los mecanismos del protocolo, ésta es más bien grande, con una longitud mínima de 20 octetos. Los campos son los siguientes:

- **Puerto origen (16 bits):** usuario TCP origen.
- **Puerto destino (16 bits):** usuario TCP destino.
- **Número de secuencia (32 bits):** número de secuencia del primer octeto en este segmento excepto si el indicador SYN está presente. Si el indicador SYN está presente, es el número de secuencia inicial (ISN, Initial Sequence Number) y en este caso el primer octeto de datos es el ISN + 1.
- **Número de confirmación (32 bits):** una confirmación *piggybacking*. Contiene el número de secuencia del siguiente octeto que la entidad TCP espera recibir.

Tabla 17.3. Primitivas de respuesta de servicio TCP.

Primitiva	Parámetros	Descripción
Open ID	nombre-conexión-local, puerto-origen, puerto-destino*, dirección-destino*	Informa al usuario TCP de un nombre de conexión asignado a una conexión pendiente solicitado en una primitiva *Open*.
Open failure	nombre-conexión-local	Informa sobre un fallo de una solicitud *Active open*.
Open success	nombre-conexión-local	Informa sobre la conclusión de una solicitud *Open* pendiente.
Deliver	nombre-conexión-local, datos, longitud-datos, indicador-URGENT	Informa sobre la llegada de datos.
Closing	nombre-conexión-local	Informa que el usuario TCP remoto ha emitido un *Open* y que todos los datos enviados por el usuario remoto han sido entregados.
Terminate	nombre-conexión-local, descripción	Informa que la conexión se ha terminado; se proporciona una descripción de la razón por la que ha terminado.
Status Response	nombre-conexión-local, puerto-origen, dirección-origen puerto-destino, dirección-destino, estado-conexión, ventana-recibida, ventana-enviada, cantidad-esperando-ACK, cantidad-esperando-recibo, estado-urgente, precedencia, seguridad, tiempo-expiración	Informa el estado actual de la conexión.
Error	nombre-conexión-local, descripción	Informa servicios solicitados o errores internos.

* = No utilizado por *Passive open* no especificado.

- **Longitud de la cabecera (4 bits):** número de palabras de 32 bits en la cabecera.
- **Reservados (6 bits):** bits reservados para un uso futuro.
- **Indicadores (6 bits):**

  URG: el campo puntero urgente es válido.

  ACK: el campo de confirmación es válido.

  PSH: función de carga.

  RST: puesta a cero de la conexión.

  SYN: sincronizar los números de secuencia.

  FIN: el emisor no tiene más datos.

- **Ventana (16 bits):** asignación de créditos de control de flujo, en octetos. Contiene el número de octetos de datos comenzando con el que se indica en el campo de confirmación y que él que envía está dispuesto a aceptar.

Tabla 17.4. Parámetros de servicio TCP.

Puerto origen	Usuario TCP local.
Tiempo expiración	El mayor retardo permitido para la entrega de datos antes de un cierre de la conexión automático o de un informe de error; especificado por el usuario.
Acción tiempo expiración	Indica si se termina la conexión o se informa sobre un error al usuario TCP cuando ha transcurrido el tiempo de expiración.
Precedencia	Nivel de precedencia para una conexión. Toma valores de cero (el más bajo) a siete (más alto); es el mismo parámetro que el definido para IP.
Rango seguridad	Rangos permitidos en grupos, restricciones de mantenimiento, códigos de control de transmisión y niveles de seguridad.
Puerto destino	Usuario TCP remoto.
Dirección destino	Dirección Internet del computador remoto.
Seguridad	Información de seguridad para la conexión, incluyendo nivel de seguridad, grupos, restricciones de mantenimiento, códigos de control de transmisión; los mismo parámetros que los definidos para IP.
Datos	Bloque de datos enviados por el usuario TCP o entregado a un usuario TCP.
Longitud datos	Longitud de los datos enviados o entregados.
Indicador CARGA	Si vale uno, indica que los datos asociados se van a suministrar con el servicio de carga de flujo de datos.
Indicador URGENTE	Si vale uno, indica que los datos asociados se van a suministrar con el servicio de indicación de datos urgentes.
Nombre conexión local	Identificador de una conexión definida por un par del tipo (socket local, socket remoto); proporcionado por TCP.
Descripción	Información suplementaria en una primitiva *Terminate* o *Error*.
Dirección fuente	Dirección Internet del computador local.
Estado de la conexión	Estado de la conexión referenciada (CERRADO, ABIERTO ACTIVO, ABIERTO PASIVO, ESTABLECIDO, CERRANDO).
Ventana recibida	Cantidad de datos en octetos que la entidad TCP local está dispuesta a recibir.
Ventana enviada	Cantidad de datos en octetos permitida que se puede enviar a la entidad TCP remota.
Cantidad esperando ACK	Cantidad de datos previamente transmitidos esperando confirmación.
Cantidad esperando recibo	Cantidad de datos en octetos almacenados temporalmente en la entidad TCP local pendiente de ser recibidos por el usuario TCP local.
Estado urgente	Informa al usuario TCP que recibe datos si hay datos urgentes disponibles o si todos los datos urgentes, si hay, han sido entregados al usuario.

- **Suma de verificación (16 bits):** el complemento a uno de la suma módulo $2^{16} - 1$ de todas las palabras de 16 bits en el segmento más una seudo-cabecera, descrita más abajo.
- **Puntero urgente (16 bits):** señala el octeto que sigue a los datos urgentes. Esto permite al receptor conocer cuantos datos urgentes llegan.
- **Opciones (Variable):** si está presente, solamente se define una opción, que especifica el tamaño máximo del segmento que será aceptado.

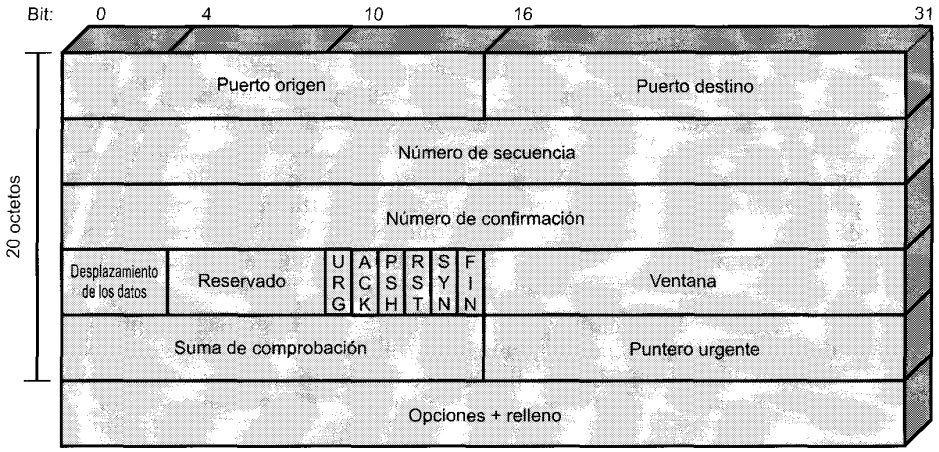


Figura 17.11. Cabecera TCP.

El *número de secuencia* y el *número de confirmación* hacen referencia a octetos en lugar de al segmento entero. Por ejemplo, si un segmento contiene el número de secuencia 1.001 e incluye 600 octetos de datos, el número de secuencia se refiere al primer octeto en el campo de datos; el segmento siguiente en orden lógico tendrá en número de secuencia 1.601. Es por eso que TCP está lógicamente orientado a flujo: acepta un flujo de datos del usuario, los agrupa en segmentos según él vea y numera cada octeto en el flujo.

El campo *suma de verificación* se aplica a todo el segmento entero más una seudo-cabecera incorporada en el momento del cálculo (tanto en la transmisión como en la recepción). La seudo-cabecera incluye los siguientes campos de la cabecera IP: dirección internet origen y destino, el protocolo y un campo longitud del segmento. Con la inclusión de la seudo-cabecera, TCP se protege a sí mismo de una transmisión errónea de IP. Esto es, si IP lleva un segmento a un computador erróneo, aunque el segmento esté libre de errores, la entidad TCP receptora detectará el error de transmisión.

Comparando la cabecera TCP con la interfaz de usuario TCP definida en las Tablas 17.2 y 17.3, el lector podría pensar que algunos campos están ausentes de la cabecera TCP, y es verdad en este caso. TCP está diseñado específicamente para trabajar con IP. Por tanto, algunos parámetros de usuario se pasan a través TCP a IP para su inclusión en la cabecera IP. Los más relevantes son:

- Prioridad: un campo de 3 bits.
- Retardo-normal/bajo-retardo.
- Rendimiento-normal/rendimiento-alto.
- Seguridad-normal/seguridad-alta.
- Protección: un campo de 11 bits.

Merece la pena observar que esta unión TCP/IP significa que la información suplementaria mínima requerida para cada unidad de datos es en realidad de 40 octetos.

MECANISMOS TCP

Podemos agrupar los mecanismos de TCP en las categorías de establecimiento de la conexión, transferencia de datos y cierre de la conexión.

Establecimiento de la conexión

El establecimiento de la conexión en TCP siempre utiliza un diálogo en tres sentidos. Cuando el indicador SYN está activado, el segmento es esencialmente una petición de conexión y funciona como se ha indicado en la Sección 17.1. Para iniciar una conexión, una entidad envía un SYN, $SN = X$, donde X es el número de secuencia inicial. El receptor responde con SYN, $SN = Y$, $AN = X + 1$ mediante el establecimiento de los indicadores SYN y ACK. Hay que darse cuenta que la confirmación indica que el receptor está ahora esperando recibir un segmento comenzando con un octeto de datos $X + 1$, confirmando el SYN que ocupaba $SN = X$. Finalmente, el que inicia la conexión responde con $AN = Y + 1$. No se producen problemas si ambos extremos emiten SYN y éstos se cruzan en los trayectos. Ambos lados responden con ACK.

Una conexión está únicamente determinada por los puertos origen y destino. Así, en cualquier instante de tiempo, sólamente puede haber una única conexión TCP entre un único par de puertos. Sin embargo, un puerto dado puede admitir múltiples conexiones, cada una con diferentes puertos.

Transferencia de datos

Aunque los datos se transmiten en segmentos a través de una conexión de transporte, la transferencia de datos es vista desde un punto de visto lógico como un flujo de octetos. Por tanto, cada octeto es numerado, modulo 2^{32}. Cada segmento contiene el número de secuencia del primer octeto en el campo de datos. El control de flujo se ejerce utilizando un esquema de asignación de créditos en el cual el crédito es un número de octetos en lugar de segmentos, como se ha explicado en la Sección 17.1.

Los datos se almacenan en memoria temporal por la entidad de transporte tanto en la transmisión como en la recepción. TCP normalmente aplica su propio criterio a la hora de construir un segmento para transmitirlo o cuando entrega los datos recibidos al usuario. El indicador PUSH se usa para forzar a que los datos acumulados sean enviados por el transmisor y entregados al usuario por el receptor. Esto sirve como una función de fin-de-bloque.

El usuario puede especificar un bloque de datos como urgente. TCP designará el fin de ese bloque con un puntero de urgente y lo enviará en el flujo de datos ordinario. El usuario receptor es alertado que se están recibiendo datos urgentes.

Si, durante el intercambio de datos, llega un segmento que aparentemente no va dirigido a la conexión actual, el valor del indicador RST se activa en un segmento saliente. Ejemplos de esta situación se encuentran en los SYN duplicados, retrasados y en las confirmaciones de datos todavía no enviados.

Cierre de la conexión

El procedimiento normal de terminar una conexión es un cierre ordenado. Cada usuario TCP debe emitir una primitiva CLOSE. La entidad de transporte establece el bit FIN en el último segmento que envía y que contiene los últimos datos que se envían en esa conexión.

Si el usuario emite una primitiva ABORT ocurre un cierre abrupto. En este caso, la entidad de transporte abandona todos los intentos de enviar o recibir datos y descarta los datos en las memorias temporales de transmisión y recepción. Se envía un segmento RST al otro extremo.

OPCIONES EN LOS CRITERIOS DE IMPLEMENTACIÓN DE TCP

El estándar TCP proporciona una especificación precisa del protocolo que se va a utilizar entre entidades TCP. Sin embargo, ciertos aspectos del protocolo admiten varias opciones de implementación posibles. Aunque dos implementaciones que eligen opciones alternativas puede interoperar, hay implicaciones en el rendimiento. Las áreas de diseño para las que se especifican opciones son las siguientes:

- Criterio de envío.
- Criterio de entrega.
- Criterio de aceptación.
- Criterio de retransmisión.
- Criterio de confirmación.

Criterio de envío

En ausencia de datos marcados con el indicador de carga (PUSH) y una ventana de transmisión cerrada (véase Figura 17.3a), la entidad TCP que envía datos es libre de enviarlos a su propia conveniencia. Conforme los datos son emitidos por el usuario, estos se almacenan en las memorias temporales de transmisión. TCP podría construir un segmento por cada lote de datos proporcionado por su usuario o podría esperar hasta que se acumula una cierta cantidad de datos antes de construir y enviar el segmento. El criterio real dependerá de consideraciones de rendimiento. Si las transmisiones son grandes e infrecuentes, hay poca información suplementaria en términos de generación de segmentos y procesamiento. Por otro lado, si las transmisiones son frecuentes y pequeñas, entonces el sistema está proporcionando una respuesta rápida.

Criterio de entrega

En ausencia del indicador PUSH, una entidad TCP receptora es libre de entregar los datos al usuario de acuerdo a su propia conveniencia. Puede entregar los datos conforme se reciben los segmentos en orden o podría almacenar los datos de varios segmentos en las memorias temporales de recepción antes de hacer la entrega. El criterio real dependerá en consideraciones de rendimiento. Si las entregas son infrecuentes y grandes, el usuario no está recibiendo los datos tan pronto como sería deseable. Por otro lado, si las entregas son frecuentes y pequeñas, habría un procesamiento innecesario en el software de TCP y del usuario, así como un número innecesario de interrupciones del sistema operativo.

Criterio de aceptación

Cuando todos los segmentos de datos llegan en orden a una conexión TCP, los datos se sitúan en las memorias temporales de recepción para entregarlos al usuario. Es posible, sin embargo, que los segmentos lleguen fuera de secuencia. En este caso, la entidad TCP receptora tiene dos opciones:

- Aceptación **en-orden:** acepta sólo segmentos que llegan en orden; cualquier segmento que llega fuera de secuencia se descarta.
- Aceptación **en-ventana:** acepta todos los segmentos que están dentro de la ventana de recepción (véase Figura 17.3b).

El criterio de aceptación en-orden da lugar a una implementación sencilla pero transfiere el problema a la red, ya que la entidad TCP que envía debe retransmitir aquellos segmentos a los que expira el temporizador de retransmisión y que se recibieron correctamente pero descartados por la recepción fuera de secuencia. Además, si se pierde un único segmento en la transmisión, entonces todos los segmentos siguientes deben ser retransmitidos una vez que expira el temporizador del segmento perdido.

El criterio de aceptación en-ventana reduciría las transmisiones pero requiere un test de aceptación más complejo y un esquema de almacenamiento de datos más sofisticado para almacenar y llevar el registro de los datos aceptados fuera de secuencia.

Criterio de retransmisión

TCP mantiene una lista de los segmentos que han sido enviados pero que todavía no han sido confirmados. La especificación de TCP establece que TCP retransmitirá un segmento si no recibe una confirma-

ción dentro de un tiempo determinado. Una implementación TCP podría emplear una de estas tres estrategias de retransmisión:

- **Primero-solamente:** mantiene un temporizador de retransmisión para la lista entera. Si se recibe una confirmación, elimina el segmento o segmentos apropiados de la lista y pone a cero el temporizador. Si el temporizador expira, retransmite el segmento primero de la lista y pone a cero el temporizador.
- **Por lotes:** mantiene un temporizador de retransmisión para la lista entera. Si se recibe una confirmación, elimina el segmento o segmentos apropiados de la lista y pone a cero el temporizador. Si el temporizador expira, retransmite todos los segmentos de la lista y pone a cero el temporizador.
- **Individual:** mantiene un temporizador de retransmisión para cada segmento en la lista. Si se recibe una confirmación, elimina el segmento o segmentos apropiados de la lista y destruye el temporizador o temporizadores asociados. Si cualquier temporizador expira, retransmite el segmento correspondiente individualmente y pone a cero su temporizador.

El criterio «primero-solamente» es eficiente en términos de tráfico generado, ya que solamente se retransmiten los segmentos perdidos (o segmentos cuyo ACK se perdió). Ya que el temporizador para el segundo segmento en la cola no se establece hasta que el primer segmento se confirma, puede haber retardos considerables. El criterio «individual» soluciona este problema a expensas de una implementación más compleja. El criterio «por lotes» también reduce la probabilidad de un gran retardo pero podría producir retransmisiones innecesarias.

La efectividad real del criterio de retransmisión depende en parte del criterio de aceptación del receptor. Si el receptor está usando un criterio de aceptación en-orden, entonces descartará los segmentos recibidos tras un segmento perdido. Este criterio encaja mejor con una retransmisión por lotes. Si el receptor está usando un criterio de aceptación en-ventana, entonces es mejor un criterio de retransmisión primero solamente o individual. Por supuesto, en una red mixta de computadores, se pueden usar ambos criterios de aceptación.

Criterio de confirmación

Cuando llega un segmento que está en secuencia, la entidad TCP receptora tiene dos opciones en cuanto a la generación de las confirmaciones:

- **Inmediato:** cuando los datos se aceptan, inmediatamente se transmite un segmento vacío (sin datos) conteniendo el número de confirmación apropiado.
- **Acumulativo:** cuando los datos se aceptan, registra la necesidad de una confirmación pero espera un segmento de datos de salida con datos y mediante la técnica de *piggybacking* incluye la confirmación. Para evitar grandes retardos, establece un temporizador de ventana (véase Tabla 17.1); si el temporizador expira antes de que se envíe una confirmación, transmite un segmento vacío conteniendo el número de confirmación apropiado.

El criterio «inmediato» es sencillo y mantiene a la entidad TCP emisora completamente informada, lo que evita retransmisiones innecesarias. Sin embargo, este criterio da lugar a retransmisiones de segmentos extras, a saber, segmentos vacíos usados sólo para ACK. Además, este criterio puede causar una carga superior en la red. Considérese que una entidad TCP recibe un segmento e inmediatamente envía un ACK. Entonces los datos se pasan a la aplicación, lo que expande la ventana de recepción, activando otro segmento TCP vacío que proporciona un crédito adicional a la entidad TCP emisora.

Normalmente, a causa de la información suplementaria potencial de un criterio «inmediato», generalmente se usa el criterio «acumulativo». Hay que darse cuenta que, sin embargo, el uso de este criterio requiere más procesamiento en el extremo receptor y complica la tarea de estimar el retardo de ida-y-vuelta por la entidad TCP emisora.

17.3. CONTROL DE LA CONGESTIÓN EN TCP

El mecanismo de control de flujo basado en créditos de TCP se diseñó para permitir que el destino restrinja el flujo de segmentos de una fuente y evitar la saturación de la memoria temporal en el destino. Este mismo mecanismo de control de flujo se utiliza ahora de varias formas ingeniosas para proporcionar control de congestión sobre Internet entre una fuente y un destino. La congestión, como ya se ha visto varias veces en este libro, tiene dos efectos principales. Primero, cuando la congestión empieza a ocurrir, el tiempo de tránsito a través de la red o la interconexión de redes aumenta. Segundo, conforme la congestión se hace severa, los paquetes o los segmentos se descartan por la red o por los nodos de la interconexión. El mecanismo de control de flujo de TCP se puede utilizar para identificar el comienzo de la congestión (reconociendo el incremento de los tiempos de retardo y de los segmentos descartados) y reaccionar mediante la reducción del flujo de datos. Si muchas de las entidades TCP que operan a lo largo de una red practican este tipo de contención, la congestión en Internet se puede aliviar.

Desde la publicación del RFC 793, se han implementado varias técnicas que intentaban mejorar las características de control de congestión de TCP. Ninguna de estas técnicas extienden o violan el estándar TCP original; más bien representan criterios de implementación que están dentro del ámbito de la especificación de TCP. Muchas de estas técnicas son de uso obligatorio en TCP como se refleja en el RFC 1122 (Obligaciones de los Computadores en Internet), mientras otras se especifican en el RFC 2001. Las técnicas se pueden agrupar, en un sentido amplio, en dos categorías: gestión de los temporizadores de retransmisión y gestión de la ventana. En esta sección se examinan algunas de las técnicas más importantes y más utilizadas.

GESTIÓN DE LOS TEMPORIZADORES DE RETRANSMISIÓN

Conforme cambian las condiciones de red o del conjunto de redes, un temporizador de retransmisión estático puede llegar a ser demasiado grande o demasiado breve. De acuerdo con esto, virtualmente todas las implementaciones de TCP intentan estimar el retardo de ida y vuelta actual mediante la observación del patrón de retardo de los segmentos más recientes, y entonces establecer el temporizador a un valor un poco mayor que el retardo de ida y vuelta estimado.

Promediado simple

Una técnica sería tomar la media de los tiempos de ida y vuelta observados sobre un determinado número de segmentos. Si la media predice con precisión los retardos de ida y vuelta futuros, entonces el temporizador de retransmisión proporcionará unas buenas prestaciones. El método de promediado simple se puede expresar como:

$$\text{ARTT}(K+1) = \frac{1}{K+1}\sum_{i=1}^{K+1}\text{RTT}(i) \tag{17.1}$$

donde RTT(i) es el tiempo de ida y vuelta observado para el segmento i-ésimo transmitido y ARTT(K) es el tiempo de ida y vuelta medio para los K primeros segmentos.

Esta expresión se puede reescribir como:

$$\text{ARTT}(K+1) = \frac{K}{K+1}\text{ARTT}(K) + \frac{1}{K+1}\text{RTT}(K+1) \tag{17.2}$$

Con esta formulación, no es necesario calcular la sumatoria completa cada vez.

Promedio exponencial

Nótese que a cada término en la sumatoria se le da un peso igual; esto es, cada término se multiplica por la misma constante $1/(K + 1)$. Normalmente, nos interesaría dar mayor peso a los casos más recientes ya que es más probable que reflejen el comportamiento futuro. Una técnica común para predecir los valores siguientes sobre la base de una serie de tiempos de valores pasados, y que es el especificado en el RFC 793, es el promediado exponencial:

$$\text{SRTT}(K + 1) = \alpha \times \text{SRTT}(K) + (1 - \alpha) \times \text{RTT}(K + 1) \tag{17.3}$$

donde SRTT (K) se llama estimación del tiempo de ida y vuelta suavizado y se define SRTT(0) = 0. Compárese esta ecuación con la Ecuación (17.2). Mediante el uso de un valor constante de $\alpha(0 < \alpha < 1)$, independientemente del número de observaciones pasadas, tenemos una circunstancia en la cual se consideran todas los valores pasados, pero con menos peso las más distantes. Para ver esto más claramente, consideremos la expansión de la Ecuación (17.3):

$$\begin{aligned}\text{SRTT}(K + 1) = {} & (1 - \alpha)\text{RTT}(K + 1) + \alpha(1 - \alpha)\text{RTT}(K) + \\ & + \alpha^2(1 - \alpha)\text{RTT}(K - 1) + \cdots + \alpha^K(1 - \alpha)\text{RTT}(1)\end{aligned}$$

Ya que α y $(1 - \alpha)$ son menores que uno, cada término sucesivo en la ecuación precedente es más pequeño. Por ejemplo, para $\alpha = 0{,}8$, la expansión es

$$\text{SRTT}(K + 1) = 0{,}2\text{RTT}(K + 1) + 0{,}16\text{RTT}(K) + 0{,}128\text{RTT}(K - 1) + \cdots$$

Cuanto más antigua es la observación menos cuenta en el promedio.

Cuanto más pequeño es el valor de α, más grande es el peso dado a las observaciones más recientes. Para $\alpha = 0{,}5$, prácticamente todo el peso se le da a las cuatro o cinco observaciones más recientes, mientras que si $\alpha = 0{,}875$, el promediado se extiende hasta la observación 10 o de ese orden. La ventaja de utilizar valores pequeños de α es que el promedio reflejará rápidamente un cambio rápido en las cantidades observadas. La desventaja es que si hay un transitorio breve en las cantidades observadas y después se vuelve a algún valor relativamente constante, el uso de valores pequeños de α resultará en cambios desiguales en el promedio.

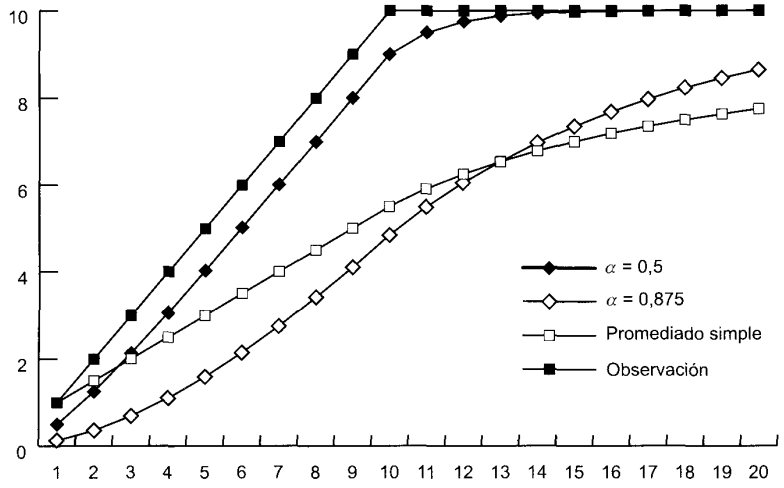
La Figura 17.12 compara el promediado simple con el promediado exponencial (para dos valores de α). En la parte (a) de la figura, el valor observado empieza con 1, crece gradualmente hasta el valor de 10 y luego permanece ahí. En la parte (b) de la figura, el valor observado empieza en 20, decrece gradualmente hasta 10 y luego permanece ahí. Nótese que el promediado exponencial sigue los cambios en el comportamiento del proceso más rápido que el promediado simple y el valor más pequeño de α resulta en reacciones más rápidas al cambio en el valor observado.

La Ecuación (17.3) es utilizada en el RFC 793 para estimar el tiempo actual de ida y vuelta. Como se mencionó, el valor del temporizador se debe establecer a un valor un poco mayor que el tiempo estimado de ida y vuelta. Una posibilidad es utilizar un valor constante:

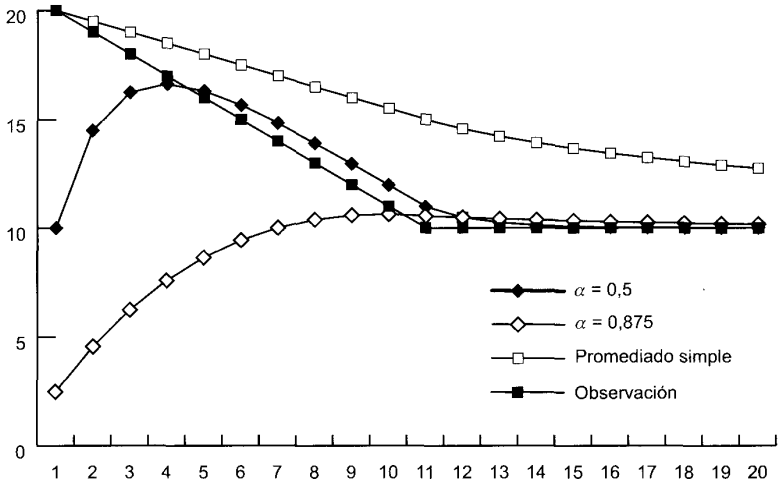
$$\text{RTO}(K + 1) = \text{SRTT}(K + 1) + \Delta$$

donde RTO es el temporizador de retransmisión (también llamado el valor de expiración de retransmisión) y Δ es una constante. La desventaja de esto es que Δ no es proporcional a SRTT. Para valores grandes de SRTT, Δ es relativamente pequeño y las fluctuaciones en el valor real de RTT resultan en retransmisiones innecesarias. Para valores pequeños de SRTT, Δ es relativamente grande y causa retardos innecesarios en la retransmisión de segmentos perdidos. De acuerdo a esto, el RFC 793 especifica la utilización de un temporizador cuyo valor es proporcional a SRTT, dentro de unos límites:

$$\text{RTO}(K + 1) = \text{MIN}(\text{UBOUND}, \text{MAX}(\text{LBOUND}, \beta \times \text{SRTT}(K + 1))) \tag{17.4}$$



(a) Función creciente



(b) Función decreciente

Figura 17.12. Utilización del promediado exponencial.

donde UBOUND y LBOUND son unos límites superior e inferior, fijos y preseleccionados, al valor del temporizador y β es una constante. El RFC 793 no recomienda valores específicos pero da como «valores ejemplos» los siguientes: α entre 0,8 y 0,9 y β entre 1,3 y 2.

Estimación de la varianza de RTT (Algoritmo de Jacobson)

La técnica especificada en el estándar TCP, y descrita en las Ecuaciones (17.3) y (17.4), habilita a una entidad TCP a adaptarse a los cambios en el tiempo de ida y vuelta. Sin embargo, no trata bien una

situación en la que el tiempo de ida y vuelta exhibe una varianza relativamente elevada. [ZHAN86] señala tres fuentes de esta varianza elevada:

1. Si la velocidad de transferencia de datos en una conexión TCP es relativamente baja, entonces el retardo de retransmisión será relativamente grande comparado con el tiempo de propagación y la varianza en el retardo debida a la varianza en el tamaño de los datagramas IP será significativa. De esta forma, el estimador de SRTT está fuertemente influenciado por las características que son propiedad de los datos y no de la red.
2. La carga de tráfico y las condicione en Internet pueden cambiar abruptamente debido al tráfico de otras fuentes, causando cambios bruscos en el RTT.
3. La entidad TCP par podría no confirmar inmediatamente cada segmento debido a su propio retardo de procesamiento o debido a que ejerce su privilegio de utilizar confirmaciones acumulativas.

La especificación original de TCP intenta dar cuenta de esta variabilidad multiplicando la estimación de RTT por un factor constante, como se muestra en la Ecuación (17.4). En un entorno estable, con una varianza baja de RTT, esta formulación resulta en un valor alto de RTT innecesario, y en un entorno inestable un valor de $\beta = 2$ podría ser inadecuado para proteger contra retransmisiones innecesarias.

Una propuesta más efectiva es estimar la variabilidad en los valores de RTT y utilizar esto como entrada en el cálculo de una RTO. Una medida de variabilidad que es fácil estimar es la desviación media, definida como

$$\text{MDEV}(X) = \text{E}[|X - \text{E}[X]|]$$

donde E[X] es el valor esperado de X.

Como se hizo con la estimación de RTT, se puede utilizar un promediado simple para estimar MDEV:

$$\begin{aligned}
\text{AERR}(K+1) &= \text{RTT}(K+1) - \text{ARTT}(K) \\
\text{ADEV}(K+1) &= \frac{1}{K+1}\sum_{i=1}^{K+1} |\text{AERR}(i)| \\
&= \frac{K}{K+1}\,\text{ADEV}(K) + \frac{1}{K+1}\,|\text{AERR}(K+1)|
\end{aligned}$$

donde ARTT(K) es la media simple definida en la Ecuación (17.1) y AERR(K) es la desviación media simple medida en el instante K.

Como con la definición de ARRT, cada término en la sumatoria de ADEV tiene el mismo peso; esto es, cada término se multiplica por la misma constante $1/(K+1)$. De nuevo, queremos dar un peso mayor a las medidas más recientes ya que es más probable que ellos reflejen el comportamiento futuro. Jacobson, que propuso la utilización de una estimación dinámica de la variabilidad en la estimación de RTT [JACO88], sugiere utilizar la misma técnica de suavizado exponencial como se hace en el cálculo de SRTT. El algoritmo completo propuesto por Jacobson se puede expresar como sigue:

$$\begin{aligned}
\text{SRTT}(K+1) &= (1-g) \times \text{SRTT}(K) + g \times \text{RTT}(K+1) \\
\text{SERR}(K+1) &= \text{RTT}(K+1) - \text{SRTT}(K) \\
\text{SDEV}(K+1) &= (1-h) \times \text{SDEV}(K) + h \times |\text{SERR}(K+1)| \\
\text{RTO}(K+1) &= \text{SRTT}(K+1) + f \times \text{SDEV}(K+1)
\end{aligned} \tag{17.5}$$

Como en la definición del RFC 793 [Ecuación (17.3)], SRTT es una estimación exponencial suavizada de RTT, con $(1-g)$ equivalente a α. Ahora, sin embargo, en lugar de multiplicar la estimación

SRTT por una constante [Ecuación (17.4)], se suma a SRTT un múltiplo de la desviación media estimada para formar el temporizador de retransmisión. Basándose en sus experimentos de temporización, Jacobson propone en su artículo original los siguientes valores para las constantes:

$$g = 1/8 = 0{,}125$$
$$h = 1/4 = 0{,}25$$
$$f = 2$$

Después de investigaciones posteriores [JACO90], recomendó cambiar el valor de f a 4, y éste es el valor estándar utilizado en la implementación actual.

La Figura 17.13 muestra el uso de la Ecuación (17.5) en el mismo conjunto de datos que se utilizó en la Figura 17.12. Una vez que el tiempo de llegada se estabiliza, la estimación de la variación SDEV declina. El valor de RTO para ambos casos $f = 2$ y $f = 4$ es bastante conservador mientras RTT está cambiando, pero comienza a converger a RTT cuando se estabiliza.

La experiencia ha demostrado que el algoritmo de Jacobson puede mejorar significativamente el rendimiento de TCP. Sin embargo, no se basta por sí mismo. Se deben considerar otros dos factores:

1. ¿Qué valor de RTO se debería utilizar en un segmento retransmitido? Para este propósito se utiliza el algoritmo de decaimiento exponencial de RTO.
2. ¿Qué muestras se deberían utilizar como entrada al algoritmo de Jacobson? El algoritmo de Karn determina qué muestras se utilizan.

Decaimiento exponencial de RTO

Cuando expira un temporizador en el emisor TCP, debe retransmitir ese segmento. El RFC 793 supone que se va a utilizar el mismo RTO para este segmento retransmitido. Sin embargo, ya que el que expire un temporizador se debe probablemente a la congestión de red, manifestada en el descarte del paquete o en un retardo grande en el tiempo de ida y vuelta, no es aconsejable mantener el mismo valor de RTO.

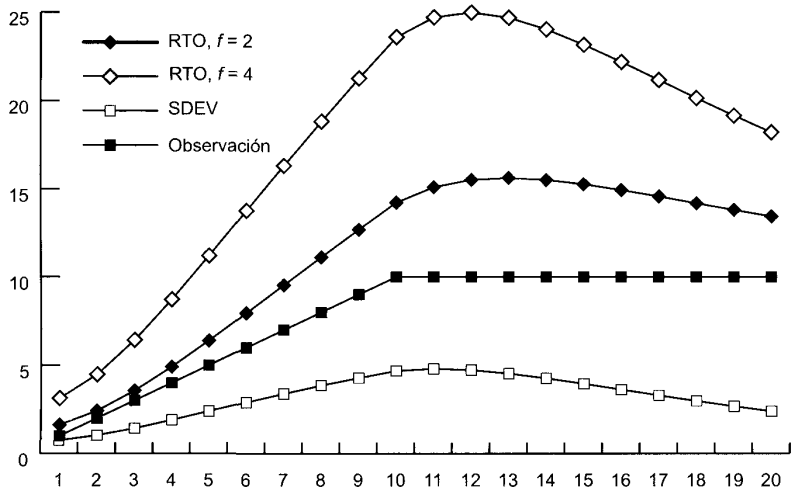
Considere el siguiente escenario. Existen varias conexiones TCP activas de varias fuentes enviando tráfico a un conjunto de redes. Aparece la congestión en una región de forma que los segmentos en muchas de las conexiones se pierden o retrasan más allá del tiempo RTO de las conexiones. Por lo tanto, casi al mismo tiempo, muchos segmentos serán retransmitidos hacia el conjunto de redes, manteniendo o incluso incrementando la congestión. Todas las fuentes esperan un tiempo RTO local (para cada conexión) y retransmiten de nuevo. Este modelo de comportamiento podría causar una condición de congestión continua.

Un criterio más sensible dicta que la fuente TCP incremente su RTO cada vez que se retransmite un segmento; esto se conoce como proceso de *decaimiento*. En el escenario de párrafo anterior, después de la primera retransmisión de un segmento en cada conexión afectada las fuentes TCP esperarán un tiempo mayor antes de intentar la segunda retransmisión. Esto le da tiempo al conjunto de redes a despejar la congestión actual. Si se necesita una segunda retransmisión, cada fuente TCP esperará un tiempo mayor todavía antes de que expire el temporizador para una tercera retransmisión, dando al conjunto un periodo mayor todavía para recuperarse.

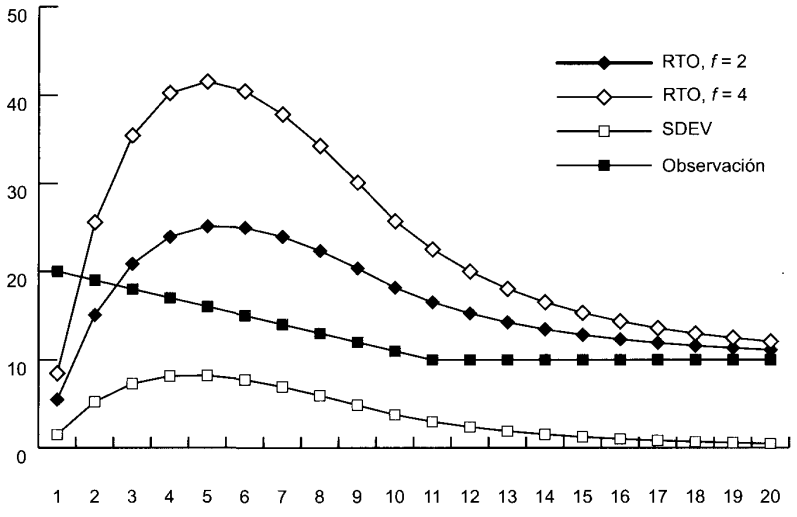
Una técnica simple para implementar el decaimiento de RTO es multiplicar el RTO de un segmento por una valor constante para cara retransmisión:

$$\text{RTO} = q \times \text{RTO} \tag{17.6}$$

La Ecuación (17.6) hace que el RTO crezca exponencialmente con cada retransmisión. El valor de q más utilizado comúnmente es 2. Con este valor, la técnica se conoce como *decaimiento exponencial binario*. Ésta es la misma técnica que se utiliza en el protocolo CSMA/CD de Ethernet (Capítulo 14).



(a) Función creciente



(b) Función decreciente

Figura 17.13. Cálculo del RTO de Jacobson.

Algoritmo de Karn

Si no se retransmiten segmentos, el proceso de muestreo del algoritmo de Jacobson es directo. El RTT de cada segmento se puede incluir en los cálculos. Suponga, sin embargo, que expira el temporizador de un segmento y se debe retransmitir. Si se recibe una confirmación, existen dos posibilidades:

1. Ésta es el ACK de la primera transmisión del segmento. En este caso, el RTT es simplemente mayor que el esperado pero es un reflejo preciso de las condiciones de la red.

2. Ésta es el ACK de la segunda transmisión.

La fuente TCP no puede distinguir entre estos dos casos. Si es verdadero el segundo caso y la entidad TCP mide simplemente el RTT desde la primera transmisión hasta la recepción del ACK, el tiempo medido será demasiado grande. El RTT medido será del orden del RTT actual más el RTO. Pasando este falso RTT al algoritmo de Jacobson producirán un valor alto innecesario de SRTT y por lo tanto de RTO. Además, este efecto se propaga hacia adelante un determinado número de iteraciones, ya que el valor de SRTT de una iteración es el valor de entrada en la siguiente iteración.

Un criterio incluso peor sería medir el RTT desde la segunda transmisión hasta la recepción del ACK. Si éste es en realidad el ACK de la primera transmisión, entonces el RTT medido sería demasiado pequeño, produciendo un valor demasiado pequeño de SRTT y RTO. Esto probablemente tenga un efecto de realimentación positiva, causando retransmisiones adicionales y medidas falsas adicionales.

El algoritmo de Karn [KARN91] resuelve este problema con las reglas siguientes:

1. No utilizar el RTT medido en una retransmisión para actualizar SRTT y SDEV [Ecuación (17.5)].
2. Calcular el RTO de decaimiento utilizando la Ecuación (17.6) cuando ocurra una retransmisión.
3. Utilizar el valor del RTO de decaimiento para sucesivos segmentos hasta que llegue una confirmación para un segmento que no se ha retransmitido.

Cuando se recibe una confirmación para un segmento que no se ha retransmitido, se activa de nuevo el algoritmo de Jacobson para calcular valores futuros de RTO.

GESTIÓN DE LA VENTANA

Además de las técnicas para mejorar la efectividad del temporizador de retransmisión, se han examinado una serie de criterios para gestionar la ventana de emisión. El tamaño de la ventana de emisión de TCP puede tener un efecto crítico en si TCP puede ser utilizado eficientemente sin causar congestión. Se discuten dos técnicas que se encuentran en virtualmente todas las implementaciones recientes de TCP: el comienzo lento y el ajuste dinámico de la ventana en caso de congestión.

Comienzo lento

Cuanto mayor es la ventana de emisión, más segmentos puede enviar la fuente TCP antes de que deba esperar una confirmación. Esto puede crear un problema cuando se establece por primera vez una conexión TCP, ya que la entidad TCP es libre de vaciar la ventana de datos completa en el conjunto de redes.

Una estrategia que se podría seguir es que el emisor TCP empiece a enviar con una ventana relativamente grande pero no a su máximo valor, esperando que se aproxime finalmente al tamaño que sería proporcionado por la conexión. Esto sin embargo es arriesgado ya que el emisor podría inundar el conjunto de redes con muchos segmentos antes de darse cuenta a partir de los temporizadores que el flujo era excesivo. En lugar de eso, se necesita algún medio para expandir gradualmente la ventana hasta que se reciba una confirmación.

Jacobson [JACO88] recomienda un procedimiento llamado comienzo lento. TCP hace uso de una ventana de congestión, medida en segmentos en lugar de octetos. En cualquier instante de tiempo, la transmisión TCP está condicionada por la siguiente regla:

$$awnd = \text{MIN}[crédito, cwnd] \tag{17.7}$$

donde

awnd = ventana permitida en segmentos. Éste es el número de segmentos que TCP tiene permitido enviar sin recibir confirmaciones adicionales.

cwnd = ventana de congestión, en segmentos. Ventana utilizada por TCP durante el proceso de aumentar el flujo y para reducir el flujo durante los periodos de congestión.
crédito = la cantidad de créditos concedidos y no utilizados en la confirmación más reciente, en segmentos. Cuando se recibe una confirmación, este valor se calcula como *ventana/tamaño-de-segmento*, donde *ventana* es el campo ventana del segmento TCP recibido (la cantidad de datos que la entidad TCP par está dispuesta a aceptar).

Cuando se abre una conexión, la entidad TCP inicializa *cwnd* = 1. Esto es, a TCP sólo se le permite enviar un segmento y después debe esperar una confirmación antes de enviar un segundo segmento. Cada vez que recibe una confirmación, se incrementa el valor de *cwnd* en una unidad, hasta algún valor máximo.

En realidad, el mecanismo de comienzo lento chequea el conjunto de redes para asegurarse de que no está enviado demasiados segmentos en un ambiente ya congestionado. Conforme van llegando las confirmaciones, a TCP se le permite abrir su ventana hasta que el flujo se controla por las confirmaciones entrantes en lugar de por *cwnd*.

El término *comienzo lento* es un nombre poco apropiado, ya que *cwnd* crece en realidad exponencialmente. Cuando llega la primera ACK, TCP abre *cwnd* hasta 2 y puede enviar dos segmentos. Cuando estos dos segmentos se confirman, TCP puede desplazar la ventana 1 segmento por cada ACK que llega e incrementar *cwnd* en uno por cada ACK. Por lo tanto, en este punto TCP puede enviar cuatro segmentos. Cuando se confirmen estos cuatro segmentos, TCP podrá enviar ocho segmentos.

Ajuste dinámico de la ventana en caso de congestión

Se ha encontrado que el algoritmo de comienzo lento funciona de una forma efectiva para inicializar una conexión. Permite a TCP determinar rápidamente un tamaño de ventana razonable para la conexión. ¿No sería útil la misma técnica cuando hay necesidad de atajar la congestión? En particular, suponga que una entidad TCP inicia una conexión y lo hace mediante el procedimiento de comienzo lento. En determinado punto, antes o después de que *cwnd* alcance el tamaño de créditos asignados por la otra parte, se pierde un segmento (expira un temporizador). Esto es una señal de que está ocurriendo congestión. Pero no está claro como de seria es la congestión. Por lo tanto, un procedimiento prudente sería inicializar *cwnd* a 1 y comenzar el procedimiento de comienzo lento de nuevo.

Esto parece un procedimiento razonable y conservativo, pero en realidad no es lo bastante conservativo. Jacobson [JACO88] señala que «es fácil llevar una red a la saturación pero difícil que la red se recupere». En otras palabras, una vez que la congestión ocurre, puede transcurrir un tiempo bastante grande hasta que ésta desaparezca[1]. Así, de esta forma el crecimiento exponencial de *cwnd* bajo el comienzo lento puede ser demasiado agresivo y empeorar la congestión. En lugar de esto, Jacobson propone el uso del comienzo lento para comenzar la conexión, seguido de un crecimiento lineal de *cwnd*. Las reglas son las siguientes. Cuando expira un temporizador:

1. Establecer un umbral de comienzo lento igual a la mitad de la ventana de congestión actual; esto es, hacer *ssthresh* = *cwnd*/2.
2. Hacer *cwnd* = 1 y ejecutar el procedimiento de comienzo lento hasta que *cwnd* = *ssthresh*. En esta fase, *cwnd* se incrementa 1 por cada ACK recibida.
3. Para *cwnd* $\geqslant$ *sstrersh*, incrementar *cwnd* en uno por cada tiempo de ida-y-vuelta.

La Figura 17.14 muestra este comportamiento. Nótese que le lleva 11 tiempos de ida-y-vuelta recuperar el nivel *cwnd* que inicialmente se consiguió con 4 tiempos de ida-y-vuelta.

---

[1] Kleinrock se refiere a este fenómeno como un efecto de una cola grande en periodos punta. Véase la Sección 2.7 y la 2.10 de [KLEI76] para una discusión detallada.

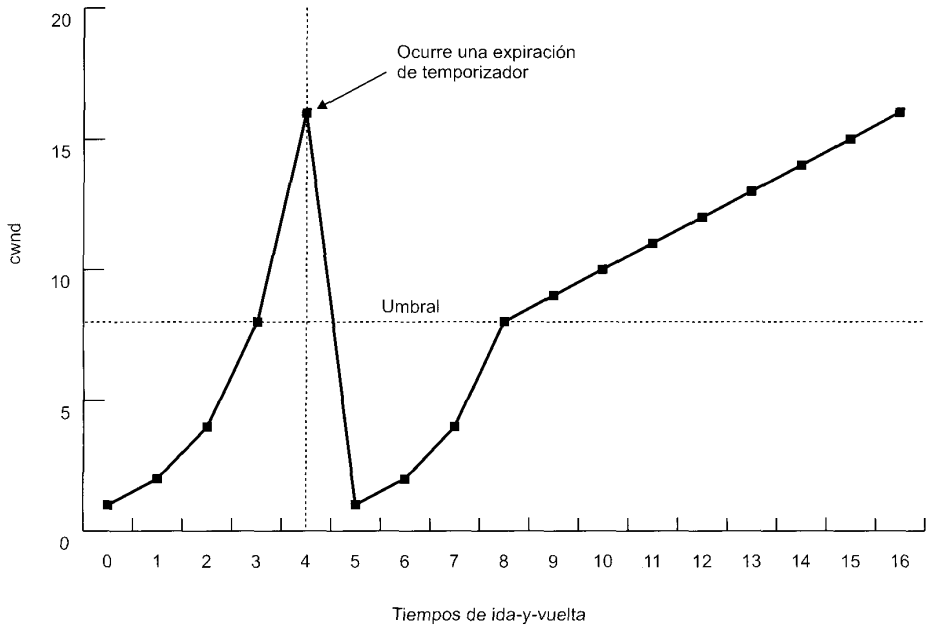


Figura 17.14. Ilustración del comienzo lento y la prevención de la congestión.

17.4. UDP

Además de TCP, existe otro protocolo en la capa de transporte que se usa comúnmente como parte del conjunto de protocolos TCP/IP: el protocolo de datagrama de usuario (UDP, User Datagram Protocol), especificado en el RFC 768. UDP proporciona un servicio no orientado a conexión para los procedimientos de la capa de aplicación. Así, UDP es básicamente un servicio no seguro; la entrega y la protección contra duplicados no están garantizadas. En contrapartida se reduce la información suplementaria del protocolo lo que puede ser adecuado en muchos casos. Como ejemplo de uso de UDP se tiene el contexto de gestión de red, como se describe en el Capítulo 19.

La potencia del enfoque orientado a conexión es clara. Permite características relacionadas con la conexión como son el control de flujo, control de errores y entrega en secuencia. Sin embargo, un servicio no orientado a conexión es más apropiado en algunos contextos. En capas inferiores (interconexión, red) son más robustos (por ejemplo, ver la discusión de la Sección 10.1). Además, representa el «menor denominador común» del servicio que esperan las capas superiores. Pero, incluso a nivel de transporte y superiores existe una justificación para un servicio no orientado a conexión. Existen casos en los que la información suplementaria del establecimiento y mantenimiento de la conexión no están justificados o son contraproducentes. Algunos ejemplos de esto mismo son los siguientes:

- **Recolección de datos de entrada:** supone una actividad periódica o muestreo de datos pasivo, tales como los procedentes de sensores, de informes de auto-test automáticos de equipos de red o de componentes de la red. En una situación de monitorización en tiempo real, la pérdida ocasional de una unidad de datos no causaría ningún desastre ya que la siguiente muestra debería llegar en breves momentos.
- **Diseminar datos de salida:** incluye la difusión de mensajes a los usuarios de la red, el anuncio de un nuevo nodo o el cambio de la dirección de un servicio, y la distribución de los valores de reloj en tiempo real.

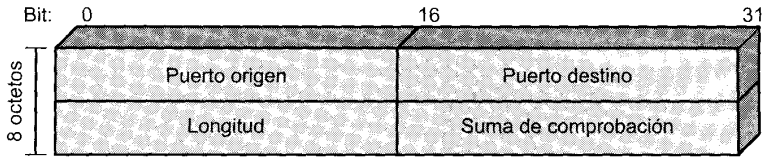


Figura 17.15. Cabecera UDP.

- **Petición-respuesta:** aplicaciones en las que un servidor común proporciona un servicio de transacción a un número de usuarios distribuidos y para lo cual es típico usar una secuencia del tipo petición/respuesta. El uso del servicio se regula en la capa de aplicación y las conexiones a las capas son innecesarias y molestas.
- **Aplicaciones en tiempo real:** tales como voz y telemedida, que llevan consigo el requisito de utilizar redundancias y transmisión en tiempo real. Estos requisitos no pueden tener funciones orientadas a conexión tal como es la retransmisión.

Así, tiene sentido que en la capa de transporte tengan cabida tanto servicios orientados a conexión como servicios no orientados a conexión.

UDP se sitúa encima de IP. Ya que es no orientado a conexión, UDP tiene pocas funciones que hacer. Esencialmente, incorpora un direccionamiento a puerto a las capacidades de IP. Esto se ve mejor examinando la cabecera UDP mostrada en la Figura 17.15. La cabecera incluye un puerto origen y un puerto destino. El campo de longitud contiene la longitud del segmento UDP entero, incluyendo la cabecera y los datos. La suma de verificación es el mismo algoritmo usado para TCP e IP. Para UDP, la suma de verificación se aplica al segmento UDP entero más una seudo-cabecera incorporada a la cabecera UDP cuando se calcula la suma y es la misma que la usada para TCP. Si se detecta un error, el segmento se descarta sin tomar ninguna medida adicional.

El campo de suma de verificación en UDP es opcional. Si no se utiliza, éste se pone todo a cero. Sin embargo, hay que indicar que la suma de verificación de IP se aplica sólo a la cabecera IP y no al campo de datos, que está compuesto, en este caso, de la cabecera UDP y los datos de usuario. Así, si UDP no implementa ningún cálculo de suma de verificación, los datos de usuario no se comprueban.

17.5. LECTURAS RECOMENDADAS

Quizás el mejor tratamiento de las varias estrategias de TCP para el control de flujo y de la congestión se encuentre en [STEV94]. Un artículo fundamental para entender las cuestiones implicadas es el clásico [JACO88].

JACO88 Jacobson, V. «Congestion Avoidance and Control.» *Proceedings, SIGCOMM'88, Computer Communication Review*, August 1988; reprinted in *Computer Communication Review*, January 1995; a slightly revised version is available at ftp.ee.lbl.gov/papers/congavoid.ps.Z.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols.* Reading, MA: Addison-Wesley, 1994.

17.6. PROBLEMAS

17.1. Es una práctica común en la mayoría de los protocolos de transporte (en realidad, en la mayoría de los protocolos en todas las capas) que los datos y las señales de control se multiplexen sobre

el mismo canal lógico en cada conexión por usuario. Una alternativa es establecer una única conexión de transporte de control entre cada par de entidades de transporte que se comunican. Esta conexión se usaría para transmitir las señales de control de todas las conexiones de los usuarios de transporte entre las dos entidades. Discutir las implicaciones de esta estrategia.

17.2. La discusión sobre control de flujo con un servicio de red seguro, referido como mecanismo de presión hacia atrás (*backpressure*), utiliza un protocolo de control de flujo de una capa inferior. Discutir las desventajas de esta estrategia.

17.3. Dos entidades de transporte se comunican a través de una red segura. Supongamos que el tiempo normalizado para transmitir un segmento es igual a 1. Suponer que el retardo de propagación extremo-a-extremo es 3 y que la entrega de un segmento recibido al usuario de transporte requiere un tiempo de 2. El emisor tiene inicialmente concedido un crédito de siete segmentos. El receptor utiliza un criterio de control de flujo conservativo y actualiza su asignación de créditos a cada oportunidad. ¿Cuál es el máximo rendimiento alcanzable?

17.4. Dibuje un diagrama similar al de la Figura 17.5 para las siguientes condiciones (suponer un servicio de red seguro y con secuenciamiento):

a) Cierre de la conexión: activo/pasivo.

b) Cierre de la conexión: activo/activo.

c) Rechazo de conexión.

d) Proceso de cancelar una conexión: un usuario emite un OPEN a un usuario que está escuchando y entonces emite un CLOSE antes de que se intercambie algún dato.

17.5. Con un servicio de red seguro y con secuenciamiento, ¿son estrictamente necesarios los números de secuencia de los segmentos? ¿Qué capacidad, si hay alguna, se pierde sin ellos?

17.6. Considere un servicio de red orientado a conexión que sufre un reinicio. ¿Cómo podría ser tratado por un protocolo de transporte que supone que el servicio de red es seguro excepto en el caso de un reinicio?

17.7. La discusión del criterio de retransmisión hizo referencia a tres problemas asociados con el cálculo dinámico del valor del temporizador. ¿Qué modificaciones del criterio ayudarían para aliviar estos problemas?

17.8. Considere un protocolo de transporte que usa un servicio de red orientado a conexión. Suponga que ese protocolo de transporte utiliza un esquema de asignación de créditos para el control de flujo y que el protocolo de red usa un esquema de ventana deslizante. ¿Qué relación, si existe, debería haber entre la ventana dinámica del protocolo de transporte y la ventana fija del protocolo de red?

17.9. En una red que tiene un tamaño máximo de paquete de red de 128 bytes, un tiempo de vida máximo de 30 s y un número de secuencia de paquetes de 8 bits, ¿cuál es la máxima tasa de transmisión de datos por conexión?

17.10. ¿Es posible un interbloqueo utilizando un diálogo en dos sentidos en lugar de un diálogo en tres sentidos? Dé un ejemplo o demuéstrelo.

17.11. Debajo se enumeran cuatro estrategias que se pueden utilizar para proporcionar a un usuario de transporte las direcciones de un usuario de transporte destino. Para cada una, describa una analogía con un usuario del servicio de correos.

a) Conocer la dirección de antemano.

b) Hacer uso de una dirección «bien-conocida».

c) Utilizar un servidor de nombres.

d) Las direcciones se generan cuando se realiza la petición.

17.12. En un esquema de créditos para control de flujo, ¿qué provisión de créditos se puede hacer para la asignación de créditos que se pierdan o se desordenen durante la transmisión?

17.13. ¿Qué ocurre en la Figura 17.4 si llega un SYN mientras el usuario solicitado está en el estado CERRADO? ¿Hay alguna forma de llamar la atención del usuario cuando éste no está escuchando?

17.14. Normalmente, el campo ventana en la cabecera TCP da una asignación de créditos en octetos. Cuando se utiliza la opción de Escalado de Ventana, el valor del campo Ventana se multiplica por 2^F, donde F es el calor de la opción de escalado de ventana. El valor máximo de F que acepta TCP es 14. ¿Por qué se limita esta opción a 14?

17.15. Una dificultad con la estimación original de SRTT de TCP es la elección de un valor inicial. En ausencia de un conocimiento especial de las condiciones de la red la opción típica es elegir un valor arbitrario, tal como 3 segundos, y esperar que esto converja rápidamente a un valor preciso. Si la estimación es demasiado pequeña, TCP llevará a cabo retransmisiones innecesarias. Si es demasiado grande, TCP esperará un periodo grande de tiempo antes de retransmitir si el primer segmento se perdió. También, la convergencia puede ser lenta, como indica este problema.

a) Elegir $\alpha = 0{,}85$ y SRTT(0) = 3 segundos y suponer que todos lo valores medidos son iguales a 1 segundo y que no se pierden paquetes. ¿Cuál es el valor de SRTT(9)? *Sugerencia*: la Ecuación 17.3 se puede reescribir para simplificar los cálculos, utilizando la expresión $(1 - \alpha^n)/(1 - \alpha)$.

b) Sea ahora SRTT(0) = 1 segundo y suponga que los valores medidos de RTT son 3 segundos y que no se pierden paquetes. ¿Cuál es el valor de SRTT(19)?

17.16. Una implementación pobre del esquema de ventana deslizante de TCP puede llevar a un rendimiento extremadamente pobre. Existe un fenómeno conocido como «síndrome de la ventana absurda» (SWS, Silly Window Syndrome), que puede fácilmente causar una degradación en el rendimiento en varias decenas. Como ejemplo de SWS, considere una aplicación que está ocupada en la transferencia de un fichero largo y que TCP está transfiriendo el fichero en segmentos de 200 octetos. El receptor inicialmente asigna un crédito de 1.000. El emisor agota esta ventana con 5 segmentos de 200 octetos. Ahora suponga que el receptor devuelve una confirmación por cada segmento y proporciona un crédito adicional de 200 octetos por cada segmento recibido. Desde el punto de vista del receptor, esto de nuevo expande la ventana hasta 1.000 octetos. Sin embargo, desde el punto de vista del emisor, si la primera confirmación llega después de que se han enviado 5 segmentos solamente hay disponible una venta de 200 octetos solamente. Suponga que en el mismo punto, el receptor calcula una ventana de 200 octetos pero sólo tiene 50 octetos para enviar cuando alcanza un punto de «carga». Por lo tanto, él envía 50 octetos en un segmento, seguido de 150 octetos en el siguiente segmento y reanuda la transmisión de segmentos de 200 octetos. ¿Qué podría ahora ocurrir que de lugar a un problema en el rendimiento? Plantee el SWS en términos más generales.

17.17. TCP impone que tanto el receptor como el emisor incorporen mecanismos para tratar el SWS.

a) Sugiera una estrategia para el receptor. *Sugerencia*: suponga que el receptor «miente» sobre la capacidad de memoria temporal de que se dispone bajo ciertas circunstancias. Plantee una regla razonable grosso modo para esto.

b) Sugiera una estrategia para el emisor. *Sugerencia*: considere la relación entre la ventana máxima posible de envío y lo que hay disponible para enviar.

17.18. En la Ecuación (17.5), reescriba la definición de SRTT(K + 1) para que sea función de SERR(K + 1). Interprete el resultado.

17.19. Una entidad TCP abre una conexión y utiliza un comienzo lento. Aproximadamente, ¿cuántos tiempos de ida y vuelta se necesitan antes que TCP pueda enviar N segmentos?

17.20. Aunque el comienzo lento con la prevención de congestión es una técnica efectiva para tratar la congestión, puede resultar en tiempos de recuperación grandes en redes de capacidad alta, como demuestra este problema:

a) Suponga un retardo de ida y vuelta de 60 ms (lo que podría ocurrir a través de un continente) y un enlace con un ancho de banda disponible de 1 Gbps y un tamaño de segmento de 576 octetos. Determine el tamaño de ventana necesario para mantener lleno el cauce y el tiempo que tardaría en alcanzar el tamaño de ventana después de una expiración utilizando el criterio de Jacobson.

b) Repita (a) para un tamaño de venta de 16 Kbytes.

17.21. ¿Por qué es necesario UDP? ¿Por qué no puede un programa de usuario acceder directamente a IP?

CAPÍTULO 18

Seguridad en redes

- Las amenazas a la seguridad de red se dividen en dos categorías: **amenazas pasivas**, llamadas a vece escuchas, y que suponen el intento de un atacante de obtener información relativa a una comunica ción; y **amenazas activas** que suponen alguna modificación de los datos transmitidos o la creación transmisiones falsas.
- Hasta ahora la herramienta automática más importante para la seguridad en red y de la comunicació es el **cifrado**. Con el cifrado convencional, dos partes comparten una clave de cifrado/descifrado. E principal reto del cifrado convencional es la distribución y la protección de las claves. Un esquema de cifrado de clave pública implica dos claves, una para el cifrado y la otra para el descifrado. Una de las claves es privada de la parte que genera el par de claves y la otra se hace pública.
- El cifrado convencional y el cifrado de clave pública se suelen combinar en aplicaciones de red seguras. El cifrado convencional se utiliza para cifrar los datos transmitidos, con una clave utilizada una sola una vez o clave de sesión temporal. La clave de sesión la puede distribuir un centro de distribución de claves de confianza o ser transmitida cifrada utilizando un cifrado de clave pública. El cifrado de clave pública también se utiliza para crear firmas digitales, que pueden autentificar la fuente de los mensajes transmitidos.
- Una mejora en la seguridad utilizada con IPv4 e IPv6, llamada IPSec, proporciona mecanismos de confidencialidad y autentificación.

Los requisitos en la **seguridad de la información** dentro de un organismo han sufrido principalmente dos cambios en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información, que era de valor para una institución se conseguía fundamentalmente por medios físicos y administrativos. Como ejemplo del primer medio es el uso de cajas fuertes con combinación de apertura para almacenar documentos confidenciales. Un ejemplo del segundo es el uso de procedimientos de investigación de personal durante la fase de contratación.

Con la introducción de los computadores, fue evidente la necesidad de herramientas automáticas para proteger ficheros y otra información almacenada en los computadores. Éste es especialmente el caso de los sistemas multiusuario, como con los sistemas de tiempo compartido, y la necesidad es más aguda para sistemas a los que se puede acceder desde teléfonos públicos o redes de datos. El término genérico del campo que trata las herramientas diseñadas para proteger los datos y frustrar a los piratas informáticos es **seguridad en computadores.** Aunque éste es un tópico muy importante, está fuera del ámbito de este libro y será tratado muy brevemente.

El segundo cambio relevante, que ha afectado a la seguridad, es la introducción de sistemas distribuidos y la utilización de redes y facilidades de comunicación para transportar datos entre terminales de usuario y computadores, y de computador a computador. Las medidas de **seguridad en red** son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos.

Virtualmente la tecnología esencial subyacente en todas las redes automáticas y las aplicaciones de seguridad en computadores es el cifrado. Existen dos técnicas fundamentales en uso: cifrado convencional, también conocido como cifrado simétrico, y el cifrado con clave pública, también conocido como cifrado asimétrico. Conforme examinemos las diversas técnicas de seguridad en red, se explorarán los dos tipos de cifrado.

Este capítulo comienza con una visón global de los requisitos de seguridad en red. A continuación, se examinará el cifrado convencional y su utilización para proporcionar privacidad. A esto le sigue una

discusión sobre autentificación de mensajes. Se examina el uso del cifrado de clave pública y las firmas digitales. El capítulo termina con un examen de las características de seguridad en IPv4 e IPv6.

18.1. REQUISITOS Y AMENAZAS A LA SEGURIDAD

Para ser capaz de entender los tipos de amenazas a la seguridad que existen, conviene definir los requisitos en seguridad. La seguridad en computadores y en redes implica tres requisitos:

- **Secreto:** requiere que la información en un computador sea accesible para lectura sólo por los entes autorizados. Este tipo de acceso incluye la impresión, mostrar en pantalla y otros formas de revelación que incluye cualquier forma de dar a conocer la existencia de un objeto.
- **Integridad:** requiere que los recursos de un computador sean modificados solamente por entes autorizados. La modificación incluye escribir, cambiar, cambiar de estado, suprimir y crear.
- **Disponibilidad:** requiere que los recursos de un computador estén disponibles a los entes autorizados.

Una clasificación útil de las agresiones a la seguridad en red se hace en términos de agresiones pasivas y agresiones activas (Figura 18.1).

ATAQUES PASIVOS

Las agresiones pasivas son del tipo de las escuchas, o monitorizaciones, de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones: divulgación del contenido de un mensaje y análisis del tráfico.

La **divulgación del contenido de un mensaje** se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico, un fichero transferido puede contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.

El segundo tipo de agresión pasiva, el **análisis del tráfico**, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se está realizando.

Los ataques pasivos son muy difíciles de detectar ya que no implican la alteración de los datos. Sin embargo, es factible prevenir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones está en la prevención antes que la detección.

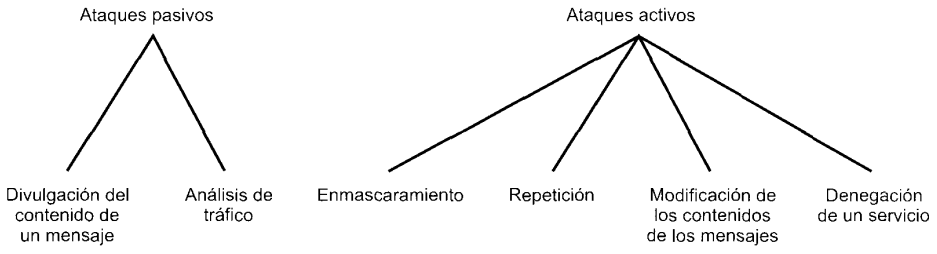


Figura 18.1. Agresiones a la seguridad de red activas y pasivas.

ATAQUES ACTIVOS

Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos y subdividen en 4 categorías: enmascaramiento, repetición, modificación de mensajes y denegación de servicio.

Un **enmascaramiento** tiene lugar cuando una entidad pretende ser otra entidad diferente. Una a sión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La **repetición** supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

La **modificación de mensajes** significa sencillamente que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje con un significado «Permitir a John Smith leer el fichero confidencial de cuentas» se modifica para tener el significado «Permitir a Fred Brown leer el fichero confidencial de cuentas».

La **denegación de un servicio** previene o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular (por ejemplo, al servicio de vigilancia de seguridad). Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es bastante difícil prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. Por consiguiente, la meta es detectarlas y recuperarse de cualquier perturbación o retardo causados por ellas. Ya que la detección tiene un efecto disuasivo, también puede contribuir a la prevención.

18.2. PRIVACIDAD CON CIFRADO CONVENCIONAL

La técnica universal para proporcionar privacidad en los datos transmitidos es el cifrado convencional. Esta sección examina primero los conceptos básicos del cifrado convencional, y sigue con una discusión de las dos técnicas de cifrado convencional más populares: DES y DES triple. Después se examinarán las aplicaciones de estas técnicas para alcanzar la privacidad.

CIFRADO CONVENCIONAL

El cifrado convencional, también llamado cifrado simétrico o de clave única, era el único tipo de cifrado en uso antes de la introducción del cifrado de clave pública a finales de la década de los 70. El cifrado convencional ha sido utilizado para las comunicaciones secretas por incontables individuos y grupos, desde Julio César hasta la fuerza alemana de los U-boat y actualmente los diplomáticos, militares y los comerciantes. Es todavía el cifrado más utilizado mundialmente de los dos tipos de cifrado.

Un esquema de cifrado convencional tiene cinco ingredientes (Figura 18.2):

- **Texto nativo («plaintext»):** es el mensaje original o datos que actúan como entrada al algoritmo.
- **Algoritmo de cifrado:** el algoritmo de cifrado lleva a cabo varias substituciones y transformaciones en el texto nativo.
- **Clave secreta:** la clave secreta es también una entrada al algoritmo de cifrado. Las substituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.

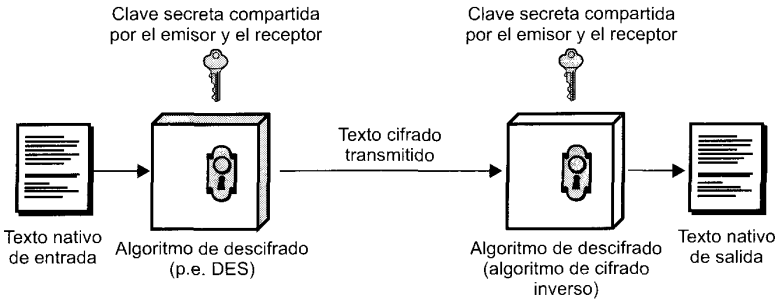


Figura 18.2. Modelo simplificado del cifrado convencional.

- **Texto cifrado:** es el mensaje aleatorio que se produce en la salida. Depende del texto nativo y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- **Algoritmo de descifrado:** es esencialmente el algoritmo de cifrado ejecutado al revés. Toma como entradas el texto cifrado y la clave secreta y produce el texto nativo original.

Existen dos requisitos para la utilización segura del cifrado convencional:

1. Se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear un algoritmo tal que si el oponente conoce el algoritmo y tiene acceso a más de un texto cifrado, sea incapaz de descifrar el texto o adivinar la clave. Este requisito se puede enunciar de una forma más estricta: el oponente debería ser incapaz de descifrar el texto o descubrir la clave incluso si él o ella posee un determinado número de texto cifrados junto a los textos nativos que producen cada texto cifrado.
2. El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y conoce el algoritmo, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Existen dos enfoque generales para atacar el esquema de cifrado convencional. El primer ataque se conoce como **criptoanálisis**. El ataque de criptoanálisis se basa en la naturaleza del algoritmo más quizás algún conocimiento de las características generales del texto nativo o incluso de algunos pares texto nativo-texto cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo específico o deducir la clave que se está utilizando. Si el ataque tiene éxito en deducir la clave, el efecto es catastrófico: todos los mensajes cifrados antiguos y futuros con esa clave están comprometidos.

El segundo método, conocido como ataque de **fuerza bruta**, es intentar cada clave posible en un trozo de texto cifrado hasta que se obtenga una traducción inteligible del texto nativo. La Tabla 18.1 muestra cuánto tiempo se necesita para el caso de varios tamaños de clave. La tabla muestra los resultados para cada tamaño de clave, suponiendo que se tarda 1 μs. en llevar a cabo un único descifrado, que es un orden de magnitud razonable para los computadores de hoy en día. Con el uso de una arquitectura paralela masiva de microcomputadores, sería posible alcanzar velocidades de procesamiento

Tabla 18.1. Tiempo promedio necesario para una búsqueda de clave exhaustiva

Tamaño de la clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrados/μs
32	$2^{32} = 4{,}3 \times 10^9$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ años	$5{,}4 \times 10^{18}$ años
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ años	$5{,}9 \times 10^{30}$ años

de varias órdenes de magnitud superiores. La última columna de la tabla considera los resultados de un sistema que pudiera procesar 1 millón de claves por microsegundo. Como se puede ver, a este nivel de rendimiento, ya no se puede considerar computacionalmente segura una clave de 56 bits.

ALGORITMOS DE CIFRADO

Los algoritmos de cifrado usados más comúnmente son los cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo, y produce un bloque de texto cifrado de igual tamaño para cada bloque de texto nativo. Los dos algoritmos convencionales más importantes, cifradores de bloque, son el DES y el TDEA.

El estándar de cifrado de datos (DES, Data Encryption Standard)

El esquema de cifrado más utilizado mundialmente se define en el estándar de cifrado de datos (DES) adoptado en 1977 por el Buró Nacional de Estándares, ahora el Instituto Nacional de Estándares y Tec-

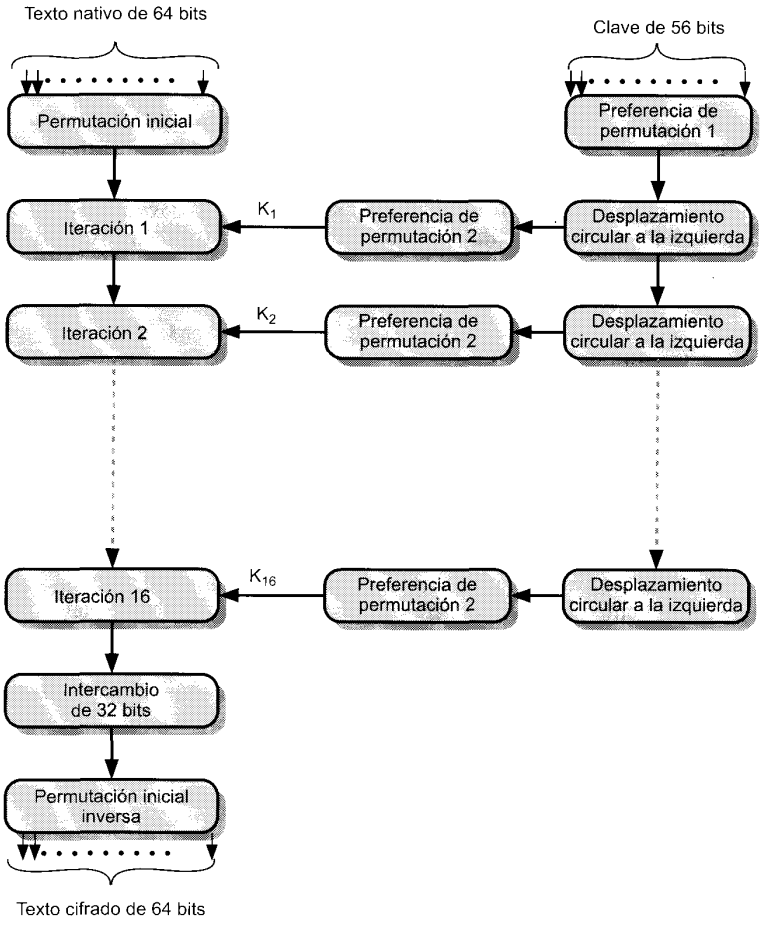


Figura 18.3. Esquema general del algoritmo de cifrado DES.

nología (NIST, National Institute of Standars and Technology»), como Estándar Federal de Procesamiento de la Información 46 (FIPS PUB 46). En 1994, el NIST «reafirmó» a DES para su uso federal por otros 5 años en FIPS PUB-46-2. El algoritmo se denomina algoritmo de Cifrado de Datos (DEA, Data Encryption Algorithm).

El esquema global del cifrado DES se muestra en la Figura 18.3. El texto nativo debe tener una longitud de 64 bits y la clave 56 bits; los textos nativos más grandes se procesan en bloques de 64 bits.

El lado izquierdo de la figura muestra que el procesamiento del texto nativo se realiza en tres fases. Primero, los 64 bits del texto nativo se transforman por medio de una permutación inicial (IP) que reordena los bits para producir la entrada permutada. A esto le sigue una fase que consta de 16 iteraciones de la misma función. La salida de la última iteración (la 16) consta de 64 bits que son función del texto nativo y la clave. La mitad izquierda y la derecha se intercambian para producir la salida previa. Finalmente, la salida previa se permuta con IP^{-1}, que es la inversa de la función de permutación inicial, para producir los 64 bits del texto cifrado.

La parte derecha de la Figura 18.3 muestra la forma cómo se usan los 56 bits de la clave. Inicialmente, la clave se transforma por una función de permutación. Después, para cada una de las 16 iteraciones, se produce una subclave (K_i) por medio de un desplazamiento circular y una permutación. La función de permutación es la misma para cada iteración, pero se produce una subclave diferente debido al desplazamiento repetido de los bits de la clave.

La Figura 18.4 muestra con más detalle el algoritmo para una iteración. Los 64 bits permutados de entrada pasan a través de las 16 iteraciones, produciendo un valor de 64 bits intermedios a la conclusión de cada iteración. La mitad izquierda y derecha de cada valor intermedio de 64 bits se tratan como

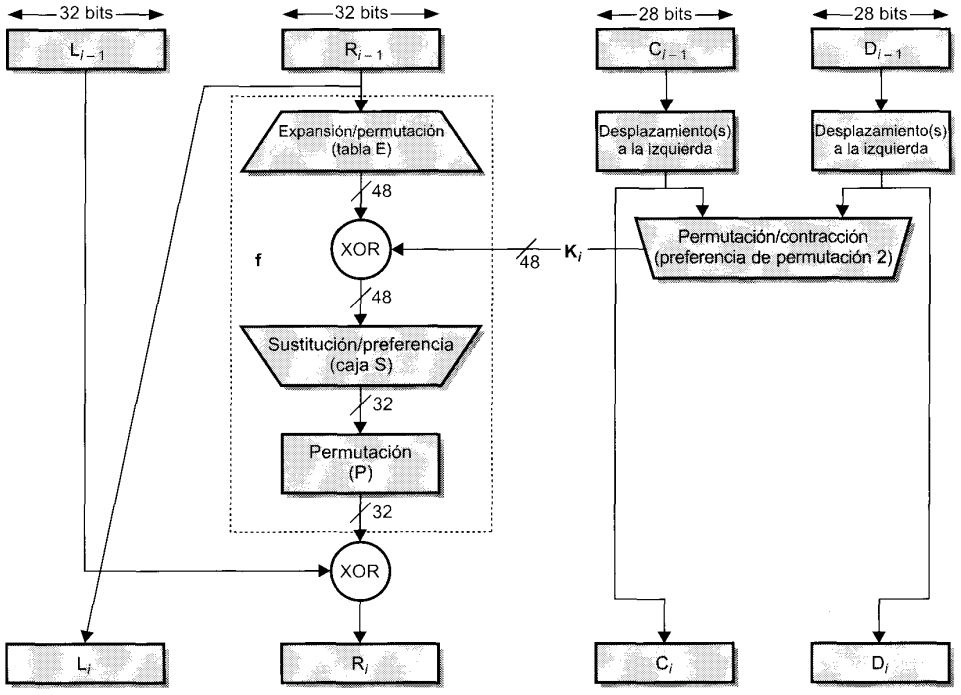


Figura 18.4. Iteración simple del algoritmo DES.

cantidades de 32 bits separadas, rotuladas L (izquierda) y R (derecha). El procesamiento global de cada iteración se puede resumir en las siguientes fórmulas:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus (R_{i-1}, K_i)$$

donde $\oplus$ denota la función XOR bit-a-bit.

Así, la parte izquierda de la salida de una iteración (L_i) es simplemente igual a la parte derecha de la entrada a esa iteración (R_{i-1}). La parte derecha de la salida (R_i) es la función OR-exclusive de (L_{i-1}) y una función compleja de R_{i-1} y K_i. Esta función compleja supone operaciones de permutación y sustitución. La operación de sustitución, representada por tablas llamadas «cajas S», simplemente traduce cada combinación de entrada de 48 bits en un modelo particular de 32 bits.

Volviendo a la Figura 18.3, vemos que la clave de 56 bits usada como entrada al algoritmo, sufre primero una permutación. La clave resultante de 56 bits se trata entonces como dos cantidades de 28 bits, rotuladas como C_0 y D_0. En cada iteración, C y D sufren de forma separada un desplazamiento circular a la izquierda, o rotación, de 1 o 2 bits. Estos valores desplazados sirven como entrada para la siguiente iteración. También se utilizan como entrada a otra función de permutación, que produce una salida de 48 bits que sirve como entrada a la función $f(R_{i-1}, K_i)$.

El proceso de descifrado con DES es esencialmente el mismo que el proceso de cifrado. La regla es como sigue: usar un texto cifrado como entrada al algoritmo DES, pero usar la clave K_i en orden inverso. Esto es, utilizar K_{16} en la primera iteración, K_{15} en la segunda iteración y así hasta que se utilice K_1 en la iteración 16 y última.

La potencia de DES

Ya desde finales de la década de los 70, los expertos advirtieron que los días de DES como algoritmo seguro estaban contados y era sólo cuestión de tiempo el aumento de la velocidad de los procesadores y la caída del coste del hardware que hicieran una cuestión simple romper DES fácilmente. El paciente se declaró muerto en julio de 1998, cuando la Fundación de la Fronteras Electrónicas (EFF, Electronic Frontier Foundation) anunció que había roto el nuevo reto DES utilizando una máquina saboteadora de DES de propósito específico que se construyó por menos de 250.000 dólares. El ataque duró menos de tres días. La EFF ha publicado una descripción detallada de la máquina, permitiendo que otros construyan su propio saboteador [EFF98]. Y, por supuesto, los precios del hardware continuarán cayendo y la velocidad aumentando, haciendo de DES un algoritmo sin ningún valor.

Afortunadamente, existen varias alternativas disponibles en el mercado. A continuación se examina la alternativa más utilizada.

DEA Triple

El DES Triple fue propuesto por primera vez por Tuchman [TUCH79] y fue la primera normalización para aplicaciones comerciales en el estándar ANSI X9.17 de 1985. TDEA se incorporó como una parte del Estándar de Cifrado de Datos en 1999, con la publicación de FIPS PUB46-3.

El TDEA utiliza dos claves y tres ejecuciones del algoritmo DES. La función sigue una secu cifrado-descifrado-cifrado (EDE):

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

donde

C = texto cifrado

P = texto nativo

$E_K[X]$ = cifrado de X utilizando K

$D_K[Y]$ = descifrado de Y utilizando K

La utilización del descifrado en la segunda etapa no tiene significado criptográfico. Su única ventaja es que permite a los usuarios de DES Triple descifrar datos de usuarios del antiguo DES:

$$C = E_{K1}[D_{K2}[E_{K1}[P]]] = E_{K1}[P]$$

Con tres claves distintas, TDEA tiene una longitud de clave efectiva de 168 bits. FIPS 46-3 también permite el uso de dos claves haciendo K1 = K3; esto proporciona una longitud de clave de 112 bits. FIPS 46-3 incluye las siguientes indicaciones para TDEA:

- TDEA es el algoritmo elegido para el cifrado convencional aprobado por FIPS.
- El DEA original, que utiliza una clave única de 56 bits, se permite sólo por el estándar para sistemas que previamente disponían de él. Los nuevos procedimientos deberían permitir TDEA.
- Los organismos gubernamentales con sistemas DEA antiguos se les anima a hacer una transición a TDEA.
- Se anticipa que TDEA y el Estándar de Cifrado Avanzado (AES, Advanced Encryption Standard) coexistirán como algoritmos aprobados por FIPS, permitiendo una transición gradual a AES.

AES es el nuevo estándar de cifrado convencional que está desarrollándose por el Instituto Nacional de Estándares y Tecnología. Se pretende que AES proporcione una seguridad en el cifrado robusta en el futuro próximo. Su característica principal es que utiliza un tamaño de bloque de 128 bits (comparado con los 64 bits de DEA y TDEA) y una longitud de clave de al menos 128 bits. Sin embargo, faltan unos cuantos años antes de que se finalice y antes de que se vea sujeto al criptoanálisis intenso al que se vio sometido DEA. La ventaja de AES es que será probablemente más fácil de implementar y rápido en ejecutarse, en hardware y software, que TDEA.

LOCALIZACIÓN DE LOS DISPOSITIVOS DE CIFRADO

El enfoque más potente y más común en contra de los ataques a la seguridad de red es el cifrado. Si se va a utilizar el cifrado en contra de estas amenazas, entonces necesitamos decidir qué vamos a cifrar y dónde se va a situar la máquina de cifrado. Como muestra la Figura 18.5, hay dos alternativas fundamentales: cifrado de enlace y cifrado extremo-a-extremo.

Con el cifrado de enlace, cada enlace de comunicación vulnerable se equipa en ambos extremos con un dispositivo de cifrado. Así, todo el tráfico a través de los enlaces de comunicaciones se protege. Aunque esto requiere muchos dispositivos de cifrado en redes grandes, el valor de esta opción está claro. Una desventaja es que el mensaje debe ser descifrado cada vez que entra un paquete en un conmutador; esto es así ya que el conmutador debe leer la dirección (número de circuito virtual) en la cabecera del paquete para encaminarlo. De esta forma, el mensaje es vulnerable en cada nodo. Si la red es de conmutación de paquetes pública, el usuario no tiene control sobre la seguridad en los nodos.

Con un cifrado extremo-a-extremo, el proceso de cifrado se realiza en los dos sistemas finales. El computador o terminal origen cifra los datos. Los datos cifrados se transmiten sin alterarlos a través de la red hasta el computador o terminal destino. El destino comparte una clave con el origen y es, por lo tanto, capaz de descifrar los datos. Esta técnica parece proteger la transmisión contra agresiones en los enlaces o conmutadores de red. Hay, sin embargo, un punto débil.

Considere la siguiente situación. Un computador se conecta a una red de conmutación de paquetes X.25, establece un circuito virtual a otro computador y se prepara para enviar datos al otro computador utilizando una cifrado extremo-a-extremo. Los datos se transmiten por esa red en la forma de paquetes, que constan de una cabecera y algunos datos de usuario. ¿Qué parte de cada paquete cifrará el computador? Supongamos que el computador cifra el paquete entero, incluyendo la cabecera. Esto no funcionará

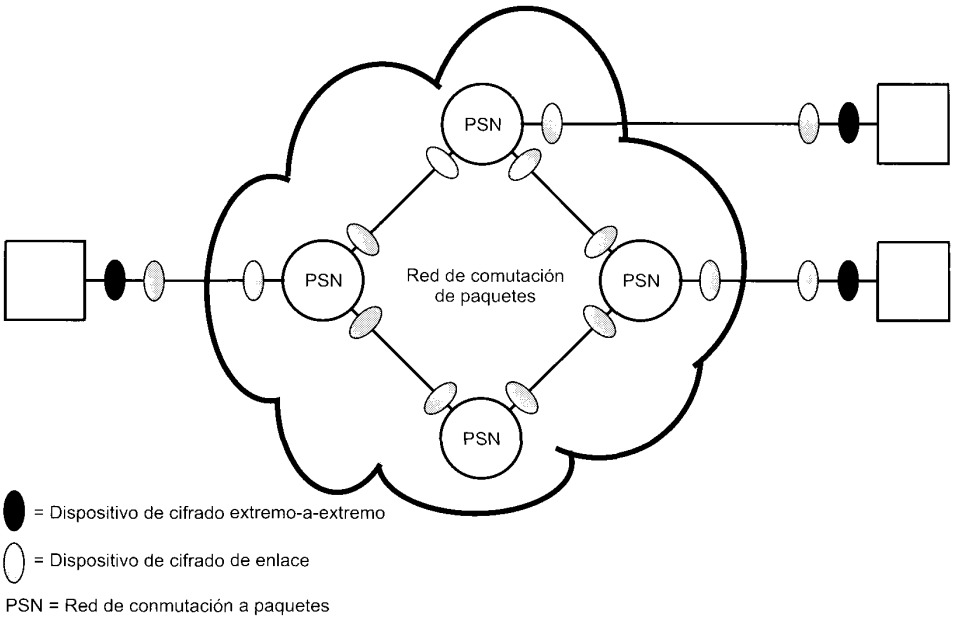


Figura 18.5. Cifrado a través de una red de conmutación a paquetes.

ya que, recuerde, sólo el otro computador puede descifrar el paquete. El nodo de conmutación recibirá el paquete cifrado y no será capaz de leer la cabecera. Por lo tanto, no será capaz de encaminar el paquete. De esto se concluye que el computador sólo puede cifrar la parte de datos de usuario y no la parte de cabecera, para que ésta pueda ser leída por la red.

Así, con el cifrado extremo-a-extremo, los datos de usuario están seguros. Sin embargo, el modelo de tráfico no lo está, ya que las cabeceras de los paquetes se transmiten sin cifrarlas. Para alcanzar un mayor grado de seguridad, se necesita cifrado de enlace y extremo-a-extremo, como se muestra en la Figura 18.5.

Para resumir, cuando se utilizan ambas formas, el computador cifra la parte de datos de usuario usando una clave de cifrado extremo-a-extremo. Después se cifra el paquete entero usando una clave de cifrado de enlace. Conforme el paquete viaja por la red, cada nodo conmutador descifra el paquete utilizando una clave de cifrado de enlace para poder leer la cabecera y luego cifra de nuevo el paquete entero para enviarlo al siguiente enlace. Ahora el paquete está seguro excepto durante el tiempo en el que el paquete está en la memoria del nodo de conmutación, en el que la cabecera está desprotegida.

DISTRIBUCIÓN DE CLAVES

Para que funcione el cifrado convencional, las dos partes que intercambian datos deben tener la misma clave y ésta debe ser protegida para que no la conozcan otros. Además, es deseable realizar normalmente cambios de la clave para limitar la cantidad de datos comprometidos si una agresión aprende la clave. Por lo tanto, la potencia de cualquier sistema de cifrado se apoya en una técnica de distribución de claves, un término que se refiere a los medios para distribuir una clave a dos partes que quieren intercambiar datos, impidiendo que otros vean la clave. La distribución de claves se puede conseguir de varias formas. Para dos partes A y B:

1. A puede seleccionar una clave y entregarla físicamente a B.

2. Una tercera parte selecciona la clave y la entrega físicamente a A y a B.
3. Si A y B han utilizado previamente y recientemente una clave, una de las partes podría transmitir la nueva clave a la otra cifrada utilizando la clave previa.
4. Si A y B tienen cada uno una conexión cifrada a una tercera parte C, C podría entregar una clave a través de los enlaces cifrados a A y a B.

Las opciones 1 y 2 exigen una entrega manual de una clave. Éste es un requisito razonable para el cifrado de enlace ya que cada dispositivo de cifrado de enlace sólo va a intercambiar datos con su pareja en el otro extremo de enlace. Sin embargo, para cifrado extremo-a-extremo, la entrega manual es difícil. En un sistema distribuido, cualquier terminal o computador se ve envuelto en intercambios con muchos otros terminales o computadores durante mucho tiempo. Así, cada dispositivo necesita varias claves, suministradas dinámicamente. El problema es especialmente difícil en sistemas distribuidos a través de una gran área.

La opción 3 es una posibilidad válida tanto para el cifrado de enlace como el de extremo-a-extremo, pero si un agresor tiene éxito al conseguir una clave, todas las claves siguientes serán reveladas. Incluso si se hacen cambios frecuentes en la clave de cifrado de enlace, éstos se deberían hacer manualmente. La opción 4 es la preferible para proporcionar claves de cifrado extremo-a-extremo.

La Figura 18.6 muestra una implementación que cumple con la opción 4 para el cifrado extremo-a-extremo. En la figura se ha ignorado el cifrado de enlace. Ésta se puede incorporar, o no, según se requiera. Para este esquema, se identifican dos clases de claves:

- **Clave de sesión:** cuando dos sistemas finales (computadores, terminales, etc.) desean comunicarse, establecen una conexión lógica (por ejemplo, circuitos virtuales). Durante la duración de la conexión lógica, todos los datos de usuario se cifran con una clave de sesión de un solo uso. Al terminar la sesión, o conexión, la clave de sesión se destruye.
- **Clave permanente:** es la clave usada entre entidades con el objetivo de distribución de claves de sesión.

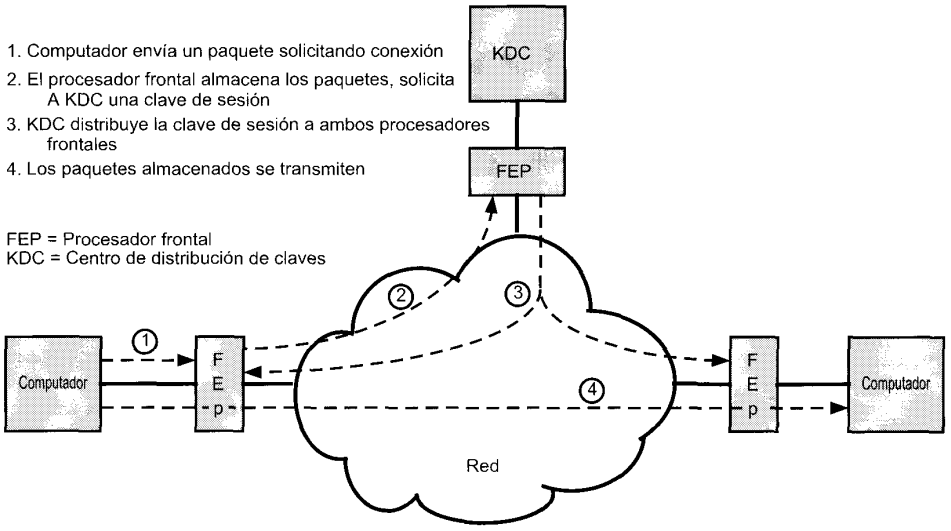


Figura 18.6. Distribución de claves automática para protocolos orientados a conexión.

La configuración consta de los siguientes elementos:

- **Centro de distribución de claves (CDC):** el centro de distribución de claves determina a qué sistemas se les permite comunicarse con otros. Cuando se concede un permiso a dos sistemas para establecer una conexión, el centro de distribución de claves proporciona una clave de sesión de un solo uso a esa conexión.
- **Procesador frontal (PF):** el procesador frontal lleva a cabo el cifrado extremo-a-extremo y obtiene las claves de sesión en representación de su computador o terminal.

Los pasos necesarios para establecer una conexión se muestran en la figura. Cuando un computador desea establecer una conexión con otro computador, transmite un paquete de solicitud de conexión (paso 1). El procesador frontal guarda el paquete y solicita permiso al CDC para establecer una conexión (paso 2). La comunicación entre el PF y el CDC está cifrada utilizando una clave maestra compartida sólo por el PF y el CDC. Si el CDC aprueba la solicitud de conexión, genera una clave de sesión y la entrega a los dos procesadores frontales apropiados, utilizando una clave única permanente para cada procesador frontal (paso 3). El procesador frontal solicitante puede ahora liberar el paquete de solicitud de conexión y se establece la conexión entre los dos sistemas finales (paso 4). Todos los datos de usuario intercambiados entre los dos sistemas finales son cifrados por sus respectivos procesadores frontales usando la clave de sesión única.

La técnica de distribución de claves automática proporciona las características de flexibilidad y de dinamismo necesarias para permitir a varios usuarios de terminales acceder a una serie de computadores, y a los computadores intercambiar datos con cada uno de los otros.

Por supuesto, el cifrado por clave pública utiliza otra técnica de distribución de claves, pero será discutida en la Sección 18.4.

RELLENO DE TRÁFICO

Se ha mencionado, en algunos casos, que los usuarios están preocupados por la seguridad en casos de análisis de tráfico. Con el uso de cifrado de enlace, las cabeceras de los paquetes se cifran, reduciendo la oportunidad de hacer un análisis de tráfico. Sin embargo, es todavía posible en estas circunstancias que un agresor calcule la cantidad de tráfico en la red y observe la cantidad de tráfico que entra y sale de cada sistema final. Una contramedida efectiva a esta agresión es el relleno de tráfico.

El relleno de tráfico es una función que produce salida de texto cifrado continuamente, incluso en ausencia de texto nativo. Se genera un flujo de datos aleatorio continuamente. Cuando hay disponible texto nativo, se cifra y se transmite. Cuando el texto nativo no está presente, los datos aleatorios se cifran y transmiten. Esto hace imposible que un agresor distinga entre flujo de datos verdaderos y ruido y por tanto le resulta imposible deducir la cantidad de tráfico.

18.3. AUTENTIFICACIÓN DE MENSAJES Y FUNCIONES DE DISPERSIÓN (HASH)

El cifrado protege de las agresiones pasivas (escuchas). Un requisito diferente es la protección a las agresiones activas (falsificación de datos y transacciones). La protección contra esas agresiones se conoce como autentificación de mensajes.

TÉCNICAS DE AUTENTIFICACIÓN DE MENSAJES

Un mensaje, fichero, documento, u otra colección de datos se dice que está autentificada cuando son genuinos y vienen del origen pretendido. La autentificación de mensajes es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos son auténticos. Los dos aspectos importantes son verificar que el contenido del mensaje no se ha alterado y que el origen es auténtico.

También estaremos interesados en verificar que los datos son oportunos (que no han sido artificialmente retrasados y reemplazados) y verificar la secuencia relativa a otros mensajes que fluyen entre dos partes.

Autentificación utilizando cifrado convencional

Es posible llevar a cabo la autentificación simplemente mediante el uso del cifrado convencional. Si suponemos que solamente el emisor y el receptor comparten la clave (que es lo que debería ocurrir), entonces solamente el emisor genuino sería capaz de cifrar un mensaje satisfactoriamente para la otra parte. Además, si el mensaje incluye un código de detección de errores y un número de secuencia, se le asegura al receptor que no se han hecho alteraciones y que la secuencia es la adecuada. Si el mensaje también incluye una marca de tiempo, el receptor tiene la seguridad de que el mensaje no se ha retrasado más de lo normalmente esperado en el tránsito por la red.

Autentificación de mensajes sin cifrado de mensajes

En esta sección, examinamos varias técnicas para autentificar mensajes sin basarse en el cifrado. En todas estas técnicas, se genera una etiqueta de autentificación que se incorpora al mensaje para su transmisión. El mensaje mismo no está cifrado y se puede leer en el destino independientemente de la función de autentificación en el destino.

Ya que las técnicas descritas en esta sección no cifran el mensaje, no se proporciona privacidad en el mensaje. Como el cifrado convencional proporciona autentificación, y como se utiliza de una forma amplia con productos disponibles, ¿por qué no utilizar esta técnica, que proporciona el secreto y la autentificación de mensajes? En [DAVI90] se sugieren tres situaciones en las que es preferible autentificación sin tener que hacer los mensajes secretos.

1. Existen una serie de aplicaciones en las que el mensaje se difunde a varios destinos. Por ejemplo, para notificar a los usuarios que la red está disponible o una señal de alarma en un centro de control. Es más barato y más seguro tener solamente un destino para monitorizar la autentificación. Así, el mensaje que se va a difundir es texto nativo con una etiqueta de mensaje de autentificación asociada. El sistema responsable lleva a cabo la autentificación. Si ocurre una violación, se alertan a los otros sistemas destinos mediante una alarma general.
2. Otro posible escenario es un intercambio en el que una de las partes tiene una carga muy elevada y no tiene tiempo de descifrar los mensajes que llegan. La autentificación se realiza de una forma selectiva, eligiendo los mensajes de forma aleatoria para realizar comprobaciones.
3. La autentificación de un programa de computador en texto nativo es un servicio interesante. El programa se puede ejecutar sin tener que descifrarlo cada vez que se ejecuta, ya que de lo contrario se produciría un derroche de los recursos del procesador. Sin embargo, si la etiqueta de autentificación de mensaje fuera incorporada al programa, se podría comprobar siempre y cuando se necesite tener certeza de la integridad del programa.

Así, existen ámbitos distintos para cifrado y autentificación, dentro de los requisitos de seguridad.

Código de autentificación de mensajes (CAM)

Otra técnica de autentificación supone el uso de una clave secreta que genera un pequeño bloque de datos, conocido como código de autentificación de mensaje, y que se incorpora al mensaje. Esta técnica supone que dos partes comunicantes, digamos A y B, comparten una clave secreta común K_{AB}. Cuando A tiene un mensaje que enviar a B, calcula el código de autentificación del mensaje como una función del mensaje y la clave: $MAC_M = F(K_{AB},M)$. Luego se transmite el mensaje y el código al destino. El receptor realiza los mismos cálculos en el mensaje recibido, utilizando la misma clave secreta, para generar un nuevo código de autentificación de mensaje. El código recibido se compara con el código cal-

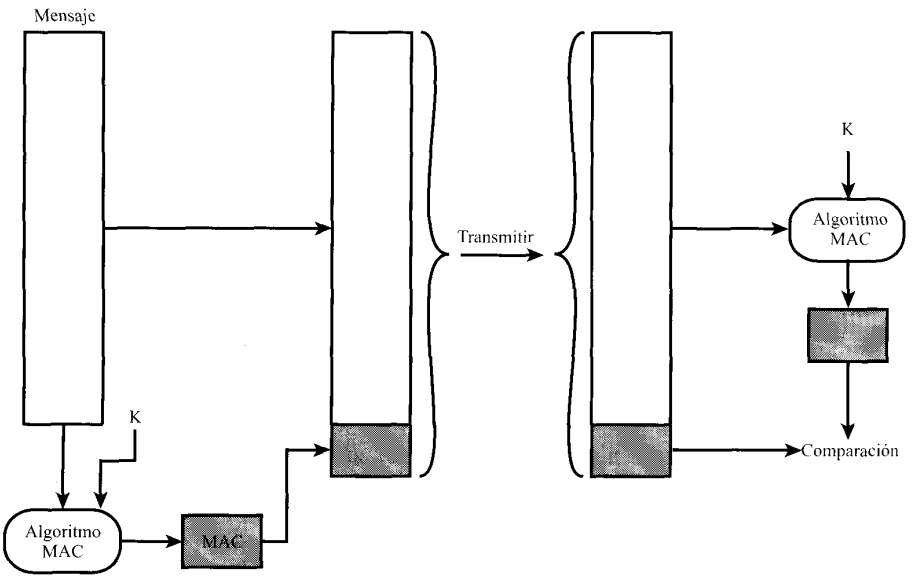


Figura 18.7. Autentificación de mensajes utilizando un código de autentificación de mensaje (MAC).

culado (Figura 18.7). Si suponemos que sólo el emisor y el receptor conocen la identidad de la clave, y si el código recibido coincide con el calculado, entonces:

1. El receptor está seguro que el mensaje no ha sido alterado. Si un agresor altera el mensaje pero no el código, el código calculado en el receptor diferirá del código recibido. Ya que se supone que el agresor no conoce la clave secreta, éste no podrá modificar el código para que corresponda con la modificación en el mensaje.
2. El receptor está seguro que el mensaje es del emisor pretendido. Ya que nadie más conoce la clave secreta, nadie podría preparar un mensaje con el código apropiado.
3. Si el mensaje incluye un número de secuencia (como los que se utilizan con X.25, HDLC y TCP), entonces el receptor puede estar seguro de la secuencia adecuada, ya que un agresor no puede alterar el número de secuencia satisfactoriamente.

Se pueden utilizar una serie de algoritmos para generar el código. El Buró Nacional de Estándares, en su publicación *Modos de operación de DES*, recomienda el uso del algoritmo DEA. El algoritmo DEA se utiliza para generar una versión cifrada del mensaje, y los últimos bits del texto cifrado se utilizan como código. Son normales códigos de 16 o 32 bits.

El proceso descrito es similar al de cifrado. Una diferencia es que el algoritmo de autentificación no necesita ser reversible, como es el caso para el descifrado. Resulta que debido a las propiedades matemáticas de la función de autentificación, éste es menos vulnerable que el cifrado cuando se rompe el mensaje.

Función de dispersión de un solo sentido

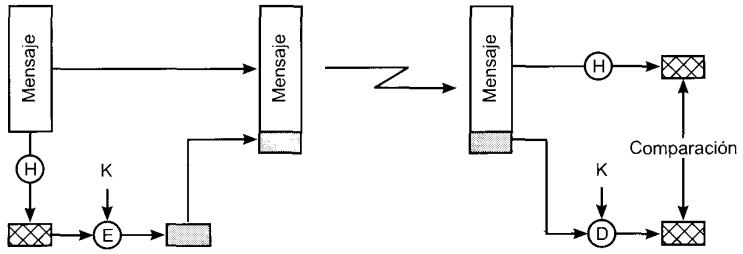
Una variación al código de autentificación de mensajes y que ha recibido mucha atención recientemente es la función de dispersión de un solo sentido. Como con el código de autentificación de mensajes, una función de dispersión acepta un mensaje de longitud variable M como entrada y produce una etiqueta de

tamaño fijo H(M), como salida. A diferencia del CAM, la función de dispersión no tiene como entrada una clave secreta. El resumen del mensaje se envía junto al mensaje de tal forma que el resumen del mensaje se puede utilizar en el receptor para autentificarlo.

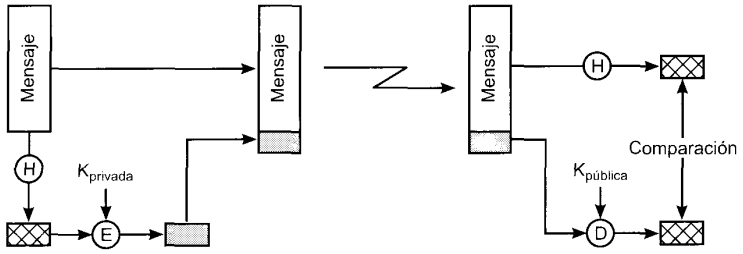
La Figura 18.8 muestra tres formas en las que se puede autentificar un mensaje. El resumen del mensaje se puede cifrar utilizando cifrado convencional (parte (a)); si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autentificación. El mensaje también se puede cifrar utilizando cifrado por clave pública (parte (b)); esto se explica en la Sección 18.4. La técnica de clave pública tiene dos ventajas: proporciona una firma digital así como autentificación de mensajes, y no requiere la distribución de claves a las partes que se comunican.

Estas dos técnicas tienen la ventaja sobre otras técnicas que cifran el mensaje entero en que requieren menos computación. Sin embargo, existe una serie de razones para desarrollar una técnica que evite el cifrado del conjunto. En [TSUD92] se indican algunas de estas razones:

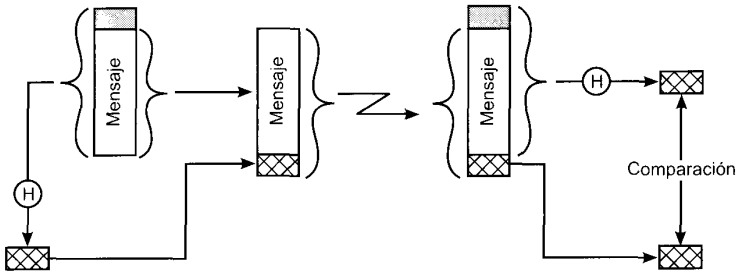
- El software de cifrado es muy lento. Incluso aunque la cantidad de datos que se van a cifrar sea pequeña, puede producirse una secuencia constante de mensajes entrando y saliendo del sistema.



(a) Utilizando cifrado convencional



(b) Utilizando cifrado de clave pública



(c) Utilizando un valor secreto

Figura 18.8. Autentificación de mensajes utilizando una función de dispersión de un solo sentido.

- El coste del hardware de cifrado no es despreciable. Están disponibles implementaciones en circuitos de bajo coste del algoritmo DES, pero este coste se puede incrementar bastante si todos los nodos de una red tienen que tener esta capacidad.
- El hardware de cifrado está optimizado para tamaños de datos grandes. Para bloques de datos pequeños, se emplea una gran cantidad de tiempo en la inicialización y en la invocación.
- Los algoritmos de cifrado pueden estar protegidos por patentes. Algunos algoritmos de cifrado, como el algoritmo de clave pública RSA, están patentados y se necesita licencia, lo que aumenta el coste.
- Los algoritmos de cifrado pueden estar sujetos a control de exportación. Esto es cierto para DES.

La Figura 18.8c muestra una técnica que utiliza una función de dispersión pero no utiliza cifrado para realizar la autentificación del mensaje. Esta técnica supone que las dos partes comunicantes, digamos A y B, comparten un valor secreto común S_{AB}. Cuando A envía un mensaje a B, calcula la función de dispersión utilizando la concatenación de la clave secreta y el mensaje: $MD_M = H(S_{AB}||M)$[1]. Entonces envía $[M||MD_M]$ a B. Ya que B posee S_{AB}, puede recalcular $H(S_{AB}||M)$ y verificar MD_M. Ya que el valor secreto no se envía, no es posible que un agresor modifique un mensaje interceptado. Mientras el valor secreto permanezca oculto, no es posible que un agresor genere un mensaje falso.

Esta tercera técnica, consistente en utilizar una valor secreto común, es la que ha adoptado IP para implementar las características en seguridad; también ha sido especificada para SNMPv3, discutido en el Capítulo 19.

FUNCIONES DE DISPERSIÓN SEGURAS

La función de dispersión de un solo sentido, o función de dispersión segura, es importante no sólo para la autentificación de mensajes, sino para las firmas digitales. En esta sección comenzaremos discutiendo los requisitos necesarios para obtener una función de dispersión segura. Después examinaremos una de las funciones de dispersión más relevantes, SHA-1.

Requisitos de una función de dispersión segura

El objetivo de una función de dispersión es producir una «huella dactilar» de un fichero, mensaje u otro bloque de datos. Para que sea útil para la autentificación, una función de dispersión H debe tener las siguientes propiedades:

1. H puede ser aplicada a bloques de datos de cualquier tamaño.
2. H produce una salida de longitud fija.
3. Para un x dado es relativamente fácil calcular $H(x)$, haciendo práctica la implementación hardware y software.
4. Para un código dado h, es imposible computacionalmente encontrar un x tal que $H(x) = h$.
5. Para un bloque dado x, es imposible computacionalmente encontrar un $y \neq x$ con $H(y) = H(x)$.
6. Es imposible computacionalmente encontrar una pareja (x, y) tal que $H(x) = H(y)$.

Las tres primeras propiedades son requisitos para la aplicación práctica de una función de dispersión a la autentificación de mensajes.

La cuarta propiedad es la propiedad de «un solo sentido»: es fácil generar un código dado un mensaje, pero virtualmente imposible generar un mensaje dado un código. Esta propiedad es importante si la técnica de autentificación supone el uso de un valor secreto (Figura 18.8c). El valor secreto no se envía;

[1] || indica concatenación.

sin embargo, si la función de dispersión no es de un solo sentido, un agresor puede descubrir fácilmente el valor secreto: si el agresor puede observar o interceptar una transmisión, el agresor obtiene el mensaje M y el código de dispersión $MD_M = H(S_{AB}||M)$. El agresor entonces invierte la función de dispersión para obtener $S_{AB}||M = H^{-1}(MD_M)$. Ya que el agresor tiene ahora M y $S_{AB}||M$ es una cuestión trivial obtener S_{AB}.

La quinta propiedad garantiza que no se puede encontrar un mensaje alternativo que produzca el mismo valor que un mensaje dado. Esto previene la falsificación cuando se utiliza un código de dispersión cifrado (Figuras 18.8a y 18.8b). Si esta propiedad no fuera válida, un agresor sería capaz de realizar la secuencia siguiente: primero, observar o interceptar un mensaje más su código de dispersión cifrado; segundo, generar un código de dispersión descifrado a partir del mensaje; tercero, generar un mensaje alternativo con el mismo código de dispersión.

Una función de dispersión que satisface las cinco primeras propiedades de la lista anterior se le conoce como función de dispersión débil. Si satisface también la sexta propiedad entonces se le conoce como función de dispersión fuerte. La sexta propiedad protege de una clase de agresión sofisticada conocida como agresión de cumpleaños[2].

Además de proporcionar autentificación, un resumen del mensaje proporciona también integridad de los datos. Lleva a cabo la misma función que la secuencia de comprobación de trama: si algún bit se altera accidentalmente en el tránsito, el resumen del mensaje producirá un error.

LA FUNCIÓN DE DISPERSIÓN SEGURA SHA-1

El algoritmo seguro de dispersión (SHA) fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) y publicado como estándar federal para el procesamiento de la información (FIPS PUB 180) en 1993; en 1985 se publicó una versión revisada como FIPS PUB 180-1 y generalmente se conoce como SHA-1.

El algoritmo toma como entrada un mensaje con una longitud máxima de 2^{64} bits y produce un resumen del mensaje de 160 bits. La entrada se procesa en bloques de 512 bits. La Figura 18.9 muestra el procesamiento general de un mensaje para producir un resumen. El procesamiento consta de los siguientes pasos:

Paso 1: incorporar bits de relleno. Se incorporan al mensaje bits de relleno para que su longitud en bits sea congruente con 448 módulo 512 (longitud = 448 modo 512). Esto es, la longitud del mensaje al que se le incorpora el relleno es 64 bits menos que un múltiplo entero de 512 bits. Siempre se incorpora el relleno, incluso si el mensaje tiene ya la longitud deseada. Así, el número de bits de relleno está en el rango de 1 a 512. El relleno consiste de un único bit con valor 1 seguido de los bits necesarios con valor cero.

Paso 2: incorporar la longitud. Se incorpora un bloque de 64 bits al mensaje. Este bloque se trata como un entero de 64 bits sin signo (los bits más significativos primero) y contiene la longitud del mensaje original (antes de incorporar el relleno). La inclusión de un valor de longitud hace más difícil un tipo de agresión, conocida como agresión de relleno [TSUD92].

La salida de los dos primeros pasos produce un mensaje que es un múltiplo entero de 512 bits en longitud. En la Figura 18.9, el mensaje ampliado se representa como una secuencia de bloques de 512 bits $Y_0, Y_1, \ldots, Y_{L-1}$, de manera que la longitud del mensaje ampliado es $L \times 512$ bits. Equivalentemente, el resultado es un múltiplo de 16 palabras de 32 bits. Las palabras del mensaje resultante se denotan como $M[0 \ldots N-1]$, con N un múltiplo entero de 16. Así, $N = L \times 16$.

Paso 3: inicializar la memoria temporal MD. Se utiliza una memoria temporal de 160 bits para almacenar los resultados intermedios y finales de la función de dispersión. La memoria temporal se

[2] Véase [STAL99a] para una discusión del ataque de cumpleaños.

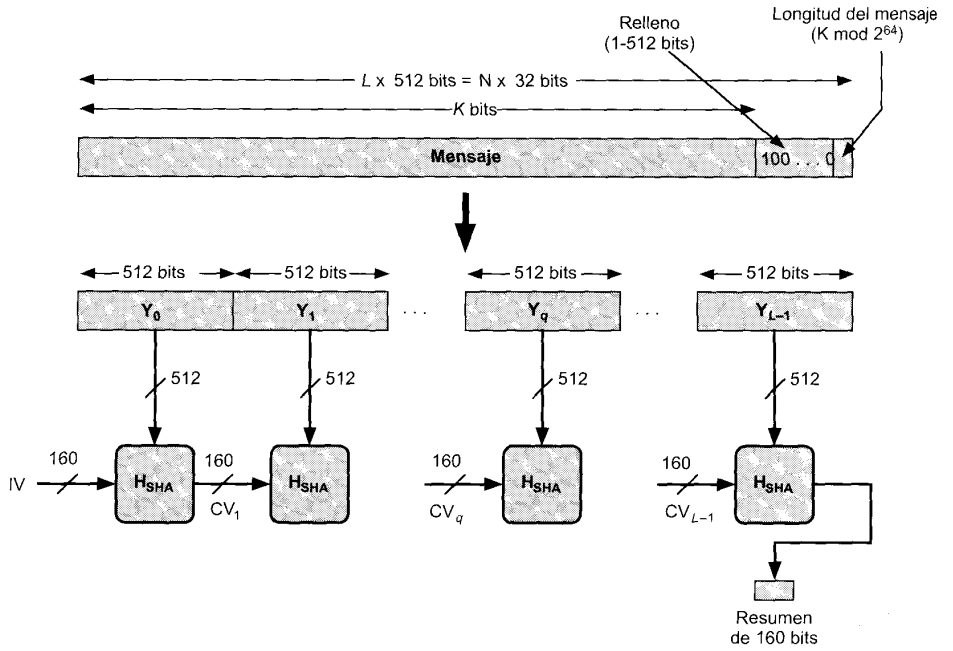


Figura 18.9. Generación de resumen de mensaje utilizando SHA-1.

puede representar con 5 registros de 32 bits (A, B, C, D, E). Estos registros se inicializan a los valores enteros de 32 bits siguientes (valores hexadecimales):

A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0

Paso 4: procesar el mensaje en bloques de 512 bits (palabras de 16 bits). El corazón del algoritmo es un módulo que consta de 4 rondas de procesamiento de 20 pasos cada uno. La lógica asociada se muestra en la Figura 18.10. Las cuatro rondas tienen una estructura similar pero cada una utiliza una función lógica primitiva diferente, conocidas como f_1, f_2, f_3 y f_4.

Cada ronda toma como entrada el bloque de 512 bits que se está procesando (Y_q) y el valor de la memoria temporal de 160 bits ABCDE y actualiza el contenido de la memoria temporal. Cada ronda también hace uso de una constante aditiva K_t, donde $0 \leqslant t \leqslant 79$ indica uno de los 80 pasos a lo largo de las cinco rondas. De hecho, sólo se utilizan cuatro constantes diferentes. Los valores, en hexadecimal y decimal, son los siguientes:

Número de paso	Hexadecimal	Tomar la parte entera de:
$0 \leqslant t \leqslant 19$	K_t = 5A827999	$[2^{30} \times \sqrt{2}]$
$20 \leqslant t \leqslant 39$	K_t = 6ED9EBA1	$[2^{30} \times \sqrt{3}]$
$40 \leqslant t \leqslant 59$	K_t = 8F1BBCDC	$[2^{30} \times \sqrt{5}]$
$60 \leqslant t \leqslant 79$	K_t = CA62C1D6	$[2^{30} \times \sqrt{10}]$

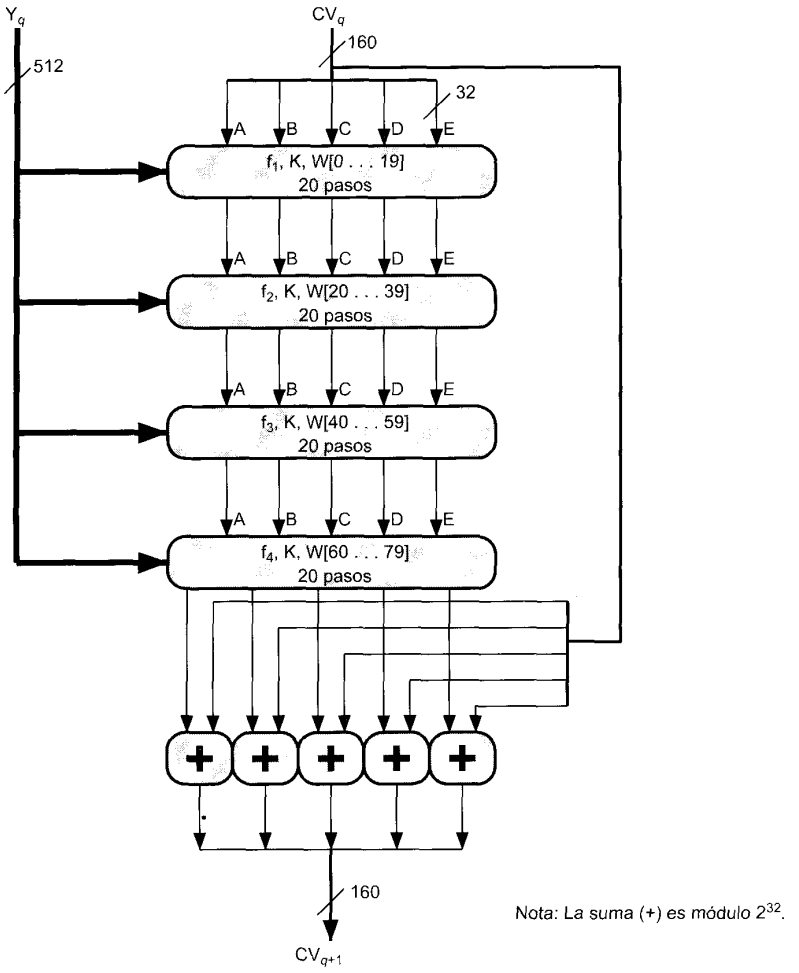


Figura 18.10. Procesamiento SHA-1 de un único bloque de 512 bits.

La salida de la ronda cuarta (octavo paso) se suma a la entrada de la primera ronda (CV_q) para producir (CV_{q+1}). Esta suma se hace independientemente para cada una de las cinco palabras almacenadas en la memoria temporal con cada palabra correspondiente en CV_q, utilizando suma módulo 2^{32}.

Paso 5: salida. Después de que los L bloques de 512 bits se han procesado, el resumen del mensaje de 160 bits es la salida de la etapa L-ésima.

El algoritmo SHA-1 tiene la propiedad de que cada bit del código de dispersión es una función de cada bit de la entrada. La repetición compleja de la función base f_t produce resultados que están bien mezclados; esto es, no es probable que dos mensajes elegidos aleatoriamente, incluso si exhiben regularidades similares, tengan el mismo código de dispersión. A menos que exista alguna debilidad oculta en SHA-1, lo cual todavía no se ha publicado, la dificultad de alcanzar dos mensajes que tienen el mismo resumen de mensaje es del orden de 2^{80} operaciones, mientras que la dificultad de encontrar un mensaje con un resumen dado es del orden de 2^{160} operaciones.

18.4. CIFRADO DE CLAVE PÚBLICA Y FIRMAS DIGITALES

El cifrado de clave pública tiene la misma importancia que el cifrado convencional, y encuentra su utilización en la autentificación de mensajes y en la distribución de claves. Esta sección examina primero los conceptos básicos del cifrado de clave pública, seguido por una discusión de las firmas digitales. Después se discute el algoritmo de clave pública más utilizado: RSA. Después se examina el problema de la distribución de claves.

CIFRADO DE CLAVE PÚBLICA

El cifrado de clave pública, propuesta en público por primera vez por Diffie y Hellman en 1976 [DIFF76], es el primer avance realmente revolucionario en el cifrado en literalmente miles de años. Y esto es debido a una razón, el algoritmo de clave pública se basa en funciones matemáticas en lugar de sustituciones y permutaciones. Pero lo más importante, la criptografía de clave pública es asimétrica y supone el uso de dos claves independientes, en contraste con el cifrado simétrico convencional, que sólo utiliza una clave. Utilizar dos claves tiene consecuencias profundas en las áreas de privacidad, distribución de claves y autentificación.

Antes de proseguir, deberíamos mencionar varios malentendidos comunes que afectan al cifrado de clave pública. Uno de tales malentendidos es que el cifrado de clave pública es más seguro frente al criptoanálisis que el cifrado convencional. En realidad, la seguridad de cualquier esquema de cifrado depende de (1) la longitud de la clave y (2) el trabajo computacional que requiere romper un cifrado. No hay nada en principio del cifrado convencional o de clave pública que haga a uno superior al otro desde el punto de vista de resistir el criptoanálisis. Un segundo malentendido es que el cifrado de clave pública es una técnica de uso general que ha hecho que se quede obsoleta el cifrado convencional. Por el contrario, a causa de la computación suplementaria de los esquemas actuales de cifrado por clave pública, no es probable que el cifrado convencional sea abandonado. Finalmente, existe el parecer de que la distribución de claves es trivial cuando se utiliza cifrado de clave pública, comparado con el diálogo más bien molesto que se requiere con los centros de distribución de claves en el cifrado convencional. De hecho, se necesita alguna forma de protocolo, a menudo implicando a un agente central, y los procedimientos implicados no son más sencillos o más eficientes que los que se requieren para el cifrado convencional.

El esquema de cifrado de clave pública tiene seis ingredientes (Figura 18.11):

- **Texto nativo:** es el mensaje legible o datos que se pasan al algoritmo como entrada.
- **Algoritmo de cifrado:** el algoritmo de cifrado lleva a cabo varias operaciones sobre el texto nativo.
- **Clave pública y privada:** éste es el par de claves que se ha seleccionado para que una se utilice para el cifrado y la otra para el descifrado. Las transformaciones exactas que realiza el algoritmo de cifrado dependen de la clave pública o privada que se suministra como entrada.
- **Texto cifrado:** es el mensaje mezclado producido como salida. Depende del texto nativo y de la clave. Para un mensaje dado, dos claves diferentes producen dos textos cifrados diferentes.
- **Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la otra clave y produce el texto nativo original.

Como el nombre sugiere, la clave pública del par se hace pública para que la utilice el resto de la gente, mientras que la clave privada solamente la conoce el dueño. Un algoritmo de criptografía de clave pública de propósito general se basa en una clave de cifrado y en una clave diferente, pero relacionada, para el descifrado. Además, estos algoritmos tienen las siguientes características importantes:

- No es factible computacionalmente determinar la clave de descifrado dado solamente el algoritmo de criptografía y la llave de cifrado.

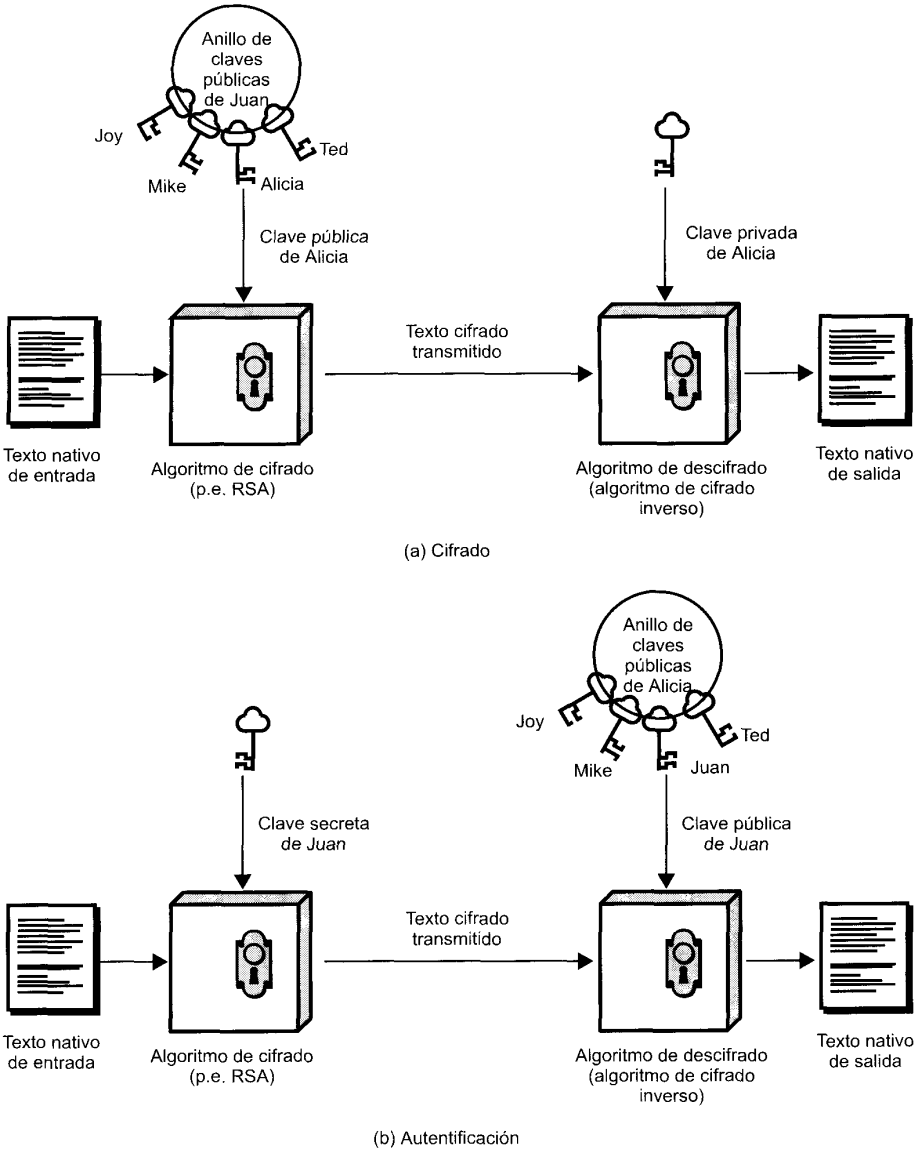


Figura 18.11. Cifrado de clave pública.

- Para la mayoría de los esquemas de clave pública, cualquiera de las dos claves que se utilizan, se puede emplear para el cifrado y la otra para el descifrado.

Los pasos esenciales son los siguientes:

1. Cada usuario genera un par de claves que se van a utilizar para el cifrado y el descifrado de los mensajes.

2. Cada usuario publica una de las dos claves de cifrado situándola en un registro o fichero público. Ésta es la clave pública. La clave compañera se mantiene privada. Como sugiere la Figura 18.11, cada usuario mantiene una colección de claves públicas de otros usuarios.
3. Si Juan desea enviar un mensaje privado a Alicia, él cifra el mensaje utilizando la clave pública de Alicia.
4. Cuando Alicia recibe el mensaje, los descifra utilizando su clave privada. Ningún otro destino puede descifrar el mensaje ya que solamente Alicia conoce la clave privada de Alicia.

Con esta técnica, todos los participantes tienen acceso a las claves públicas y las claves privadas se generan localmente por cada participante y por lo tanto nunca se distribuyen. Mientras un usuario controle su clave privada, los mensajes que le llegan son seguros. Un usuario puede cambiar su clave privada en cualquier instante de tiempo y publicar la clave pública compañera para reemplazar la clave pública obsoleta.

FIRMAS DIGITALES

El cifrado de clave pública se puede utilizar de otra forma, como se muestra en la Figura 18.11b. Suponga que Juan quiere enviar un mensaje a Alicia y, aunque no es importante que el mensaje se mantenga secreto, quiere que Alicia esté segura que en realidad el mensaje es de él. En este caso, Juan utiliza su propia clave privada. Cuando Alicia recibe el texto cifrado, encuentra que puede descifrarlo con la clave pública de Juan, demostrando así que el mensaje ha sido cifrado por Juan. Nadie más tiene la clave privada de Juan y, por lo tanto, nadie más ha podido crear el texto cifrado que se descifra con la clave pública de Juan. De esta forma, el mensaje cifrado completo sirve como **firma digital.** Además, es imposible alterar el mensaje sin acceder a la clave privada de Juan, por lo tanto el mensaje está autentificado en términos de la fuente y de integridad de los datos.

En el esquema precedente, se cifra el mensaje entero, lo que, aunque valida al autor y al contenido, requiere una gran cantidad de almacenamiento. Cada documento de debe guardar en texto nativo para ser útil por motivos prácticos. Se debe guardar también una copia del texto cifrado para que se pueda verificar el origen y el contenido en caso de disputa. Una forma más eficiente de conseguir el mismo resultado es cifrar un bloque pequeño de bits que sea una función del documento. Este bloque, llamado autentificador, debe tener la propiedad de que no sea factible cambiar el documento sin cambiar el autentificador. Si el autentificador se cifra con la clave privada del emisor, sirve como una firma que verifica al origen, el contenido y el secuenciamiento. Un código seguro de dispersión como es SHA-1 puede servir como función.

Es importante enfatizar que el proceso de cifrado que se acaba de describir no proporciona privacidad. Esto es, el mensaje que se envía está seguro frente a alteraciones, pero no lo está de ser escuchado. Esto es obvio en el caso de una firma basada en una parte del mensaje, ya que el resto del mensaje no está cifrado. Incluso en el caso de cifrar el mensaje entero, no hay protección de confidencialidad ya que cualquier observador puede descifrar el mensaje utilizando la clave pública del emisor.

EL ALGORITMO DE CIFRADO DE CLAVE PÚBLICA RSA

Uno de los primeros esquemas de clave pública fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT y publicado por primera vez en 1978 [RIVE78]. El esquema RSA ha sido considerado desde entonces como la única técnica mundialmente aceptada e implementada de algoritmo de cifrado de clave pública. RSA es un cifrador de bloque en el que el texto nativo y el texto cifrado son enteros entre 0 y $n - 1$ para algún n.

Para algún texto nativo M y un bloque cifrado C, el cifrado y el descifrado son de la siguiente forma:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Ambos, el emisor y el receptor deben conocer el valor de n. El emisor conoce el valor de e y el receptor sólo debe conocer el valor de d. De esta forma, éste es un algoritmo de clave pública con una clave pública dada por KU = $[e, n]$ y una clave privada KR = $[d, n]$. Para que este algoritmo sea satisfactoriamente un algoritmo de cifrado de clave pública, se deben satisfacer los siguientes requisitos:

1. Es posible encontrar valores de e, d, n tal que $M^{ed} = M \bmod n$ para todo $M < n$.
2. Es relativamente fácil calcular M^e y C^d para todos los valores de $M < n$.
3. Es imposible determinar d dado e y n.

Los dos primeros requisitos son fáciles de satisfacer. El tercer requisito se puede satisfacer para un valor grande de e y n.

La Figura 18.12 resume el algoritmo RSA. Se empieza por seleccionar dos números primos, p y q y calculando su producto n, que es el módulo para el cifrado y el descifrado. A continuación, necesitamos la cantidad $\phi(n)$, que se conoce como totalizador (*totient*) de Euler de n, y que es el número de enteros positivos menores que n y relativamente primo a n. Entonces, se selecciona el entero e que es relativamente primo a $\phi(n)$, esto es, el máximo común divisor de e y $\phi(n)$ debe ser 1. Finalmente, se calcula d como la inversa del multiplicador de e, módulo $\phi(n)$. Se puede demostrar que d y e tienen las propiedades deseas.

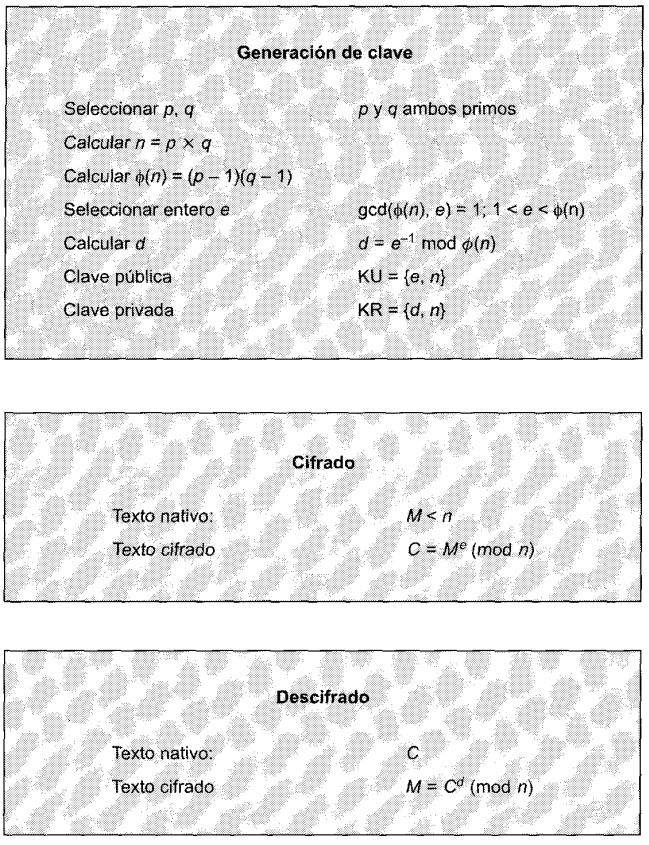


Figura 18.12. El algoritmo RSA.

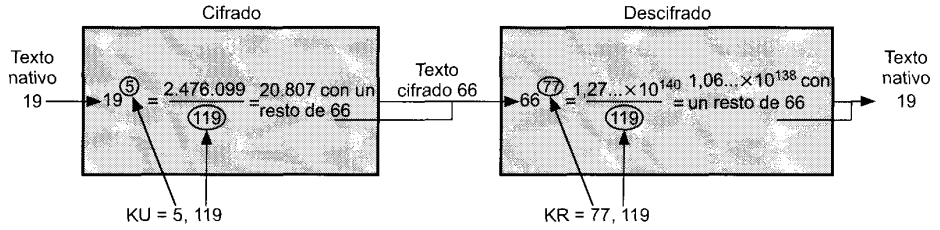


Figura 18.13. Ejemplo del algoritmo RSA.

Suponga que un usuario A ha publicado su clave pública y que el usuario B quiere enviar un mensaje M a A. Para ello, B calcula $C = M^e \pmod{n}$ y transmite C. Cuando se recibe el mensaje cifrado, A lo descifra calculando $M = C^d \pmod{n}$.

En la Figura 18.13 se muestra un ejemplo. En este ejemplo, las claves se generaron como sigue:

1. Seleccionar dos números primos, $p = 7$ y $q = 17$.
2. Calcular $n = pq = 7 \times 17 = 119$.
3. Calcular $\phi(n) = (p - 1)(q - 1) = 96$.
4. Seleccionar e tal que e es relativamente primo a $\phi(n) = 96$ y es menor que $\phi(n)$; en este caso, $e = 5$.
5. Determinar d tal que $de = 1 \pmod{96}$ y $d < 96$. El valor correcto es $d = 77$, ya que $77 \times 5 = 385 = 4 \times 96 + 1$.

Las claves resultantes son la clave pública KU = {5,119} y la clave privada KR = {77,119}. El ejemplo muestra el uso de estas claves para un texto nativo de entrada $M = 19$. En el cifrado, 19 se eleva a la quinta potencia, produciendo 2.476.099. Dividiendo por 119, se obtiene un resto de 66. Por lo tanto $19^5 \equiv 66 \pmod{119}$, y el texto cifrado es 66. En el descifrado, se determina que $66^{77} \equiv 19 \pmod{119}$.

Existen dos técnicas posibles para inutilizar el algoritmo RSA. La primera es una técnica de fuerza bruta: probar todas las claves privadas posibles. Así, cuanto más grandes sean en bits los números e y d, el algoritmo será más seguro. Sin embargo, a causa de los cálculos necesarios, tanto la generación de claves como el cifrado/descifrado son complejos y cuanto más grandes sean los tamaños de las claves más lento será el sistema.

La mayoría de las discusiones sobre el criptoanálisis se han centrado en la tarea de factorizar n en sus dos números primos. Para un n grande con factores primos grandes, la factorización es un problema difícil, pero no tanto como solía ser. Una ilustración sorprendente de esto es la siguiente. En 1977, los tres inventores de RSA desafiaron a los lectores de *Scientific American* a decodificar un texto cifrado que imprimieron en la columna «Juegos Matemáticos» de Martin Gardner. Ofrecieron 100 dólares como recompensa a quien les enviara la oración en texto nativo, un hecho que ellos predijeron que no ocurriría en 40 trillones de años. En abril de 1994 un equipo mundial cooperando con Internet y utilizando 1.600 computadores ha reclamado el premio después de sólo 8 meses de trabajo [LEUT94]. Este reto utilizaba un tamaño de clave pública (longitud de n) de 129 dígitos decimales, alrededor de 428 bits. Este resultado no invalida el uso de RSA; simplemente significa que se deben utilizar tamaños de clave más grandes. Actualmente, se considera bastante potente un tamaño de clave de 1.024 bits (aproximadamente 300 dígitos decimales) para virtualmente todas las aplicaciones.

GESTIÓN DE CLAVES

Con el cifrado convencional, un requisito fundamental para dos entes que se comunican de una forma segura es que compartan una clave secreta. Supóngase que Juan quiere crear una aplicación para enviar

mensajes que le permitirá intercambiar correo electrónico de una forma segura con cualquiera que tenga acceso a Internet o a alguna otra red que los dos comparten. Supóngase que Juan quiere hacer esto utilizando sólo cifrado convencional. Con el cifrado convencional, Juan y su corresponsal, digamos, Alicia, deben presentar una forma para compartir la clave secreta única y que nadie más conoce. ¿Cómo van a hacer esto? Si Alicia está en la habitación de al lado, Juan puede generar la clave y escribirla en un papel o almacenarla en un disquete y dársela a Alicia. Pero si Alicia está en la otra parte del continente o del mundo, ¿qué puede hacer Juan? Bien, podría cifrar la clave utilizando cifrado convencional y enviarla por correo electrónico a Alicia, pero esto significa que Juan y Alicia deben compartir una clave secreta para poder cifrar esta nueva clave secreta. Por lo tanto, Juan y cualquiera que utilice este nuevo paquete de correo electrónico se debe enfrentar al mismo problema con cualquier corresponsal potencial. Cada par de corresponsales deben compartir una clave secreta única.

El mayor problema para utilizar cifrado convencional es cómo distribuir las claves secretas de una forma segura. Este problema se elimina con el cifrado de clave pública por el simple hecho de que la clave privada nunca se distribuye. Si Juan quiere establecer correspondencia con Alicia u otra persona, genera un único par de claves, una privada y otra pública. Guarda la clave privada de una forma segura y difunde la clave pública a todos y cada uno. Si Alicia hace lo mismo, entonces Juan tiene la clave pública de Alicia, Alicia tiene la clave pública de Juan y ya pueden comunicarse con seguridad. Cuando Juan desea comunicarse con Alicia, puede hacer lo siguiente:

1. Preparar un mensaje.
2. Cifrar el mensaje utilizando cifrado convencional con una clave de sesión convencional.
3. Cifrar la clave de sesión utilizando cifrado de clave pública con la clave pública de Alicia.
4. Incorporar la clave de sesión cifrada al mensaje y enviarlo a Alicia.

Solamente Alicia es capaz de descifrar la clave de sesión y por tanto de recuperar el mensaje original.

Es justo señalar, sin embargo, que hemos reemplazado un problema por otro. La clave privada de Alicia es segura ya que no necesita revelarla nunca; sin embargo, Juan debe estar segura que la clave pública con el nombre de Alicia escrita en ella es de hecho la clave pública de Alicia. Alguien podría haber difundido una clave pública y haber dicho que era la de Alicia. La forma común de solucionar este problema es ingeniosa: utilizar cifrado de clave pública para autentificar claves públicas. Esto supone la existencia de alguna autoridad o individuo señalado y de confianza que actúe como sigue:

1. Alicia genera una clave pública y la envía a la Agencia X para certificarla.
2. X determina por algún procedimiento, como con una entrevista personal, que ésta es la auténtica clave pública de Alicia.
3. X incorpora una marca de tiempo a la clave pública, genera un código de dispersión al resultado y cifra el resultado con su clave privada formando una firma.
4. La firma se incorpora a la clave pública.

Cualquiera equipado con una copia de la clave pública de X puede ahora verificar que la clave pública de Alicia es auténtica.

18.5. SEGURIDAD CON IPv4 E IPv6

En 1994, el Comité de Arquitectura de Internet (IAB, Internet Architecture Board) publicó un informe titulado *Seguridad en la Arquitectura de Internet* (RFC 1636). El informe afirmaba el consenso general de que Internet necesitaba más y una mejor seguridad e identificaba las áreas clave para los mecanismos de seguridad. Entre éstos estaba la necesidad de hacer segura la infraestructura de red para evitar la monitorización no autorizada y el control del tráfico de red y la necesidad hacer seguro el tráfico usuario final a usuario final utilizando mecanismos de autentificación y cifrado.

Estas preocupaciones están plenamente justificadas. Como confirmación, el informe anual de 1998 del Equipo de Respuesta a Emergencias en Computadores (CERT, Computer Emergency Response Team) indicaba alrededor de 1.300 incidentes de seguridad documentados afectando a casi 20.000 sitios [CERT99]. Los tipos de ataques más serios incluían «falsos IP», el que un intruso crea un paquete con una dirección IP falsa y explota las aplicaciones que utilizan la autentificación basada en direcciones IP; y varias formas de escuchas y capturas de paquetes, en los que los atacantes leen la información transmitida, incluyendo información de conexión a sistemas y contenidos de bases de datos.

En respuesta a estas cuestiones, el IAB incluyó la autentificación y el cifrado como características de seguridad necesarias en el protocolo IP de nueva generación, que se ha denominado IPv6. Afortunadamente, estas capacidades de seguridad se diseñaron para que fueran utilizadas con IPv4 e IPv6. Esto significa que los fabricantes pueden ya empezar a ofrecer estas características, y ya muchos fabricantes tienen algunas capacidades de IPSec en sus productos.

APLICACIONES DE IPSec

IPSec proporciona la capacidad de hacer segura las comunicaciones a través de una LAN, una WAN privada o pública y a través de Internet. Algunos ejemplos de su uso incluyen los siguientes:

- **Conectividad segura entre oficinas sucursales a través de Internet:** una compañía puede construir una red privada virtual sobre Internet o a través de una WAN pública. Esto permite a un negocio apoyarse firmemente en Internet y reducir su necesidad de una red privada, ahorrando costes y gestión de red suplementaria.
- **Acceso remoto seguro a través de Internet:** un usuario final cuyo sistema está equipado con protocolos de seguridad IP puede hacer llamadas locales a su proveedor de servicios Internet (PSI) y acceder de forma segura a una red de una compañía. Esto reduce el coste de los gastos de peaje de los empleados de viaje y de los abonados.
- **Establecimiento de conectividad intranet y extranet con asociados:** IPSec se puede utilizar para hacer las comunicaciones seguras con otras organizaciones, asegurando la autentificación y la privacidad y proporcionando un mecanismo de intercambio de claves.
- **Mejorando la seguridad en el comercio electrónico:** incluso aunque algunas aplicaciones Web y de comercio electrónico tienen protocolos de seguridad internos, la utilización de IPSec mejora esa seguridad.

La principal característica de IPSec que le permite soportar estas aplicaciones variadas es que puede cifrar y/o autentificar *todo* el tráfico a nivel IP. Así, todas las aplicaciones distribuidas, incluyendo la conexión remota, cliente/servidor, correo electrónico, transferencia de ficheros, acceso a la Web y así muchas más, se pueden hacer seguras cinco propuestas de normalizaciones relacionadas con seguridad y que definían las capacidades de seguridad en la capa internet. Los documentos producidos eran:

EL ÁMBITO DE IPSec

IPSec proporciona tres facilidades principales: una función de sólo autentificación conocida como Cabecera de Autentificación (AH, Authentication Header), una función combinada de autentificación/cifrado llamada Encapsulado de seguridad de la carga útil (ESP, Encapsulating Security Payload) y una función de intercambio de claves. Para redes privadas virtuales generalmente se desea autentificación y cifrado, ya que es importante (1) asegurar que usuarios no autorizados no entran en la red privada virtual y (2) asegura que si hay personas dedicadas a hacer escuchas en Internet no pueden leer los mensajes enviados por la red privada virtual. Ya que ambas características son deseables, la mayoría de las implementaciones utilizan ESP en lugar de AH. La función de intercambio de claves permite el intercambio manual de claves así como un esquema automático.

Las especificaciones IPSec son bastantes complejas y se tratan en muchos documentos. Los más importantes de éstos, publicados en noviembre de 1998, son los RFCs 2401, 2402, 2406 y 2408 (véase Apéndice B). En esta sección se proporciona un repaso general a los elementos más importantes de IPSec.

ASOCIACIONES DE SEGURIDAD

Un concepto clave que aparece tanto en los mecanismos de autentificación como de privacidad en IP es la asociación de seguridad (SA, Security Association). Una asociación es una relación en un solo sentido entre un emisor y un receptor que proporciona servicios de seguridad al tráfico que se transporta. Si se necesita una relación paritaria, para un intercambio seguro en dos sentidos, entonces se requieren dos asociaciones de seguridad. Los servicios de seguridad se proporcionan a una SA para que utilice AH o ESP, pero no ambos.

Una asociación de seguridad está identificada unívocamente por tres parámetros:

- **Un índice de parámetros de seguridad (SPI, Security Parameters Index):** una cadena de bits asignada a esta SA y con significado local solamente. El SPI se transporta en las cabeceras AH y SPI para permitir que sistema receptor seleccione la SA bajo la que se procesarán los paquetes recibidos.
- **Dirección IP destino:** actualmente sólo se permiten direcciones monodistribución; ésta es la dirección del sistema final destino de la SA, que puede ser un usuario final o un sistema de red, como es un cortafuegos o un dispositivo de encaminamiento.
- **Identificador del protocolo de seguridad:** esto indica si la asociación es una asociación de seguridad AH o ESP.

Por lo tanto, en cualquier paquete IP, la asociación de seguridad está unívocamente identificada por la dirección destino en la cabecera IPv4 o IPv6 y el SPI incluida en la cabecera de extensión (AH o ESP).

Una implementación IPSec incluye una base de datos de asociaciones de seguridad que define los parámetros asociados con cada SA. Una asociación de seguridad se define normalmente por los parámetros siguientes:

- **Contador de número de secuencia:** un valor de 32 bits utilizado para generar el campo número de secuencia en las cabeceras AH o ESP.
- **Desbordamiento del contador de secuencia:** un indicador que avisa si se debe generar un evento audible si se produce un desbordamiento del contador de números de secuencia y así prevenir de transmisiones de paquetes adicionales de esta SA.
- **Ventana de anti-repeticiones:** utilizada para determinar si un paquete AH o ESP que llega es una repetición, mediante la definición de una ventana deslizante dentro de la cual se tiene que encontrar el número de secuencia.
- **Información AH:** algoritmo de autentificación, claves, tiempos de vida de las claves y parámetros relacionados que se utilizan con AH.
- **Información ESP:** algoritmos de cifrado y autentificación, claves, valores de inicialización, tiempos de vida de las claves y parámetros relacionados que se utilizan con ESP.
- **Tiempo de vida de la asociación de seguridad:** un intervalo de tiempo o contador de bytes después del cual una SA se tiene que reemplazar por una SA nueva (y un nuevo SPI) o terminar, más una indicación de cuál de estas opciones debería ocurrir.
- **Modo de protocolo IPSec:** túnel, transporte o marca de ambos (necesario en todas las implementaciones). Estos modos se discuten más tarde en esta sección.

- **MTU del camino:** cualquier unidad de transferencia máxima observada en el camino (tamaño máximo de los paquetes que se pueden transmitir sin fragmentación) y variables de caducidad (necesario en todas las implementaciones).

El mecanismo de gestión de claves que se utiliza para distribuir las claves está acoplado a los mecanismos de autentificación y de privacidad solamente a través del índice de parámetros de seguridad. Por lo tanto, la autentificación y la privacidad han sido especificadas independientemente de cualquier mecanismo de gestión de claves.

MODOS DE TRANSPORTE Y MODOS TÚNEL

AH y ESP permiten dos modos de uso: modo de transporte y modo túnel.

Modo transporte ESP

El modo transporte proporciona protección principalmente a los protocolos de las capas superiores. Es decir, la protección del modo de transporte se extiende sea la carga útil de un paquete IP. Algunos ejemplos incluyen a segmentos TCP o UDP o paquetes ICMP que operan directamente encima de IP en la pila de protocolos de un computador. Normalmente, el modo transporte se utiliza en comunicaciones extremo-a-extremo entre dos computadores (por ejemplo, un cliente y un servidor o dos estaciones de trabajo). Cuando ambos computadores implementan AH o ESP sobre IPv4 la carga útil son los datos que siguen a la cabecera IP. Para IPv6 la carga útil son los datos que siguen a la cabecera IP y a cualquier cabecera de extensión que esté presente, con la posible excepción de la cabecera de las opciones para el destino, que se podría incluir en la protección.

ESP en modo transporte cifra y opcionalmente autentifica la carga útil de IP pero no la cabecera IP. AH en modo transporte autentifica la carga útil de IP y porciones seleccionadas de la cabecera IP.

Modo túnel ESP

El modo túnel proporciona protección al paquete IP entero. Para alcanzar esto, después de que los campos AH o ESP se han incorporado al paquete IP, el paquete entero más un campo de seguridad se tratan como la carga útil de un paquete IP «exterior» nuevo con una cabecera IP exterior nueva. El paquete original entero, o interior, viaja a través del túnel desde un punto de la red IP a otro, ningún dispositivo de encaminamiento a lo largo del camino es capaz de examinar la cabecera IP interior. Ya que el paquete original está encapsulado el nuevo, un paquete más grande podría tener direcciones origen y destino totalmente diferentes, añadiendo seguridad. El modo túnel se utiliza cuando uno o ambos extremos de una SA es una pasarela de seguridad, como son un cortafuegos o un dispositivo de encaminamiento que implementa IPSec. Con el modo túnel, un determinado número de computadores en la red y detrás del cortafuegos pueden estar implicados en comunicaciones seguras sin implementar IPSec. Los paquetes no protegidos generados por tales computadores se transmiten mediante un túnel a través de redes externas mediante SA en modo túnel establecidas por el software IPSec en el cortafuegos o el dispositivo de encaminamiento seguro en las fronteras de la red local.

A continuación se da un ejemplo de cómo opera IPSec en modo túnel. Un computador A en una red genera un paquete IP con dirección destino del computador B en otra red. El paquete se encamina desde el computador origen a un cortafuegos o un dispositivo de encaminamiento seguro en la frontera de la red de A. El cortafuegos filtra todos los paquetes de salida para determinar si necesitan procesamiento IPSec. Si este paquete de A a B requiere IPSec, el cortafuegos realiza el procesamiento IPSec y encapsula el paquete en un paquete IP exterior. La dirección IP origen de este paquete exterior es la del cortafuegos y la dirección destino podría ser la de un cortafuegos que constituye la frontera de la red local de B. Este paquete se encamina al cortafuegos de B, y los dispositivos de encaminamiento intermedios sólo examinan la cabecera IP exterior. En el cortafuegos de B, se elimina la cabecera exterior y se encamina el paquete interior a B.

ESP en modo túnel cifra y opcionalmente autentifica al paquete IP interior completo, incluyendo la cabecera IP interior. AH en modo túnel autentifica el paquete IP interior completo y porciones seleccionadas de la cabecera IP exterior.

CABECERA DE AUTENTIFICACIÓN

La cabecera de autentificación proporciona un medio para la integridad de los datos y la autentificación de los paquetes IP. La característica de integridad de los datos asegura que la modificación no detectada del contenido del paquete no es posible en su camino. La característica de autentificación habilita a un sistema final o a un dispositivo de red autentificar el usuario o la aplicación y filtrar el tráfico adecuadamente; también previene el ataque de suplantación de dirección observado actualmente en Internet. La AH también protege frente a ataques de repetición descritos más tarde en esta sección.

La autentificación se basa en el uso de un código de autentificación de mensaje (MAC, Message Authentication Code), como se describe en la Sección 18.3; por lo tanto las dos partes deben compartir una clave secreta.

La cabecera de autentificación consta de los siguientes campos (Figura 18.14):

- **Cabecera siguiente (8 bits):** identifica el tipo de cabecera que viene a continuación de ésta.
- **Longitud de la carga útil (8 bits):** longitud de la cabecera de autentificación en palabras de 32 bits, menos 2. Por ejemplo, la longitud por defecto del campo de datos de autentificación es de 96 bits, o tres palabras de 32 bits. Con una cabecera de 3 palabras fijas, hay un total de seis palabras en la cabecera, por tanto el campo longitud de la carga útil vale 4.
- **Reservado (16 bits):** para usos futuros.
- **Índice de parámetros de seguridad (32 bits):** identifica a una asociación de seguridad.
- **Número de secuencia (32 bits):** el valor de un contador que se incrementa monotónicamente.
- **Datos de autentificación (variable):** un campo de longitud variable (debe ser número entero de palabras de 32 bits) que contiene el valor de chequeo de integridad (ICV, Integrity Check Values), o el MAC para este paquete.

El contenido del campo de datos de autentificación se calcula sobre lo siguiente:

- Campos de la cabecera IP que no cambian en el camino (inmutables) o que tienen un valor predecible de AH SA cuando llega al sistema final. Los campos que pueden cambiar en el tránsito o que no se pueden predecir en la llegada se hacen cero para motivos de cálculo tanto en el origen como en la fuente.

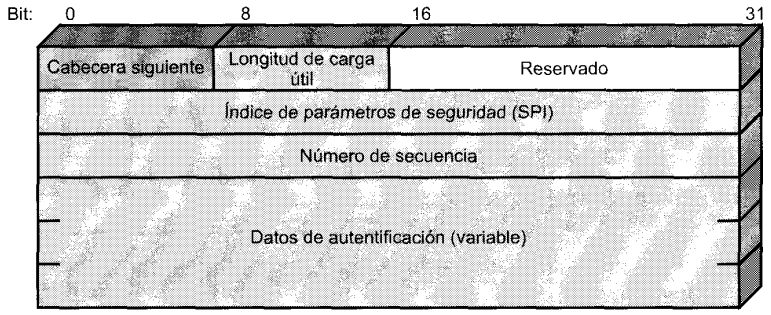


Figura 18.14. Cabecera de autentificación IPSec.

- La cabecera AH excluyendo al campo datos de autentificación. El campo de datos de autentificación se hace cero para motivos de cálculo tanto en el origen como en la fuente.
- Los datos del protocolo de la capa superior, que se supone son inmutables en el camino (por ejemplo, un segmento TCP o un paquete IP interior en modo túnel).

Para IPv4, algunos ejemplos de campos inmutables son la longitud de la cabecera IP y la dirección origen. Como ejemplo de campo sujeto a cambios pero predecible es la dirección destino (para el encaminamiento por la fuente estricto o aproximado). Ejemplos de campos sujetos a cambios que se hacen cero antes de los cálculos ICV son los campos tiempo de vida y suma de comprobación. Nótese que los campos de dirección origen y destino están protegidos, y así se previene la suplantación de dirección.

Para IPv6, algunos ejemplos de la cabecera base son *versión* (inmutable), *dirección destino* (sujeto a cambios pero predecible) *etiqueta de flujo* (sujeto a cambios y puesto a cero para los cálculos).

ENCAPSULADO DE SEGURIDAD DE LA CARGA ÚTIL

El encapsulado de seguridad de la carga útil proporciona servicios de privacidad, incluyendo confidencialidad de los contenidos de los mensajes y una confidencialidad limitada del flujo de tráfico. Como una característica opcional, ESP puede también proporcionar los mismos servicios de autentificación que AH.

La Figura 18.15 muestra el formato de un paquete. Contiene los siguientes campos:

- **Índice de parámetros de seguridad (32 bits):** identifica una asociación de seguridad.
- **Número de secuencia (32 bits):** el valor de un contador que se incrementa monóticamente.
- **Datos de carga útil (variable):** esto es un segmento de la capa de transporte (modo de transporte) o un paquete IP (modo túnel) que se protege mediante el cifrado.
- **Relleno (0-255 bytes):** este campo se puede requerir si el algoritmo de cifrado requiere que le texto nativo sea un múltiplo de algún número de octetos.
- **Longitud de relleno (8 bits):** indica el número de bytes de relleno en el campo que precede a éste.
- **Cabecera siguiente (8 bits):** identifica el tipo de datos contenidos en el campo de datos de carga útil mediante la identificación de la primera cabecera en esa carga útil (por ejemplo, una cabecera de extensión en IPv6 o un protocolo de la capa superior como TCP).

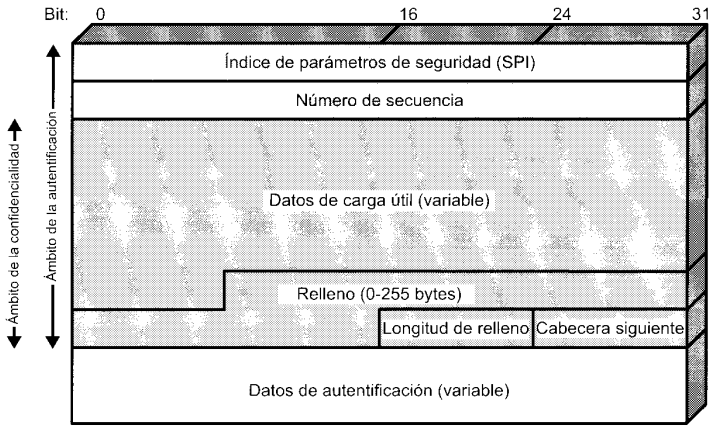


Figura 18.15. Formato ESP IPSec.

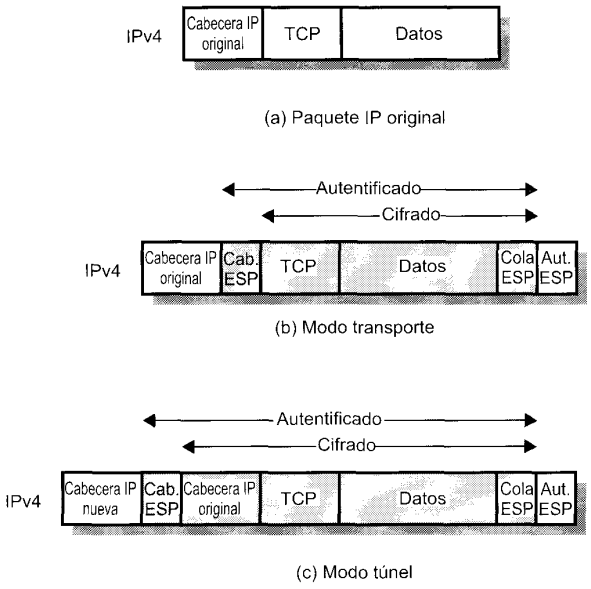


Figura 18.16. Ámbito del cifrado y la autentificación ESP.

- **Datos de autentificación (variable):** un campo de longitud variable (debe ser número entero de palabras de 32 bits) que contiene el valor de chequeo de integridad calculado sobre el paquete ESP menos el campo de datos de autentificación.

La Figura 18.16 muestra el ámbito del cifrado y autentificación ESP en los modos de transporte y túnel.

GESTIÓN DE CLAVES

La porción de gestión de claves de IPSec supone la determinación y distribución de claves secretas. Los documentos de la arquitectura de IPSec obligan a permitir dos tipos de gestión de claves:

- **Manual:** un administrador del sistema configura manualmente cada sistema con sus propias claves y con las claves de otros sistemas de comunicación. Esto es práctico para entornos pequeños y relativamente estáticos.
- **Automática:** un sistema automático habilita la creación bajo demanda de claves para SAs y facilita el uso de claves en sistemas distribuidos grandes con una configuración cambiante. Un sistema automático es lo más flexible pero requiere más esfuerzos para configurar y requiere más software, por lo tanto es más probable que las instalaciones más pequeñas opten por una gestión de claves manual.

El protocolo de gestión de claves automático que se utiliza por defecto en IPSec se conoce como ISAKMP/Oakley, que consta de los siguientes elementos:

- **Protocolo de determinación de claves Oakley:** Oakley es un protocolo de intercambio de claves basado en el algoritmo Diffie-Hellman, pero proporcionando una seguridad adicional. En particular, Diffie-Hellman sólo no autentifica a los dos usuarios que intercambian claves, haciendo el protocolo vulnerable a la suplantación. Oakley incluye mecanismos para autentificar a los usuarios.

- **Asociación de Seguridad de Internet y protocolo de Gestión de claves (ISAKMP, Internet Security Association and Key Management Protocol):** ISAKMP proporciona un entorno de trabajo para la gestión de claves en Internet y proporciona el soporte del protocolo específico, incluyendo formatos, para la negociación de los atributos de seguridad.

ISAKMP por sí mismo no impone un algoritmo de intercambio de claves específico; en lugar de eso, ISAKMP consiste de un conjunto de tipos de mensajes que permiten el uso de una variedad de algoritmos de intercambio de claves. Oakley es el algoritmo de intercambio de claves de uso obligatorio en la versión inicial de ISAKMP.

18.6. LECTURAS RECOMENDADAS Y PÁGINAS WEB

Los tópicos de este capítulo se tratan con un mayor detalle en [STAL95]. Para una mayor información sobre los algoritmos de criptografía, [SCHN96] es un trabajo de referencia esencial; contiene descripciones de virtualmente cada algoritmo y protocolo criptográfico publicado en los últimos 15 años.

SCHN96 Schneier, B. *Applied Cryptography*. New York: Wiley, 1996.

STAL99 Stallings, W. *Cryptography and Network Security: Principles and Practice, 2nd Edition*. Upper Saddle River, NJ: Prentice Hall, 1999.

SITIOS WEB RECOMENDADOS

- **COAST:** un conjunto completo de enlaces relacionados con la criptografía y la seguridad de red.
- **Área de seguridad de la IEFT:** proporciona información actualizada sobre los esfuerzos en la estandarización de la seguridad en Internet.
- **Comité Técnico de IEEE sobre seguridad y privacidad:** proporciona copias de periódicos de noticias de IEEE e información sobre la actividades relacionadas de IEEE.

18.7. PROBLEMAS

18.1. Dé algunos ejemplos donde el análisis del tráfico pueda comprometer la seguridad. Describa situaciones donde el cifrado extremo-a-extremo combinado con el cifrado de enlace permitiría todavía bastante análisis del tráfico como para que sea peligrosos.

18.2. Los esquemas de distribución de claves utilizando un centro de control de accesos y/o un centro de distribución de claves tienen puntos centrales vulnerables a ataques. Discuta las implicaciones en la seguridad de tal centralización.

18.3. Suponga que alguien sugiere la siguiente forma para confirmar que usted y su pareja están en posesión de la misma clave secreta. Usted crea una cadena de bits aleatoria de longitud igual a la de la clave, realiza la operación XOR entre la cadena y la clave y envía el resultado por el canal. Su pareja realiza la operación XOR del bloque recibido con la clave (que debería ser la misma) y envía el resultado de vuelta. Usted comprueba y si recibe la cadena de bits original, se ha verificado que su pareja tiene la misma clave sin haberla transmitido en ningún momento. ¿Hay algún defecto en este esquema?

18.4. Antes del descubrimiento de cualquier esquema de clave pública específico, como es RSA, se desarrolló una demostración de existencia cuyo propósito fue demostrar que el cifrado de clave pública era posible en teoría. Considere la función $f_1(x_1) = z_1$; $f_2(x_2, y_2) = z_2$; $f_3(x_3, y_3) = z_3$ cuyos valores son enteros con $1 \leqslant x_i, y_i, z_i \leqslant N$. La función f_i se puede representar por un vector $\mathbf{M}_i$ de longitud N, en el que la entrada k es el valor de $f_i(k)$. De igual forma, f_2 y f_3 se pueden representar por las matrices $N \times N$ $\mathbf{M}_2$ y $\mathbf{M}_3$. La intención es representar el proceso de cifrado/descifrado por búsquedas en tablas con valores muy grandes de N. Tales tablas serían imposibles de grandes pero podrían, en principio, construirse. El esquema trabaja como sigue: construya $\mathbf{M}_1$ con permutaciones aleatoria de todos lo enteros entre 1 y N; esto es, cada entero aparece exactamente una sola vez en $\mathbf{M}_1$. Construya $\mathbf{M}_2$ de forma que cada fila contenga una permutación aleatoria de los N primeros enteros. Finalmente, rellene $\mathbf{M}_3$ para que satisfaga la siguiente condición:

$$f_3(f_2(f_1(k), p), k) = p \text{ para todo } k, p \text{ con } 1 \leqslant k, p \leqslant N$$

En otras palabras:

1. $\mathbf{M}_1$ toma como entrada k y produce una salida x.
2. $\mathbf{M}_2$ toma como entrada x y p dando z como salida
3. $\mathbf{M}_3$ toma como entrada z y k y produce p.

Las tres tablas, una vez construidas, se hacen públicas.

a) Debería quedar claro que es imposible construir $\mathbf{M}_3$ para que satisfaga la condición anterior. Como ejemplo, rellene $\mathbf{M}_3$ para el caso simple siguiente:

$\mathbf{M}_1 =$

5
4
2
3
1

$\mathbf{M}_2 =$

5	2	3	4	1
4	2	5	1	3
1	3	2	4	5
3	1	4	2	5
2	5	3	4	1

$\mathbf{M}_3 =$

Convención: el elemento i de $\mathbf{M}_1$ corresponde a $k = 1$. La fila i de $\mathbf{M}_2$ corresponde a $x = i$; la columna j de $\mathbf{M}_2$ corresponde a $p = j$. La fila i de $\mathbf{M}_3$ corresponde a $z = i$; la columna j de $\mathbf{M}_3$ corresponde a $k = j$.

b) Describa la utilización de este conjunto de tablas para llevar a cabo el cifrado y el descifrado entre dos usuarios.

c) Argumente que esto es un esquema seguro.

18.5. Lleve a cabo el cifrado y el descifrado utilizando el algoritmo RSA como en la Figura 18.12, con los siguientes valores:

a) $p = 3$; $q = 11$, $d = 7$; $M = 5$

b) $p = 5$; $q = 11$, $d = 3$; $M = 9$

c) $p = 7$; $q = 11$, $d = 17$; $M = 8$

d) $p = 11$; $q = 13$, $d = 11$; $M = 7$

e) $p = 17$; $q = 31$, $d = 7$; $M = 2$. *Sugerencia*: el descifrado no es tan difícil como se piensa; utilice alguna sutileza.

18.6. En un sistema de clave pública utilizando RSA, intercepta el texto cifrado $C = 10$ enviado a un usuario cuya clave pública es $e = 5$, $n = 35$. ¿Cuál es el texto nativo M?

18.7. En un sistema RSA, la clave pública de un usuario dado es $e = 31$, $n = 3.599$. ¿Cuál es la clave privada de este usuario?

18.8. Suponga que se tiene un conjunto de bloques codificado con el algoritmo RSA y que no se tiene la clave privada. Suponga que $n = pq$, e es la clave pública. Suponga también que alguien comenta que conoce que uno de los bloques de texto nativo tiene un factor común con n. ¿Puede esto ayudar de alguna forma?

18.9. Muestre como RSA se puede representar por las matrices **M**1, **M**2 y **M**3 del Problema 18.4.

18.10. Considere el siguiente esquema:

1. Elija un número impar, E.
2. Elija dos números primos, P y Q, donde $(P - 1)(Q - 1) - 1$ es divisible por E de modo uniforme.
3. Multiplique P y Q para obtener N.
4. Calcule $D = \dfrac{(P - 1)(Q - 1)(E - 1) + 1}{E}$.

¿Es equivalente este esquema a RSA? Muestre por qué sí o por qué no.

18.11. Considere la utilización de RSA con una clave conocida para construir una función de dispersión de un solo sentido. Después, procese un mensaje constituido por una secuencia de bloques como sigue: cifre el primer bloque, realice la operación XOR entre el resultado y el segundo bloque y cífrelo de nuevo, etc. Muestre que este esquema no es seguro mediante la resolución del siguiente problema. Dado un mensaje de dos bloques, B1 y B2, y su función de dispersión:

$$\text{RSAH(B1, B2)} = \text{RSA(RSA(B1)} \oplus \text{B2)}$$

Dado un bloque arbitrario C1, elija C2 para que RSAH(C1, C2) = RSAH(B1, B2).

CAPÍTULO 19

Aplicaciones distribuidas

- La Notación Sintáctica Abstracta Uno es un lenguaje y una notación importante utilizada en muchos estándares de red de las capas superiores. ASN.1 (Abstract Syntax Notation One) se puede utilizar para definir formatos de protocolos y la estructura y semántica de las bases de datos.
- El protocolo más utilizado mundialmente para la transmisión de correo electrónico es SMTP. SMTP supone que el contenido del mensaje es un bloque de texto simple. El estándar reciente MIME amplía SMTP para permitir la transmisión de información multimedia.
- El esquema estandarizado más importante para permitir aplicaciones de gestión de red es el Protocolo de Gestión de Red Sencillo (SNMP, Simple Network Management Protocol). La versión original de SNMP está disponible en una serie amplia de productos y es utilizado mundialmente. SNMPv2 contiene una serie de mejoras funcionales sobre SNMP y está reemplazándolo. SNMPv3 proporcionada características de seguridad que se añaden a SNMPv2.
- El rápido crecimiento en la utilización de la Web se debe a la estandarización de todos los elementos que permiten las aplicaciones Web. Un elemento clave es HTTP, que es el protocolo para el intercambio de información basada en la Web entre los navegadores Web y los servidores Web.

Todos los protocolos y funciones descritos hasta ahora en la Parte V están orientados hacia un objetivo: dar soporte a las aplicaciones distribuidas que suponen la interacción de múltiples sistemas independientes. En el modelo OSI, estas aplicaciones ocupan la capa de aplicación y reciben el soporte de la capa de presentación. En el conjunto de protocolos TCP/IP, tales aplicaciones se apoyan en TCP o UDP.

Comenzamos este capítulo con una introducción a la Notación Sintáctica Abstracta Uno (ASN.1) que ha llegado a ser un lenguaje universal importante para definir las representaciones de estructuras de datos y los formatos de los protocolos, y que ha logrado una gran difusión para la definición de protocolos del nivel de aplicación. A continuación, se examinan varias aplicaciones bastantes diferentes que dan al lector una idea del rango y diversidad de las aplicaciones soportadas por una arquitectura de comunicaciones. La primera, gestión de red, es una aplicación soporte, diseñada para asegurar la monitorización efectiva y el control de un sistema distribuido. El protocolo específico que se examina es el protocolo sencillo de gestión de red (SNMP), que está diseñado para operar tanto en entornos TCP/IP como OSI. A continuación, se consideran las aplicaciones de correo electrónico, con los estándares SMTP y MIME como ejemplos; SMTP proporciona el servicio básico de correo electrónico, mientras que MIME incorpora capacidades multimedia a SMTP. Finalmente, se examina HTTP, que es la aplicación soporte sobre la que opera el «*world wide web*» (WWW). La Figura 19.1 muestra la posición de estos protocolos dentro del conjunto de protocolos TCP/IP.

19.1. NOTACIÓN SINTÁCTICA ABSTRACTA UNO (ASN.1)

ASN.1 se utiliza ampliamente en el desarrollo de normalizaciones relacionadas con OSI y con TCP/IP. Se utiliza para definir el formato de las unidades de datos del protocolo (PDU), la representación de la información distribuida y las operaciones realizadas con los datos transmitidos. Una comprensión básica de ASN.1 es esencial para aquellos que desean estudiar y trabajar en este campo.

Antes de examinar los detalles de ASN.1, necesitamos introducir el concepto de sintaxis abstracta. Después, examinaremos lo fundamental de ASN.1.

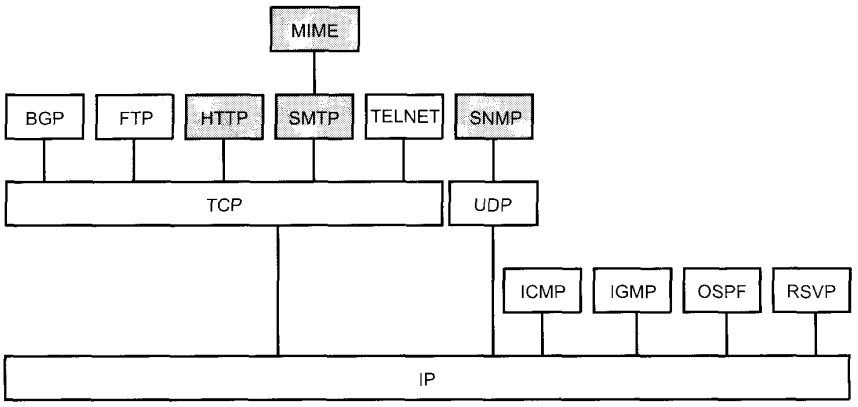


Figura 19.1. *Protocolos del nivel de aplicación en su contexto.*

SINTAXIS ABSTRACTA

La Tabla 19.1 define algunos términos claves que son relevantes en una discusión de ASN.1 y la Figura 19.2 muestra los conceptos subyacentes.

Para los objetivos de esta discusión, se puede considerar que una arquitectura de comunicaciones en un sistema final tiene dos componentes principales. La componente transferencia de datos está relacionada con los mecanismos de transferencia de datos entre sistemas finales. En el caso de la familia de protocolos TCP/IP, este componente está integrado por los elementos de TCP o UDP y los protocolos de capas más bajas. En el caso de la arquitectura OSI, estaría formado por la capa de sesión hacia abajo. El componente de aplicación es el usuario del componente de transferencia de datos y está relacionado con la aplicación del usuario final. En el caso del conjunto de protocolos TCP/IP, este componente es una aplicación tal como SNMP, FTP, SMTP o TELNET. En el caso de la arquitectura OSI, el componente consiste en la capa de aplicación, que está compuesta de una serie de elementos de servicio de aplicaciones, y la capa de presentación.

Tabla 19.1. Términos relevantes de ASN.1.

Sintaxis abstracta	Describe la estructura genérica de los datos independientemente de cualquier técnica de codificación utilizada para representar los datos. La sintaxis permite que se definan tipos de datos y valores de aquellos tipos que se van a especificar.
Tipo de datos	Un conjunto con nombre de valores. Un tipo puede ser simple, que se define especificando el conjunto de sus valores, o estructurado, que se define en términos de otros tipos.
Codificación	La secuencia completa de octetos utilizados para representar un valor de un dato.
Reglas de codificación	Una especificación de la traducción de una sintaxis a otra. Concretando, las reglas de codificación determinan algorítmicamente, para cualquier conjunto de valores de datos definidos en la sintaxis abstracta, la representación de aquellos valores en una sintaxis de transferencia.
Sintaxis de transferencia	Las forma en la que los datos se representan realmente en términos de *patrones de bits mientras están en tránsito entre entidades de presentación.*

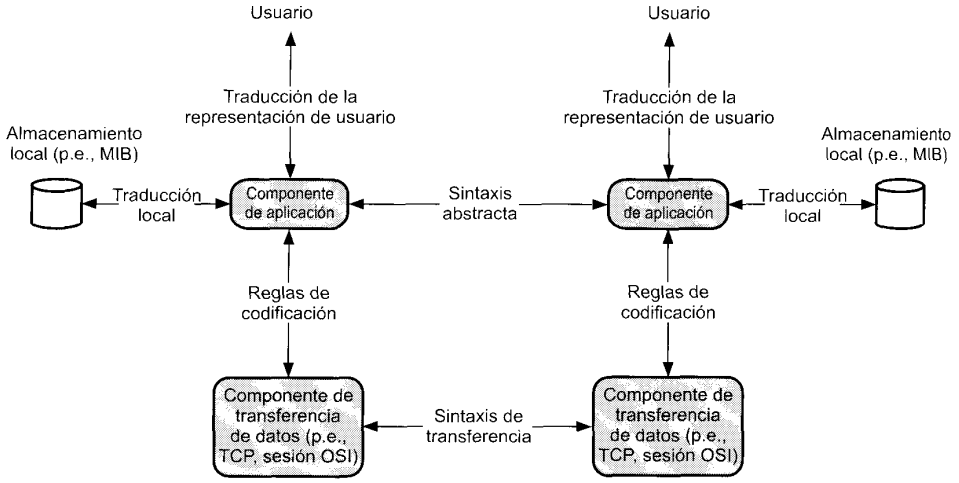


Figura 19.2. El uso de las sintaxis abstracta y de transferencia.

Conforme cruzamos el límite entre el componente de aplicación y el de transferencia, existe un cambio significativo en la forma en que se ven los datos. Para el componente de transferencia de datos, los datos recibidos de una aplicación se especifican como el valor binario de una secuencia de octetos. Este valor binario se puede ensamblar directamente en unidades de datos de servicio (SDU) para transferirlos entre capas y en unidades de datos de protocolo (PDU) para transferirlos entre entidades de protocolo dentro de una capa. El componente de aplicación, sin embargo, está relacionado con la visión de los datos que tiene un usuario. En general, este punto de vista corresponde a un conjunto estructurado de información, como un texto en un documento, un fichero personal, una base de datos integrada, o una presentación visual de información en imágenes. El usuario está relacionado principalmente con la semántica de los datos. El componente de aplicación debe proporcionar una representación de estos datos que se puedan convertir en valores binarios; esto es, debe estar relacionado con la sintaxis de los datos.

El enfoque mostrado en la Figura 19.2 para dar soporte a los datos de aplicación es como sigue. Para el componente de aplicación, la información se representa en una sintaxis abstracta que trata con tipos de datos y valores de los datos. La sintaxis abstracta especifica formalmente los datos independientemente de cualquier representación especifica. Así, una sintaxis abstracta tiene muchas similitudes con los aspectos de definición de los tipos de datos de los lenguajes de programación convencionales, como Pascal, C y Ada, y de las gramáticas como la descrita con la Forma Backus-Naur (BNF). Los protocolos de aplicación describen sus PDU en términos de una sintaxis abstracta.

Esta sintaxis abstracta se utiliza para el intercambio de información entre componentes de aplicaciones en sistemas diferentes. El intercambio se efectúa con PDU del nivel de aplicación, que contienen información de control del protocolo y datos de usuario. Dentro de un sistema, la información representada utilizando sintaxis abstracta se debe traducir en alguna forma de representación para el usuario humano. De igual forma, esta sintaxis abstracta se debe traducir en algún formato local para su almacenamiento. Por ejemplo, este tipo de traducción se utiliza en el caso de la información de gestión de red. Además, está llegando a ser común el uso de la sintaxis abstracta para definir los elementos de los datos en el almacenamiento local. Así, la notación sintáctica abstracta la utilizan los usuarios para definir la información de gestión de red; la aplicación debe entonces convertir esta definición en una forma conveniente para el almacenamiento local.

El componente debe también traducir entre la sintaxis abstracta de la aplicación y una sintaxis de transferencia que describa los valores de los datos en una forma binaria, adecuada para la interacción

con el componente de transferencia de datos. Por ejemplo, una sintaxis abstracta puede incluir un tipo de dato carácter; la sintaxis de transferencia podría especificar IRA o EBCDIC para la codificación.

La sintaxis de transferencia define así la representación de los datos que se van a intercambiar entre componentes de transferencia de datos. La traducción de la sintaxis abstracta a la sintaxis de transferencia se realiza por medio de reglas que especifican la representación de cada valor de los datos de cada tipo de datos.

Este enfoque para el intercambio de datos de aplicación resuelve dos problemas relacionados con la representación de datos en entornos distribuidos y heterogéneos.

- Existe una representación común para el intercambio de datos entre sistemas diferentes.
- Con respecto a la parte interna de un sistema, una aplicación utiliza alguna representación particular de los datos. El esquema de sintaxis abstracta de transferencia resuelve automáticamente la diferencias entre las representaciones de entidades de aplicación cooperantes.

El requisito fundamental para la selección de una sintaxis de transferencia es que permita la correspondiente sintaxis abstracta. Además, la sintaxis de transferencia puede tener otros atributos que no están relacionados con las sintaxis abstractas que puede soportar. Por ejemplo, una sintaxis abstracta se puede soportar por una de las cuatro sintaxis de transferencia, que son iguales en todos los aspectos excepto en que una proporciona compresión de datos, otra encriptado, otra ambas y la última ninguna. La elección de la sintaxis de transferencia que se va a utilizar depende de consideraciones de coste y seguridad.

CONCEPTOS DE ASN.1

El bloque básico de construcción de una especificación ASN.1 es el módulo. Comenzamos esta sección examinando el nivel más alto de la estructura del módulo. Después, se introducen algunas convenciones lexicográficas utilizadas en las definiciones ASN.1. A continuación se describen los tipos de datos definidos en ASN.1. Finalmente, de dan ejemplos del uso de ASN.1.

Definición de módulos

ASN.1 es un lenguaje que puede ser utilizado para definir estructuras de datos. La definición de una estructura se hace asignando un nombre al módulo. El nombre del módulo se puede utilizar después para referenciar la estructura. Por ejemplo, el nombre del módulo se puede utilizar como un nombre sintáctico abstracto; una aplicación puede pasar este nombre al servicio de presentación para especificar la sintaxis abstracta de las PDU de la aplicación que ésta desea intercambiar con una entidad de aplicación paritaria.

Los módulos tienen la siguiente forma:

```
⟨referencia-de-módulo⟩ DEFINITIONS :: =
 BEGIN
   EXPORTS
   IMPORTS
   Lista de asignación
 End
```

El rótulo «referencia-de-módulo» es un nombre de módulo seguido opcionalmente por un identificador de objeto para identificar el módulo. La construcción EXPORTS indica que definiciones de este módulo se pueden importar por otros módulos. La construcción IMPORTS indica definiciones de tipos y de valores de otros módulos que se van a importar en este módulo. Ni la construcción IMPORTS ni la EXPORTS pueden ser incluidas a menos que el identificador de objeto del módulo esté incluido. Finalmente, la «Lista-de-asignación» contiene asignaciones de tipo, asignaciones de valores y definiciones de

macro. Las definiciones de macro se discuten después en esta sección. Las asignaciones de tipo y de valores tienen la forma:

⟨nombre⟩ :: = ⟨descripción⟩

La forma más fácil de describir la sintaxis es con un ejemplo. Primero, necesitamos especificar algunas convenciones léxicas.

Convenciones léxicas

Las estructuras, los tipos y los valores de ASN.1 se expresan en una notación similar a la de un lenguaje de programación. Las convenciones léxicas que se siguen son:

1. La disposición no es importante; los espacios múltiples y las líneas en blanco se consideran como un único espacio.
2. Los comentarios están delimitados por un par de guiones (--) al comienzo y al final del comentario o por un par de guiones al comienzo del comentario y el final de la línea actúa como fin del comentario.
3. Los identificadores (nombres de valores y campos), las referencias de tipo (nombres de tipos) y los nombres de módulo constan de letras mayúsculas, minúsculas, dígitos y guiones.
4. Un identificador comienza por una letra minúscula.
5. Una referencia de tipo o un nombre de módulo comienza con un letra mayúscula.
6. Un tipo interior consta de letras, todas mayúsculas. Un tipo interior es un tipo comúnmente utilizado para él que se proporciona una notación normalizada.

Tipos de datos abstractos

ASN.1 es una notación para tipos de datos abstractos y sus valores. Un tipo se puede ver como una colección de valores. El número de valores que puede tomar un tipo puede ser infinito. Por ejemplo, el tipo INTEGER tiene un número infinito de valores.

Podemos clasificar los tipos en cuatro categorías:

- **Sencillo:** son tipos atómicos sin componentes.
- **Estructurado:** un tipo estructurado tienen componentes.
- **Marcado («tagged»):** estos tipos son derivados de otros tipos.
- **Otro:** esta categoría incluye los tipos CHOICE y ANY, discutidos posteriormente en esta sección.

Cada tipo de datos ASN.1, con excepción de CHOICE y ANY, tiene asociado una marca. La marca consta de un nombre de clase y un número de marca entero no negativo. Existen cuatro clases de tipos de datos, o cuatro clases de marcas:

- **Universal:** tipos independientes de la aplicación y de los mecanismos de construcción generalmente útiles en cualquier contexto; éstos se incluyen en el estándar y se muestran en la Tabla 19.2.
- **Aplicación amplia:** relevantes en aplicaciones particulares; éstos están definidos en otros estándares.
- **Específico del contexto:** también relevantes para aplicaciones particulares pero aplicables en un contexto limitado.
- **Privado:** tipos definidos por usuarios que no se encuentran en ningún estándar.

Un tipo de datos está identificado únicamente por su marca. Los tipos de ASN.1 son los mismos si y sólamente si sus números de marca son los mismos. Por ejemplo, UNIVERSAL 4 se refiere a OctetString, que es de la clase UNIVERSAL y tiene número de marca 4 dentro de la clase.

Tabla 19.2. Asignación de etiquetas de clase universal

Etiqueta	Nombre de tipo	Conjunto de valores
	Tipos básicos	
UNIVERSAL 1	Boolean	VERDADERO o FALSO
UNIVERSAL 2	Integer	El conjunto completo de número positivos y negativo, incluyendo el cero.
UNIVERSAL 3	Bit String	Una secuencia de cero o más bits.
UNIVERSAL 4	Octel String	Una secuencia de cero o más octetos.
UNIVERSAL 9	Real	Números reales.
UNIVERSAL 10	Enumerated	Una lista explícita de valores de enteros que pueden tomar una representación de tipo de datos.
	Tipos de objetos	
UNIVERSAL 6	Object Identifier	El conjunto de valores asociados con objetos de información.
UNIVERSAL 7	Object Descriptor	Cada valor es texto legible por una persona proporcionando una breve descripción de un objeto de información.
	Tipos de cadenas de caracteres	
UNIVERSAL 18	NumericString	Dígitos de 0 a 9, espacio.
UNIVERSAL 19	PrintableString	Caracteres imprimibles.
UNIVERSAL 20	TeletexString	Conjunto de caracteres definidos en la Recomendación T.61 de la CCITT.
UNIVERSAL 21	VideotexString	Conjunto de caracteres del alfabeto y gráficos definidos en Recomendación T.100 y T.101 de la CCITT.
UNIVERSAL 22	IA5String	*Alfabeto Internacional Cinco (equivalente a ASCII).*
UNIVERSAL 25	GraphicString	Conjunto de Caracteres definidos en ISO 8824.
UNIVERSAL 26	VisibleString	Conjunto de Caracteres definidos en ISO 646 (equivalente a ASCII).
UNIVERSAL 27	GeneralString	Cadena de caracteres general.
	Tipos misceláneos	
UNIVERSAL 5	NULL	El valor NULL. Utilizado comúnmente donde son posibles varias alternativas pero ninguna de ellas se aplica.
UNIVERSAL 8	EXTERNAL	Un tipo definido en algún documento externo. No necesita ser uno de los tipos ASN.1 válidos.
UNIVERSAL 23	UTCTime	Consta de la fecha, especificada con un año de dos dígitos, un mes de dos dígitos y un día de dos dígitos, seguido por la hora, especificada por las horas, minutos y opcionalmente por los segundos, seguido por una especificación opcional de la hora local diferente de la hora universal.
UNIVERSAL 24	Generalized Time	Consta de la fecha, especificada con un año de cuatro dígitos, un mes *de dos dígitos y un día de dos dígitos, seguido por la hora, especificada* por las horas, minutos y opcionalmente por los segundos, seguido por una especificación opcional de la hora local diferente de la hora universal.
UNIVERSAL 11-15	Reserved	Reservado para adendas al estándar ASN.1.
UNIVERSAL 28-	Reserved	Reservado para adendas al estándar ASN.1.
	Tipos de estructuras	
UNIVERSAL 16	SEQUENCE y SEQUENCE OF	SECUENCIA: definida haciendo referencia a una lista ordenada y fija de tipos; cada valor es una lista ordenada de valores, uno de cada tipo de componente. SECUENCIA DE: definida haciendo referencia a un único tipo existente; cada valor es una lista ordenada de cero o más valores del tipo existente.
UNIVERSAL 17	SET y SET OF	CONJUNTO: definido haciendo referencia a una lista no ordenada y fija de tipos; algunos de los cuales se pueden declarar opcionales; cada valor *es una lista no ordenada de valores, uno de cada tipo de componente.* CONJUNTO DE: definido haciendo referencia a un único tipo existente; cada valor es una lista no ordenada cero o más valores del tipo existente.

Un **tipo sencillo** es uno definido especificando directamente el conjunto de sus valores. Se pueden considerar estos tipos como tipos atómicos; todos los otros tipos están constituidos de tipos sencillos. Los tipos de datos sencillos en la clase UNIVERSAL se pueden agrupar en varias categorías, como se indica en la Tabla 19.2; éstas no son categorías «establecidas» en el estándar pero se utilizan aquí por conveniencia.

Al primer grupo de los tipos sencillos, a falta de un término mejor, se le puede denominar tipo básico. El tipo Boolean está claro. El tipo Integer es el conjunto de los enteros positivos y negativos y el cero. Además, se pueden asignar nombres a valores individuales de enteros para indicar un significado especial. El tipo BitString es un conjunto ordenado de cero o más bits; se pueden asignar nombres individuales a los bits. El valor real de un BitString se puede especificar como una cadena de dígitos binarios o hexadecimales. De igual forma, un tipo OctetString se puede especificar como una cadena de dígitos binarios o hexadecimales. El tipo de datos Real consta de números expresados en notación científica (mantisa, base, exponente); esto es:

$$M \times B^E$$

La mantisa (M) y el exponente (E) pueden tomar cualquier valor entero, positivo o negativo; se suele utilizar como base (B) los valores 2 o 10.

Finalmente, el tipo Enumerado consiste en una lista explícitamente enumerada de enteros, junto con un nombre asociado a cada entero. La misma funcionalidad se puede obtener con el tipo Integer dando nombre a algunos de los valores enteros; pero, debido a la utilidad de esta característica, se ha definido un tipo separado. Obsérvese, sin embargo, que aunque los valores de un tipo enumerado son enteros, no tienen una semántica entera. Esto es, no se pueden realizar operaciones aritméticas con los valores enumerados.

Los tipos de objetos se utilizan para nombrar y describir los objetos de información. Algunos ejemplos de objetos de información son documentos normalizados, sintaxis abstractas o de transferencia, estructuras de datos y objetos gestionados. En general, un objeto de información es una clase de información (por ejemplo, un formato de fichero) en lugar de un ejemplo de tal clase (por ejemplo, un fichero individual). El identificador de Objeto es un identificador único para un objeto particular. Su valor consiste en una secuencia de enteros. El conjunto de objetos definidos tiene una estructura en árbol, siendo la raíz de ese árbol el objeto referente al estándar ASN.1. Comenzando con la raíz del árbol identificador de objetos, cada valor de componente del identificador de objeto identifica un arco en el árbol. El descriptor Object es una descripción legible por un humano de un objeto de información.

ASN.1 define una serie de tipos de cadenas de caracteres. El valor de cada uno de estos tipos consta de una secuencia de cero o más caracteres elegidos de entre conjunto de caracteres normalizados.

Existen algunos tipos misceláneos que también se han definido en la clase UNIVERSAL. El tipo Null se utiliza para posiciones de las estructuras donde un valor puede o no puede estar presente. El tipo Null es simplemente la alternativa de que no esté presente un valor en esa posición en la estructura. Un tipo External es uno cuyos valores no están especificados en el estándar ASN.1; está definido en otro documento o estándar y se pueden definir utilizando una notación bien definida. UTCTime y GeneralizedTime son dos formatos diferentes para expresar el tiempo. En ambos casos se puede especificar un tiempo local o universal.

Los **tipos estructurados** son aquellos que consisten de componentes. ASN.1 proporciona cuatro tipos estructurados para construir tipos de datos complejos a partir de tipos de datos sencillos:

- SEQUENCE
- SEQUENCE OF
- SET
- SET OF

Los tipos SEQUENCE («secuencia») y SEQUENCE OF («secuencia de») se utilizan para definir una lista ordenada de valores de uno o más tipos de datos. Esto es análogo a la estructura registro de

muchos lenguajes de programación, como COBOL. Un tipo Sequence consta de una lista ordenada de elementos, cada uno especificando un tipo y, opcionalmente, un nombre. La notación para definir el tipo Sequence es como sigue:

```
SequenceType ::= SEQUENCE {ElementTypeList} | SEQUENCE { }
ElementTypeList ::= ElementType | ElementTypeList, ElementType
ElementType ::=
  NamedType                    |
  NamedType OPTIONAL           |
  NamedType DEFAULT Value      |
  COMPONENTS OF Type
```

donde la barra vertical indica una alternativa.

Un NamedType («tipodenominado») es una referencia de tipo con o sin nombre. Cada definición de elemento puede ser seguida por la palabra clave OPTIONAL («opcional») o DEFAULT («implícito»). La clave OPTIONAL indica que el elemento componente no necesita estar presente en un valor de secuencia. La clave DEFAULT indica que, si el elemento componente no está presente, entonces será asignado el valor especificado por la cláusula DEFAULT. La cláusula COMPONENT OF («compuesto de») se utiliza para definir la inclusión, en ese punto de la ElementTypeList («lista de tipos de elementos»), de todas las secuencias de ElementType que aparecen en el tipo referenciado.

Un tipo SEQUENCE OF consta de un número variable de elementos ordenados, todos del mismo tipo. Una definición de SEQUENCE OF tiene la siguiente forma:

```
SequenceOfType ::= SEQUENCE OF Type | SEQUENCE
```

La notación SEQUENCE se debe interpretar como SEQUENCE OF ANY («secuencia cualquièra»); el tipo ANY («cualquiera») se explicará en una subsección posterior.

Un tipo Set («conjunto») es similar a Sequence, excepto que el orden de los elementos no es significativo; los elementos pueden estar agrupados en cualquier orden cuando se codifican en una representación específica. Una definición de Set tiene la siguiente forma:

```
SetType ::= SET {ElementTypeList} | SET { }
```

Así, un tipo Set puede incluir cláusulas opcionales, implícitas y de componentes.

Un tipo SET OF («conjunto de») es un número variable de elementos desordenados, todos de un tipo. Una definición de SET OF tiene la siguiente forma:

```
SetOfType ::= SET OF Type | SET
```

La notación SET se tiene que interpretar como SET OF ANY; el tipo ANY se explica en una subsección posterior.

El término **tipo tagged** (tipo marca) es de alguna forma sin nombre ya que todos los tipos de datos en ASN.1 tienen asociado una marca. El estándar ASN.1 define un tipo marca como sigue:

> *Un tipo definido para referenciar un tipo existente y una marca; el nuevo tipo es isomórfico al tipo existente,* pero es una forma distinta. En todos los esquemas de codificación un valor del tipo nuevo se puede distinguir de un valor del tipo antiguo.

La acción de marcar es útil para distinguir tipos dentro de una aplicación. Puede ser deseable tener varios nombres de tipos diferentes, como nombre_empleado y nombre_cliente que son esencialmente del mismo tipo. Para algunas estructuras, es necesario marcar para distinguir tipos de componentes dentro del tipo estructura. Por ejemplo, a los componentes opcionales de un tipo SET o SEQUENCE se les da normalmente marcas específicas de contexto distintas para evitar las ambigüedades.

Existen dos categorías de tipos de marcas: tipos de marcas implícitas y tipos de marcas explícitas. Un tipo de marca implícita se deriva de otro tipo *reemplazando* la marca (nombre de marca antiguo,

número de marca antiguo) de un tipo antiguo con una marca nueva (nombre de marca nueva, número de marca nuevo). Por motivos de codificación sólo se utilizan las marcas nuevas.

Un tipo de marca explícito se deriva de otro tipo *incorporando* una nueva marca al tipo subyacente. En efecto, un tipo de marca explícito es un tipo de estructura con un componente, el tipo subyacente. Por motivos de codificación, tanto la marca nueva como la antigua se deben reflejar en la codificación.

Una marca implícita da lugar a una codificación más corta, pero puede ser necesaria una marca explícita para evitar ambigüedades si la marca del tipo subyacente está indeterminada (por ejemplo, si el tipo subyacente es CHOICE o ANY).

Los tipos **CHOICE («elección»)** y **ANY («cualquiera»)** son tipos de datos sin marcas. La razón para esto es que cuando se asigna un valor particular al tipo, entonces se debe asignar un tipo particular al mismo tiempo. Así, el tipo se asigna durante la ejecución.

El tipo CHOICE es una lista de tipos alternativos conocidos. Sólo uno de estos tipos será realmente utilizado al crear un valor. Ya se indicó antes que un tipo se puede ver como una colección de valores. El tipo CHOICE es la unión de conjuntos de valores de todos los tipos de componentes indicados en el tipo CHOICE. Este tipo es útil cuando los valores que se van a describir pueden ser de tipos diferentes dependiendo de las circunstancias, y todos los tipos posibles se conocen por adelantado.

La notación para definir el tipo CHOICE es como sigue:

ChoiceType ::= CHOICE {AlternativeTypeList}
AlternativeTypeList ::= NamedType | AlternativeTypeList, NamedType

El tipo ANY describe un valor arbitrario de un tipo arbitrario. La notación es sencillamente:

AnyType ::= ANY

Este tipo es útil cuando los valores que se van a describir pueden ser de tipos diferentes pero los tipos posibles no son conocidos por adelantado.

Subtipos

Un subtipo se deriva de un tipo padre restringiendo el conjunto de valores definidos para un tipo padre. Esto es, el conjunto de valores para el subtipo es un subconjunto del conjunto de valores para el tipo padre. El proceso de crear un subtipo se puede ampliar a más de un nivel: esto es, un subtipo puede ser él mismo, el padre e incluso un subtipo más reducido.

En el estándar se proporcionan seis formas diferentes de notación para designar los valores de un subtipo. La Tabla 19.3 muestra cuáles de estas formas se pueden aplicar a tipos particulares de padres. El resto de esta subsección proporciona una descripción general de cada uno de ellos.

Un **subtipo de valor único** es un listado explícito de todos los valores que el subtipo puede tomar. Por ejemplo:

Primos menores ::= INTEGER (2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29)

En este caso, Primos-menores es un subtipo del tipo interior INTEGER. Otro ejemplo:

Meses ::= ENUMERATED enero (1),
febrero (2),
marzo (3),
abril (4),
mayo (5),
junio (6),
julio (7),
agosto (8),

Tabla 19.3. Aplicabilidad de los conjuntos de valores de subtipo.

Tipo (o derivado de tal tipo mediante marcado)	Valor único	Subtipo contenido	Rango de valor	Restricción de tamaño	Alfabeto permitido	Subtipo interno
Boolean	✔	✔				
Integer	✔	✔	✔			
Enumerated	✔	✔				
Real	✔	✔	✔			
Object Identifier	✔	✔				
Bit String	✔	✔		✔		
Octel String	✔	✔		✔		
Character String Types	✔	✔		✔	✔	
Sequence	✔	✔				✔
Sequence Of	✔	✔		✔		✔
Set	✔	✔				✔
Set Of	✔	✔		✔		✔
Any	✔	✔				
Choice	✔	✔				✔

septiembre (9),
octubre (10),
noviembre (11),
diciembre (12)

Primer-cuatrimestre ::= Meses (enero | febrero | marzo)
Segundo-cuatrimestre ::= Meses (abril | mayo | junio)

Primer-cuatrimestre y Segundo-cuatrimestre son ambos subtipos del tipo enumerado Meses.

Un **subtipo contained** (contenido) se utiliza para formar nuevos subtipos a partir de subtipos existentes. El subtipo contenido incluye todos los valores de los subtipos que él contiene. Por ejemplo:

Primera-mitad ::= Meses (INCLUDES Primer-cuatrimestre | INCLUDES Segundo-cuatrimestre)

Un subtipo contenido puede también incluir un listado de valores explícitos.

Primer-trimestre ::= Meses (INCLUDES Primer-cuatrimestre | abril)

Un **subtipo value range** (de rango de valor) se aplica sólo a los tipos INTEGER y REAL. Se especifica dando los valores numéricos de los extremos del rango. Se pueden utilizar los valores especiales PLUS-INFINITY («más infinito») y MINUS INFINITY («menos infinito»). Los valores especiales MIN y MAX se pueden utilizar para indicar los valores permitidos máximos y mínimos del padre. Cada ex-

tremo del rango está abierto o cerrado. Cuando está abierto, la especificación del punto final incluye el símbolo 'menor que' («<»). Las definiciones siguientes son equivalentes:

```
EnteroPositivo ::= INTEGER (0<..PLUS-INFINITY)
EnteroPositivo ::= INTEGER (1..PLUS-INFINITY)
EnteroPositivo ::= INTEGER (0<..MAX)
EnteroPositivo ::= INTEGER (1..MAX)
```

Las siguientes líneas son equivalentes:

```
EnteroNegativo ::= INTEGER (MINUS-INFINITY..<0)
EnteroNegativo ::= INTEGER (MINUS-INFINITY..-1)
EnteroNegativo ::= INTEGER (MIN..<0)
EnteroNegativo ::= INTEGER (MIN..-1)
```

La **restricción de alfabeto permitido** sólo se puede aplicar a los tipos de cadenas de caracteres. Un tipo de alfabeto permitido consta de todos los valores (cadenas) que se pueden construir utilizando un sub-alfabeto del tipo padre. Ejemplos:

```
Teclas de Tono ::= IA5String (FROM
  ("0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9" | "*" | "#"))
Cadena de Dígitos ::= IA5String (FROM
("0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"))
```

Una **restricción de tamaño** limita el número de artículos en un tipo. Sólo se puede aplicar a tipos de cadena (cadena de bit, cadena de octetos, cadena de caracteres) y a tipos SEQUENCE OF y SET OF. Los artículos que están restringidos dependen del tipo padre como sigue:

Tipo	**Unidad de medida**
cadena de bit	bit
cadena de octetos	octeto
cadena de caracteres	carácter
Sequence-of	valor de componente
Set-of	valor de componente

Como ejemplo de tipo de cadena numérica, la Recomendación X.121 especifica que los números internacionales, que se utilizan para direccionamiento de sistemas finales en redes de datos públicas, incluyendo las redes X.25, deben de constar de al menos 5 dígitos pero no más de 14 dígitos. Esto se podría especificar como sigue:

```
DatoNumérico—itl ::= DigitString (SIZE (5..14))
```

Ahora considere una lista de parámetros para un mensaje que puede incluir hasta doce parámetros:

```
Lista-de-parámetros ::= SET SIZE (0..12) OF Parámetros
```

Una **restricción de tipo interno** se puede aplicar a los tipos SEQUENCE, SEQUENCE OF, SET, SET OF y CHOICE. Un subtipo interno incluye en su conjunto de valores sólo aquellos valores del tipo padre que satisfacen una o más restricciones y/o valores de los componentes del tipo padre. Éste es un subtipo más bien complejo y sólo se dan aquí unos pocos ejemplos.

Considérese una unidad de datos de protocolo (PDU) que puede tener cuatro campos diferentes, sin ningún orden particular:

```
PDU ::= SET alpha [0] INTEGER,
  beta [1] IA5String OPTIONAL
```

gamma [2] SEQUENCE OF Parámetros,
delta [3] BOOLEAN

La especificación de un test que requiere que Boolean sea falso y el Integer sea negativo puede realizarse así:

TestPDU ::= PDU (WITH COMPONENTS {..., delta (FALSE), alpha
(MIN..<0)})

Para especificar además que el parámetro beta esté presente y con una longitud de 5 o 12 caracteres se utiliza la siguiente línea:

FurtherTestPDU ::= TestPDU (WITH COMPONENTS {..., beta (SIZE
(5 | 12) PRESENT})

Como otro ejemplo, considere el uso de un subtipo interior en una construcción SEQUENCE OF:

Bloque-texto ::= SEQUENCE OF VisibleString
Dirección :: = Bloque-texto (SIZE (1..6) | WITH COMPONENTS (SIZE (1..32)))

Este texto indica que la dirección consta de 1 a 6 bloques de texto, y que cada bloque de texto tiene una longitud de 1 a 32 caracteres.

Ejemplo de PDU

Como ejemplo, considere la especificación ASN.1 del formato de las unidades de datos de protocolo para el protocolo SNMPv2 (descrito más tarde en este capítulo). La especificación del estándar se reproduce en la Figura 19.3.

```
SNMPv2-PDU DEFINITIONS ::= BEGIN

PDUs ::= CHOICE { obtener petición              GetRequest-PDU
                  obtener-siguiente-petición    GetNextRequest-PDU
                  obtener-grupo-petición        GetBulkRequest-PDU
                  respuesta                     Response-PDU
                  establecer-petición           SetRequest-PDU
                  informar-petición             InformRequest-PDU
                  snmp V2-trap                  SNMPv2-Trap-PDU
                  informe                       Report-PDU        }

--PDUs

GetRequest-PDU      ::=   [0] IMPLICIT PDU
GetNextRequest-PDU  ::=   [1] IMPLICIT PDU
Response-PDU        ::=   [2] IMPLICIT PDU
SetRequest-PDU      ::=   [3] IMPLICIT PDU
GetBulkRequest-PDU  ::=   [5] IMPLICIT BulkPDU
InformRequest-PDU   ::=   [6] IMPLICIT PDU
SNMPv2-Trap-PDU     ::=   [7] IMPLICIT PDU

max-variable_colección  INTEGER ::= 2147483647
```

Figura 19.3. Definiciones de formato de PDU de SNMPv2 (página 1 de 2).

```
PDU ::= SEQUENCE { identificador-solicitud  Integer32,
                   categoría-error          INTEGER {              --ignorado a veces
                                            noError (0),
                                            tooBig (1),
                                            noSuchName (2),        --para compatibilidad de representante
                                            badValue (3),          --para compatibilidad de representante
                                            readOnly (4),          --para compatibilidad de representante
                                            genError (5),
                                            noAccess (6),
                                            wrongType (7),
                                            wrongLength (8),
                                            wrongEncoding (9),
                                            wrongValue (10),
                                            noCreation (11),
                                            inconsistentValue (12),
                                            resourceUnavailable (13),
                                            commitFailed (14),
                                            undoFailed (15),
                                            authorizationError (16),
                                            notWritable (17),
                                            inconsistentName (18)  },
                   índice-error  INTEGER (0..max-variable-colección), --ignorado a veces
                   variable-colección  VarBindList  }                 --los valores son a veces
                                                                      --ignorados

BulkPDU ::= SEQUENCE  {                                --Debe ser idéntico en estructura a PDU
                   identificador-solicitud  Integer32,
                   no repetidor             INTEGER (0..max-variable-colección),
                   repeticiones = max.      INTEGER (0..max-variable-colección),
                   variable-colección       VarBindList  }        --los valores son ignorados

--variable colección

VarBind ::= SEQUENCE {nombre  ObjectName,
                   CHOICE  {valor           ObjectSyntax,
                                            unspecified    NULL, --en solicitudes de recuperación
                                                                 --excepciones en respuestas:
                                            noSuchObject [0]        IMPLICIT NULL,
                                            noSuchInstance [1]      IMPLICIT NULL,
                                            endOfMibView [2]        IMPLICIT NULL  } }
--lista variable-colección

VarBindList ::= SEQUENCE (SIZE  (0..max-variable-colección)) OF VarBind

END
```

Figura 19.3. Definiciones de formato de PDU de SNMPv2 (página 2 de 2).

La construcción del nivel más alto utiliza el tipo CHOICE para describir una variable seleccionada de una colección. Así, cualquier ejemplar del tipo PDU será uno de los ocho tipos alternativos. Obsérvese que cada una de las elecciones se etiqueta con un nombre. Todos las PDU definidas de esta forma tienen el mismo formato pero diferentes etiquetas, con la excepción de la PDU GetBulkRequest. El formato consta de una secuencia de cuatro elementos. El segundo elemento, es todo de error, enumera 19 valores enteros posibles, cada uno con una etiqueta. En el último elemento, se define la variable co-

lección (*binding*) con sintaxis VarBindList, que se define más adelante en el mismo conjunto de definiciones.

La definición BulkPDU es también una secuencia de cuatro elementos, pero difieren de las otras PDU.

VarBindList está definida como una construcción SEQUENCE OF consistente en algún número de elementos de sintaxis VarBind, con una restricción de tamaño de hasta 2147483647, o $2^{31} - 1$, elementos. Cada elemento a su vez es una secuencia de dos valores; el primero es un nombre y el segundo es una elección entre cinco elementos.

19.2. GESTIÓN DE RED—SNMP

Las redes y los sistemas de procesamiento distribuido son de una importancia crítica y creciente en los negocios, gobierno y otras instituciones. Dentro de una institución, la tendencia es hacia redes más grandes, más complejas y dando soporte a más aplicaciones y a más usuarios. A medida que estas redes crecen en escala, existen dos hechos que se hacen penosamente evidentes:

- La red y sus recursos asociados y las aplicaciones distribuidas llegan a ser indispensables para la organización.
- Hay más cosas que pueden ir mal, inutilizar la red o una parte de ella o degradar las prestaciones a un nivel inaceptable.

Una red grande no se puede instalar y gestionar sólo con el esfuerzo humano. La complejidad de un sistema tal impone el uso de herramientas automáticas de gestión de red. La urgencia de la necesidad de esas herramientas se incrementa, y también está en auge la dificultad de suministrar dichas herramientas, si la red incluye equipos de múltiples distribuidores. En respuesta, se han desarrollado normalizaciones para tratar la gestión de red, y que cubren los servicios, los protocolos y la base de información de gestión.

Esta sección comienza con una introducción a los conceptos globales de gestión de red normalizada. El resto de la sección se dedica a la discusión de SNMP, el estándar de gestión de red más utilizado.

SISTEMAS DE GESTIÓN DE RED

Un sistema de gestión de red es una colección de herramientas para monitorizar y controlar la red y que está integrado en los siguientes sentidos:

- Una interfaz de operador sencilla con un conjunto de órdenes potentes, pero agradables para el usuario, para llevar cabo la mayoría o todas las tareas de gestión de red.
- Una cantidad mínima de equipo separado del sistema de gestión. Esto es, la mayor parte del hardware y el software requeridos para la gestión de red están incorporados en el equipo del usuario.

Un sistema de gestión de red consta de hardware extra y software adicional implementados entre los componentes de red existentes. El software se utiliza para efectuar las tareas de gestión de red que residen en los computadores y en los procesadores de comunicaciones (por ejemplo, procesadores frontales y controladores de grupos de terminales). Un sistema de gestión de red está diseñado para ver la red entera como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y los atributos específicos de cada elemento y enlace del sistema conocidos. Los elementos activos de la red proporcionan una realimentación regular de información de estado al centro de control de red.

Un sistema de gestión de red tiene los siguientes elementos clave:

- Estación de gestión o gestor.

- Agente.
- Base de información de gestión.
- Protocolo de gestión de red.

La estación de gestión es normalmente un dispositivo autónomo pero puede ser implementado en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz entre el gestor de red humano y el sistema de gestión de red. La estación de gestión, tendrá, como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de los datos, recuperación de fallos, etc.
- Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.
- La capacidad de trasladar los requisitos del gestor de red a la monitorización y control real de los elementos en la red.
- Una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

El otro elemento activo en un sistema de gestión de red es el **agente**. Las plataformas claves, como los computadores, puentes, dispositivos de encaminamiento y concentradores se pueden equipar con software de agente para que puedan ser gestionados desde la estación de gestión. El agente responde a las solicitudes de información desde una estación de gestión, responde a las solicitudes de acción desde la estación de gestión y puede, de una forma asíncrona, proporcionar a la estación de gestión información importante y no solicitada.

El medio por el cual se pueden gestionar los recursos de una red es representando estos recursos como objetos. Cada objeto es, esencialmente, una variable de datos que representa un aspecto del agente de gestión. La colección de objetos se conoce como **base de información de gestión** (MIB, Management Information Base). La MIB funciona como una colección de puntos de accesos al agente por parte de la estación de gestión. Estos objetos están normalizados a través de los sistemas de una clase particular (por ejemplo, todos los puentes contienen los mismos objetos de gestión). La estación de gestión lleva a cabo la función de monitorización mediante el acceso a los valores de los objetos MIB. Una estación de gestión puede causar que una acción tenga efecto en un agente o puede cambiar la configuración de un agente mediante la modificación de los valores de variables específicas.

La estación de gestión y el agente están enlazados por el **protocolo de gestión de red.** El protocolo utilizado para la gestión en redes TCP/IP es el protocolo sencillo de gestión de red (SNMP). Para las redes basadas en OSI, se está desarrollando el protocolo de información de gestión común (CMIP, Common Management Information Protocol). Una versión mejorada de SNMP, conocida como SNMPv2, está proyectada para ambos tipos de redes, basadas en OSI y basadas en TCP/IP. Cada uno de estos protocolos incluye las siguientes capacidades clave:

- **Get:** permite a la estación de gestión obtener del agente los valores de objetos.
- **Set:** permite a la estación de gestión establecer valores de objetos del agente.
- **Notify:** permite a un agente notificar a una estación de gestión la producción de eventos significativos.

En un esquema tradicional de gestión de red centralizado, un computador en la configuración tiene el papel de estación de gestión; puede haber posiblemente una o dos estaciones de gestión con una misión de respaldo. El resto de los dispositivos en la red contiene software de agente y una MIB para permitir la monitorización y control por parte de la estación de gestión. Conforme las redes crecen en tamaño y en carga de tráfico, un sistema centralizado como el indicado no es práctico. Hay demasiada carga situada en la estación de gestión, y hay también mucho tráfico, con informes desde cada agente atravesando la red entera hasta llegar al «cuartel general». En tales circunstancias, una técnica descentralizada y distribuida funciona de mejor forma (por ejemplo, Figura 19.4). En un esquema descentraliza-

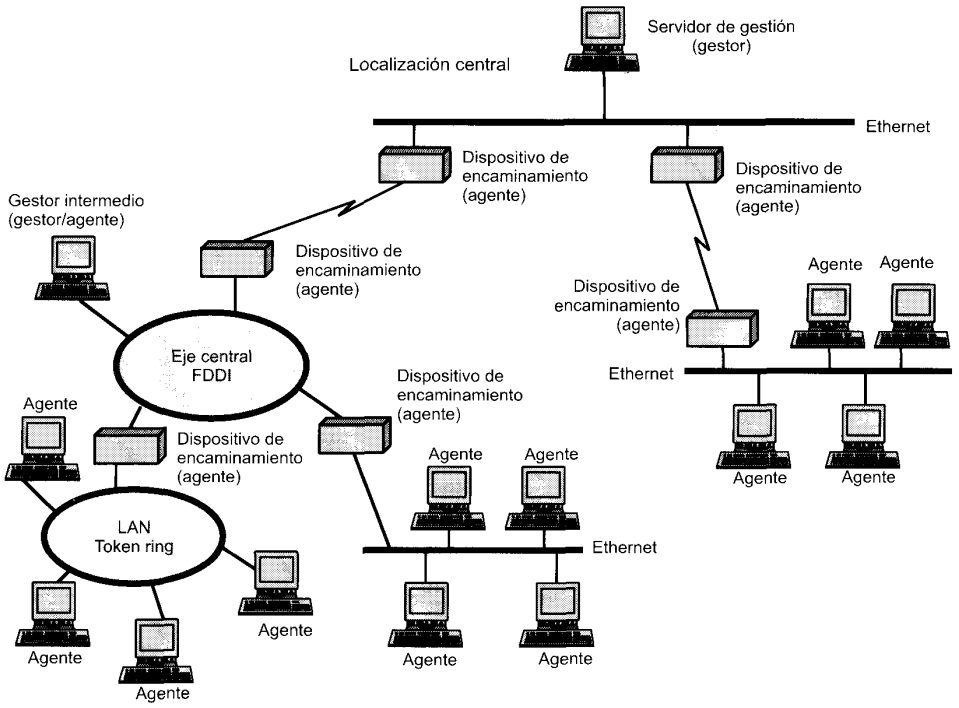


Figura 19.4. Ejemplo de configuración de gestión de una red distribuida.

do de gestión de red, puede haber múltiples estaciones de gestión del nivel más alto, que se podrían denominar servidores de gestión. Cada uno de estos servidores podría gestionar directamente una parte del conjunto total de agentes. Sin embargo, para muchos de estos agentes, el servidor de gestión delega la responsabilidad a un gestor intermedio. El gestor intermedio juega el papel de un gestor para monitorizar y controlar los agentes bajo su responsabilidad. También juega el papel de agente para proporcionar información y aceptar control desde un servidor de gestión de un nivel más alto. Este tipo de arquitectura dispersa la carga de procesamiento y reduce al tráfico total de la red.

PROTOCOLO SIMPLE DE GESTIÓN DE RED VERSIÓN 2 (SNMPv2)

En agosto de 1988, se publicó la especificación SNMP y rápidamente se convirtió en el estándar de gestión de red dominante. Una serie de suministradores ofrecen estaciones de trabajo de gestión de red basadas en SNMP y la mayoría de los vendedores de puentes, dispositivos de encaminamiento, estaciones de trabajo y PC ofrecen paquetes de agente SNMP que permiten que sus productos sean gestionados por una estación de gestión SNMP.

Como el nombre sugiere, SNMP es una herramienta sencilla para la gestión de red. Define una base de información de gestión (MIB) limitada y fácil de implementar de variables escalares y tablas de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB y para permitir a un agente emitir notificaciones no solicitadas, llamadas intercepciones (*traps*). Esta simplicidad es la potencia de SNMP. SNMP se implementa de una forma fácil y consume un tiempo modesto del procesador y de recursos de red. También, la estructura del protocolo y de la MIB es suficientemente directa de forma que no es difícil alcanzar la interacción entre estaciones de gestión y software de agente de varios vendedores.

Con una utilización tan amplia, las deficiencias de SNMP han llegado a ser bastante aparentes; éstas incluyen deficiencias funcionales y la falta de una herramienta de seguridad. Como resultado en 1993 se publicó una versión mejorada, conocida como SNMPv2, y en 1996 se publicó una versión revisada (RFC 1901 a 1908). SNMPv2 ganó rápidamente apoyos y una serie de distribuidores anunciaron productos unos meses después de la publicación del estándar.

Los elementos de SNMPv2

Sorprendentemente, SNMPv2 no proporciona gestión de red. En lugar de eso SNMPv2 proporciona un marco de trabajo en el que se pueden construir aplicaciones de gestión de red. Estas aplicaciones, como la gestión de fallos, monitorización del rendimiento, contabilización de tiempo, etc. están fuera del ámbito del estándar.

Lo que proporciona SNMPv2 es la infraestructura de la gestión de red. La Figura 19.5 es un ejemplo de una configuración que muestra esta infraestructura.

La esencia de SNMPv2 es un protocolo que se utiliza para intercambiar información de gestión. Cada «jugador» en un sistema de gestión de red mantiene una base de datos local de información relevante de gestión de red, conocida como base de información de gestión (MIB). El estándar SNMPv2 define la

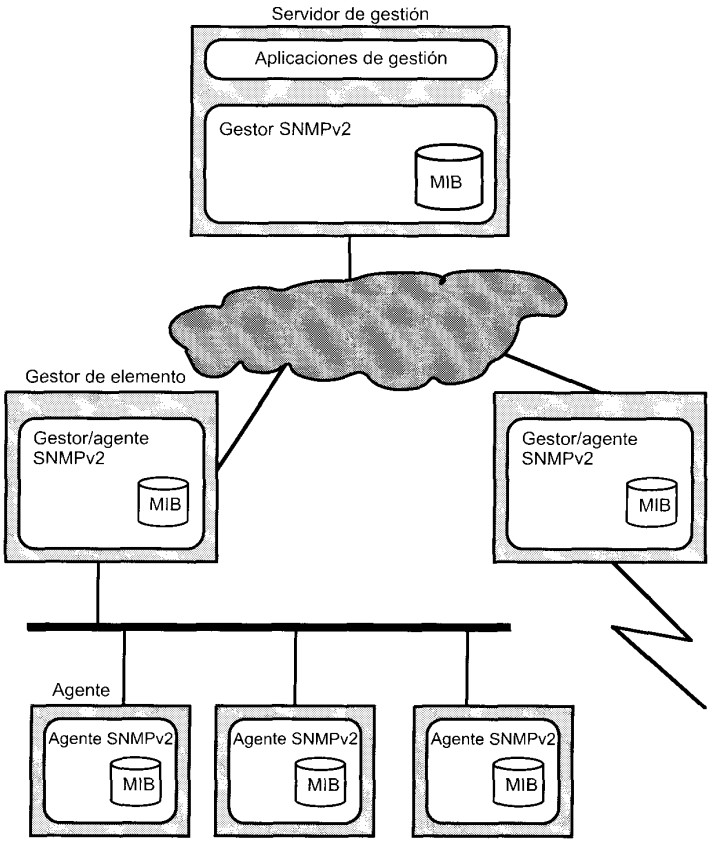


Figura 19.5. Configuración gestionada por SNMPv2.

estructura de esta información y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI, Structure of Management Information). Podemos pensar que esto constituye el lenguaje para definir la información de gestión. El estándar también proporciona varias MIB que son generalmente útiles para la gestión de red[1]. Además los vendedores y los grupos de usuarios pueden definir nuevas MIB.

Al menos un sistema de la configuración debe ser responsable de la gestión de red. Es aquí donde se debe instalar cualquier aplicación de gestión de red. Debería de haber más de una de estas estaciones de gestión, para proporcionar redundancia o simplemente dividir las obligaciones en una red grande. La mayoría del resto de los sistemas actúan con un papel de agente. Un agente recoge información localmente y la almacena para accesos posteriores de un gestor. La información incluye datos sobre el mismo sistema y también pueden incluir información del tráfico de la red o redes a las que está conectado el agente.

SNMPv2 dará apoyo a una estrategia de gestión de red altamente centralizada o distribuida. En este último caso, algunos sistemas operan con el papel de gestor y el de agente. En su papel de agente, un sistema aceptará órdenes de un sistema de gestión superior. Algunas de estas órdenes están relacionadas con la MIB local en el agente. Otras órdenes requieren que el agente actúe como delegado para dispositivos remotos. En este caso, el agente delegado asume el papel de gestor para acceder a información en un agente remoto, y después asume el papel de agente para pasar esa información a un gestor superior.

Todos estos intercambios se realizan utilizando el protocolo SNMPv2, que es un protocolo sencillo del tipo petición/respuesta. Normalmente, se implementa encima del protocolo de datagrama de usuario (UDP), que es parte del conjunto de protocolos TCP/IP. Ya que los intercambios SNMPv2 son del tipo de pares solicitud-respuesta discretos, no se requiere una conexión segura.

Estructura de la información de gestión

La estructura de la información de gestión (SMI) define el marco de trabajo general dentro del que se puede definir y construir la MIB. La SMI identifica los tipos de datos que se pueden utilizar en la MIB y cómo se pueden representar y nombrar los recursos dentro de la MIB. La filosofía que subyace en la SMI es animar la simplicidad y la amplitud dentro de una MIB. Así, la MIB puede almacenar solamente tipos de datos sencillos: escalares y matrices de dos dimensiones de escalares, llamadas tablas. La SMI no permite la creación o la recuperación de estructuras de datos complejas. Esta filosofía es la contraria a la utilizada en los sistemas de gestión de OSI, que proporciona estructuras de datos y modos de recuperación complejos para permitir una funcionalidad mayor. SMI evita los tipos y estructuras de datos complejos para simplificar la tarea de la implementación y mejorar la interoperabilidad. Las MIB inevitablemente contendrán tipos de datos creados por el vendedor y, a menos que se impongan fuertes restricciones en la definición de tales tipos de datos, la interoperabilidad se verá afectada.

Existen realmente tres elementos claves en la especificación de la SMI. En el nivel más bajo, la SMI especifica los tipos de datos que se pueden almacenar. Después, la SMI especifica la técnica formal para definir los objetos y tablas de objetos. Finalmente, SMI proporciona un esquema para asociar un identificador único con cada objeto real en un sistema, para que los datos de un agente se puedan referenciar por un gestor.

La Tabla 19.4 muestra los tipos de datos que se permiten por SMI. Éste es un conjunto bastante restringido de tipos. Por ejemplo, los números reales no se permiten. Sin embargo, es lo bastante rico como para permitir la mayoría de los requisitos de la gestión de red.

---

[1] Existe una ligera confusión sobre el término *MIB*. En su forma singular, el término *MIB* se puede utilizar para referirse a la base de datos de información completa tanto en el gestor como en el agente. También se puede utilizar en su forma singular o plural para referirse a una colección específica definida de información de gestión que forma parte de una MIB global. Así, el estándar SNMPv2 incluye la definición de varias MIB e incorpora, por referencia, MIB definidas en SNMPv1.

Tabla 19.4. Tipos de datos permitidos en SNMPv2.

Tipo de dato	Descripción
INTEGER	Enteros en el rango de -2^{31} a $2^{31} - 1$.
UInteger32	Enteros en el rango de 0 a $2^{32} - 1$.
Counter32	Un entero no negativo que se puede incrementar módulo 2^{32}.
Counter64	Un entero no negativo que se puede incrementar módulo 2^{64}.
Gauge32	Un entero no negativo que se puede incrementar o decrementar, pero que no excederá un valor máximo. El valor máximo no puede ser mayor que $2^{32} - 1$.
TimeTicks	Un entero no negativo que representa el tiempo, módulo 2^{32}, en centésimas de segundo.
OCTET STRING	Cadena de octetos para datos arbitrarios binarios o textuales; puede estar limitado a 255 caracteres.
IpAddress	Una dirección Internet de 32 bits.
Opaque	Un campo de bits arbitrario.
BIT STRING	Una enumeración de bits con nombre.
OBJECT IDENTIFIER	Nombre asignado administrativamente a objetos u otros elementos normalizados. El valor es una secuencia de hasta 128 enteros no negativos.

Funcionamiento del protocolo

El corazón del entorno de trabajo de SNMPv2 es el protocolo mismo. El protocolo proporciona un mecanismo básico y directo para intercambiar información de gestión entre un gestor y un agente.

La unidad básica de intercambio es el mensaje, que consta de un envoltorio de mensaje exterior y una unidad de datos de protocolo interior (PDU). La cabecera de mensaje exterior está relacionada con la seguridad y se discute posteriormente en esta sección.

Se pueden transmitir siete tipos de PDU en un mensaje SNMP. El formato general de éstos se muestra informalmente en la Figura 19.6; la definición formal ASN.1 se dio en la Figura 19.3. Existen varios campos que son comunes a varias PDU. El campo identificativo de solicitud es un entero asignado de forma que las solicitudes que se produzcan se identifiquen de forma única. Esto permite que un gestor relacione las respuestas de entrada con las solicitudes de salida. También permite que un agente trate el problema de dos o más PDU duplicadas generadas por un servicio de transporte no seguro. El campo de variable colección contiene una lista que recolecta los identificadores de objetos; dependiendo en el PDU, la lista puede incluir un valor de cada objeto.

El PDU GetRequest, emitido por un gestor, incluye una lista de uno o más nombres de objetos para los que se solicita un valor. Si la operación de obtener valores tiene éxito, el agente que responde enviará un PDU Response. La lista de la variable colección contendrá el identificador y el valor de todos los objetos obtenidos. Para cualquier variable que no es relevante desde el punto de vista de la MIB, se devuelve el identificador y un código de error en la lista de la variable colección. Así, SNMPv2 permite respuestas parciales a un GetRequest, lo que da lugar a una mejora significativa con respecto a SNMP. En SNMP, si una o más variables en GetRequest no se permiten, el agente devuelve un mensaje de error con un estado de noSuchName. Para poder tratar estos errores, el gestor SNMP no debe devolver valores a la aplicación solicitante o debe incluir un algoritmo que responda ante un error eliminando las variables perdidas, reenviando la solicitud, y enviando un resultado parcial a la aplicación.

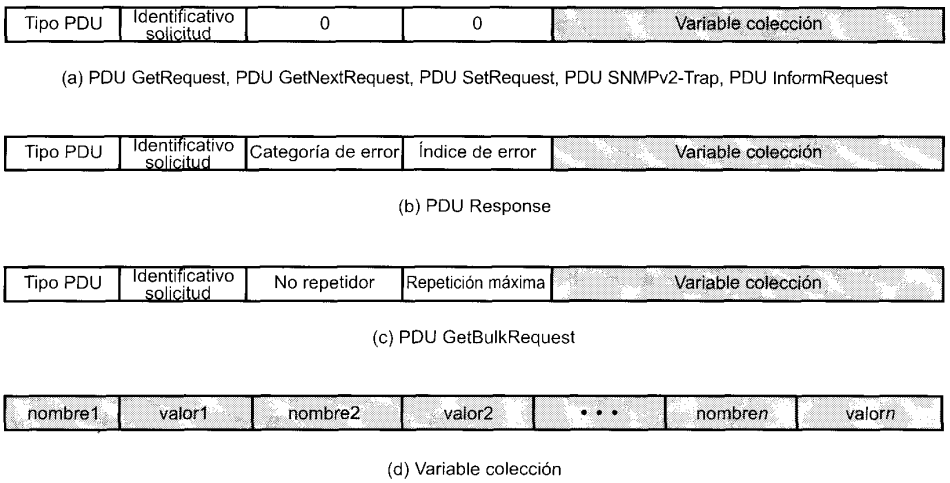


Figura 19.6. Formato de PDU de SNMPv2.

La PDU GetNextRequest también es emitida por un gestor e incluye una lista de uno o más objetos. En este caso, para cada objeto cuyo nombre se encuentra en el campo de la variable colección se devuelve un valor para ese objeto que es el siguiente en orden lexicográfico, lo que es equivalente a decir siguiente en la MIB en términos de su posición en la estructura de árbol de identificadores de objetos. Como con la PDU GetRequest, el agente devuelve valores para tantas variables como le sea posible. Una de las ventajas de la PDU GetNextRequest es que permite a un gestor descubrir la estructura de una MIB dinámicamente. Esto es útil si el gestor no conoce a *priori* el conjunto de objetos que asociados a un agente o que están en una MIB particular.

Una de las principales mejoras proporcionadas por SNMPv2 es la PDU GetBulkResquest. El objetivo de esta PDU es minimizar el número de intercambios de protocolo requeridos para obtener gran cantidad de información de gestión. La PDU GetBulkRequest permite a un gestor SNMPv2 solicitar que la respuesta sea tan grande como sea posible dada la restricción del tamaño del mensaje.

La PDU SetRequest se emite por un gestor para solicitar que el valor de uno o más objetos se modifique. La entidad SNMPv2 que la recibe responde con una PDU Response que contiene el mismo identificador de solicitud. La operación de SetRequest es atómica: o se actualizan todas las variables o ninguna. Si la entidad que responde es capaz de establecer los valores de todas las variables indicadas en la lista entrante de la variable colección, entonces la PDU Response incluye el campo de la variable colección con un valor proporcionado para cada variable. Si al menos uno de los valores de variable no se puede proporcionar, entonces no se devuelven valores ni se actualizan éstas. En este último caso, el código de estado de error indica la razón del fallo y el campo de índice de error indica la variable en la lista de variables colección que causó el fallo.

La PDU de SNMPv2 Trap se genera y transmite por un agente SNMPv2 actuando en su papel de agente cuando ocurre un evento inusual. Se utiliza para proporcionar a la estación de gestión una notificación asíncrona de algún evento significativo. La lista de la variable colección se utiliza para contener la información asociada con el mensaje Trap. A diferencia de GetRequest, GetNestRequest, GetBulkRequest, SetRequest e InformRequest, la PDU SNMPv2 Trap no provoca una respuesta de la entidad que lo recibe; es un mensaje no confirmado.

La PDU InformRequest se envía por una entidad SNMPv2 actuando como gestor, en representación de una aplicación, a otra entidad SNMPv2 en su papel de gestor, para proporcionar información de gestión a una aplicación utilizando la última entidad. Como con la PDU SNMPv2 Trap, la lista de la varia-

ble colección se utiliza para llevar la información asociada. El gestor que recibe una InformRequest las confirma con una PDU Response.

Tanto para Trap como para InformRequest, se pueden definir varias condiciones que indican cuándo se genera la notificación; también se especifica la información que se va a enviar.

PROTOCOLO SENCILLO DE GESTIÓN DE RED VERSIÓN 3 (SNMPv3)

Muchas de las deficiencias funcionales de SNMP se solucionaron en SNMPv2. Para corregir las deficiencias en seguridad de SNMPv1/SNMPv2, se publicó SNMPv3 como un conjunto de Estándares Propuestos en enero de 1998 (actualmente RFC 2570 a 2575). Este conjunto de documentos no proporciona una capacidad SNMP completa si no que define una arquitectura general de SNMP y un conjunto de capacidades en seguridad. Éstas están pensadas para que se utilicen con el SNMPv2 actual.

SNMPv3 proporciona tres servicios importantes: autentificación, privacidad y control de acceso. Los dos primeros forman parte del modelo de Seguridad Basada en Usuarios (USM, User-Based Security) y el último se define en el Modelo de Control de Acceso Basado en Consideraciones (VACM, View-Based Access Control Model). Los servicios de seguridad están gobernados por la identidad del usuario que solicita el servicio; esta identidad se expresa como un director, que puede ser un individuo o una aplicación o un grupos de individuos o aplicaciones.

El mecanismo de autentificación en USM asegura que el mensaje recibido lo transmitió el director cuya identidad aparece como fuente en la cabecera del mensaje. Este mecanismo también asegura que el mensaje no se ha alterado en la transmisión y que no se ha retardado o retransmitido artificialmente. El director que envía proporciona la autentificación mediante la inclusión de un código de autentificación del mensaje con el mensaje SNMP que envía. Este código es una función del contenido del mensaje y las identidades del emisor y el receptor. La clave secreta se debe establecer fuera de USM como una función de configuración. Esto es, el gestor de configuración o el gestor de red es responsable de la distribución de la claves secretas que se guardan en las bases de datos de los diferentes gestores y agentes SNMP. Esto se puede hacer de forma manual o utilizando alguna forma de transferencia de datos segura fuera de USM. Cuando el director receptor obtiene un mensaje, utiliza la misma clave secreta para calcular el código de autentificación de mensaje una vez más. Si la versión del código del receptor coincide con el valor añadido al mensaje, entonces el receptor sabe que el mensaje sólo lo puede haber originado el gestor autorizado y que el mensaje no se alteró en el camino. La clave secreta compartida por el emisor y el receptor debe estar preconfigurada. El código de autentificación actual se conoce como HMAC, que es un mecanismo de autentificación estándar de Internet.

El servicio de privacidad de USM habilita a los gestores y a los agentes a encriptar mensajes. De nuevo, el gestor director y el agente director deben compartir una clave secreta. En este caso, si los dos están configurados para utilizar la facilidad de privacidad, todo el tráfico entre ellos es encriptado utilizando el estándar de encriptado de datos (DES). El director que envía encripta el mensaje utilizando el algoritmo DES y su clave secreta y envía el mensaje al director receptor que lo desencripta utilizando el algoritmo DES y la misma clave secreta.

El servicio de control de acceso hace posible configurar los agentes para que proporcionen diferentes niveles de acceso a la base de información de gestión (MIB) del agente a diferentes gestores. Un director agente puede restringir el acceso a su MIB a un director gestor de dos formas. Primero, puede restringir el acceso a cierta porción de su MIB. Por ejemplo, un agente podría restringir a la mayoría de los gestores ver las estadísticas relacionadas con el rendimiento y permitir solamente a un único director gestor designado para ello a ver y actualizar los parámetros de configuración. Segundo, el agente puede limitar las operaciones que un gestor podría utilizar en esa porción de la MIB. Por ejemplo, un director gestor particular podría limitar el acceso de sólo-lectura a una porción de la MIB de un agente. El criterio de control de acceso que utilice un agente para cada gestor se debe preconfigurar y esencialmente consiste en una tabla que detalla los privilegios de acceso de los diferentes gestores autorizados.

19.3. CORREO ELECTRÓNICO—SMTP Y MIME

La aplicación más utilizada virtualmente en cualquier sistema distribuido es el correo electrónico. Desde el primer momento, el protocolo sencillo de transferencia de correo (SMTP, Simple Mail Transfer Protocol) ha sido el caballo de batalla del conjunto de protocolos TCP/IP. Sin embargo, SMTP ha estado tradicionalmente limitado a la distribución de mensajes sencillos de texto. En años recientes, ha habido demandas para que el correo tenga la capacidad de distribuir varios tipos de datos, incluyendo voz, imágenes y «vídeo clips». Para satisfacer estos requisitos se ha definido, sobre la base de SMTP, un nuevo estándar: la ampliación de correo Internet multiobjetivo (MIME, Multi-Purpose Internet Mail Extension). En esta sección se estudia primero el SMTP y después MIME.

PROTOCOLO SENCILLO DE TRANSFERENCIA DE CORREO (SMTP)

SMTP es el protocolo estándar para transferir correo entre computadores en el conjunto de protocolos TCP/IP; está definido en el RFC 821.

Aunque los mensajes transferidos por SMTP normalmente siguen el formato definido en el RFC 822, que se describe más adelante, SMTP no está involucrado ni con el formato ni con el contenido de los mensajes transferidos, con dos excepciones. Se hace referencia a este concepto diciendo que SMTP utiliza información contenida en el «sobre» del correo (cabecera del mensaje), pero no examina el contenido (cuerpo del mensaje) del sobre. Las dos excepciones son las siguientes:

1. SMTP normaliza el conjunto de caracteres del mensaje al conjunto ASCII de 7 bits.
2. SMTP incorpora información al comienzo del mensaje transferido que indica el camino que ha seguido el mensaje.

Funcionamiento básico del correo electrónico

La Figura 19.7 muestra el flujo general de correo en un sistema típico. Aunque gran parte de esta actividad está fuera del ámbito de SMTP, la figura muestra el contexto dentro del que opera normalmente SMTP.

Para empezar, el correo lo crea un programa agente de usuario en respuesta a una entrada de usuario. Cada mensaje creado consta de una cabecera que incluye la dirección de correo electrónico del destino y otra información, y un cuerpo que contiene el mensaje a enviar. Estos mensajes se sitúan de alguna forma en una cola de espera y se pasan como entrada al programa Emisor SMTP, que normalmente es un programa que siempre está presente en el computador.

Aunque la estructura de la cola de salida de correo será diferente dependiendo del sistema operativo del computador, cada mensaje en cola tiene conceptualmente dos partes:

1. El texto del mensaje, que consta de:
   - La cabecera RFC 822: ésta constituye el sobre del mensaje e incluye una indicación del destino o destinos requeridos.
   - El cuerpo del mensaje, compuesto por el usuario.
2. Una lista de destinos de correo.

La lista de destinos de correo del mensaje la obtiene el agente usuario de la cabecera de mensaje 822. En algunos casos, el destino o destinos se especifican literalmente en la cabecera del mensaje. En otros casos, el agente de usuario puede necesitar ampliar los nombres de la lista de correo, eliminar duplicados y reemplazar nombres nemónicos por el nombre real del buzón de correo. Si se solicita cualquier copia textual (BCC, Blind Carbon Copies), el agente usuario necesita preparar copias para cumplir con este requisito. La idea básica es que los formatos y estilos múltiples que utilizan las personas en la interfaz del usuario se reemplacen por una lista normalizada adecuada para el programa de envío SMTP.

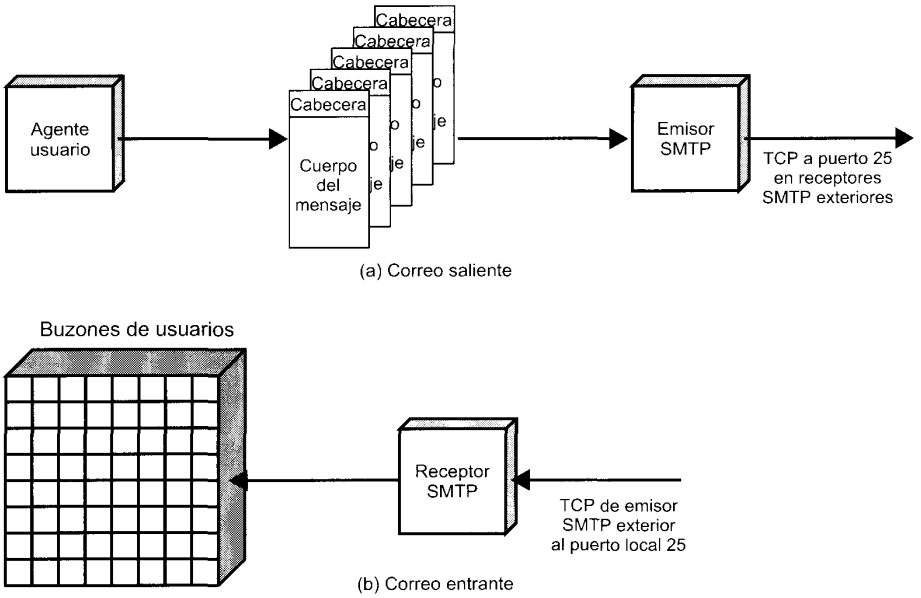


Figura 19.7. Flujo de correo SMTP.

El **programa de envío SMTP** toma los mensajes de la cola de correo de salida y los transmite al computador destino adecuado vía transacciones SMTP a través de una o más conexiones TCP al puerto 25 del computador destino adecuado. Un computador puede tener múltiples programas de envío SMTP activos simultáneamente si tiene una gran cantidad de volumen de correo de salida y también debería tener la capacidad de crear receptores SMTP bajo demanda para que el correo de un computador no produzca retardos en el correo de otro.

Siempre que el emisor SMTP completa la entrega de un mensaje particular a uno o más usuarios en un computador específico, elimina el destino correspondiente de la lista de destinos del mensaje. Cuando se han procesado todos los destinos de un mensaje particular, se elimina el mensaje de la cola. Al procesar la cola, el emisor SMTP puede implementar varias técnicas de optimización. Si un mensaje particular se envía a múltiples usuarios de un único computador, el texto del mensaje sólo se necesita enviar una vez. Si están listos para enviar múltiples mensajes al mismo computador, el emisor SMTP puede abrir una conexión TCP, transferir los múltiples mensajes y cerrar la conexión, en lugar de abrir y cerrar una conexión para cada mensaje.

El emisor SMTP debe prever varios errores. El computador destino puede ser inalcanzable, estar desconectado, o la conexión TCP puede fallar cuando se está realizando la transferencia. El emisor puede volver a poner en cola el correo para realizar la transferencia más tarde, pero renunciando a volver a intentarlo tras un periodo de tiempo determinado en lugar de mantenerlo en la cola indefinidamente. Otro error común es una dirección destino errónea, que puede ocurrir por un error de entrada de usuario o porque el destino deseado tiene una nueva dirección en un computador nuevo. El emisor SMTP debe redirigir el mensaje si es posible o devolver una notificación de error al que originó el mensaje.

El **protocolo SMTP** se utiliza para transferir un mensaje desde un emisor SMTP a un receptor SMTP a través de una conexión TCP. SMTP intenta proporcionar un funcionamiento seguro pero no garantiza recuperar los mensajes perdidos. No se devuelve una confirmación extremo-a-extremo al que origina un mensaje indicando la entrega con éxito del mensaje y tampoco se garantiza una indicación de error. Sin embargo, un sistema de correo basado en SMTP se considera por lo general seguro.

El **receptor SMTP** acepta cada mensaje que llega y lo sitúa en el buzón de correo del usuario adecuado o lo copia en la cola local de correo de salida para reenviarlo si es lo que se solicita. El receptor SMTP debe ser capaz de verificar los destinos locales del correo y tratar los errores, incluyendo los errores de transmisión y la falta de capacidad de disco.

El emisor SMTP es responsable del mensaje hasta el instante en que el receptor SMTP indica que la transferencia se ha completado; sin embargo, esto simplemente significa que el mensaje ha llegado al receptor SMTP, no que el mensaje ha sido entregado y recuperado por el destino deseado. Las responsabilidades del tratamiento de errores por parte del receptor SMTP están generalmente limitadas a renunciar a una conexión TCP que falla o que está inactiva por periodos grandes de tiempo. Así, el emisor tiene la mayor responsabilidad en el tratamiento de los errores. Los errores que se producen cuando se está indicando que la transferencia se ha completado, pueden causar mensaje duplicados pero no su pérdida.

En la mayoría de los casos, los mensajes van directamente desde la máquina que origina el mensaje hasta la máquina destino a través de una única conexión TCP. Sin embargo, ocasionalmente el mensaje puede pasar a través de máquinas intermedias aprovechando la capacidad de reenvío de SMTP, en cuyo caso el mensaje debe atravesar múltiples conexiones TCP entre la fuente y el destino. Una forma por la que ocurre esto se produce en el caso en que el emisor especifica una ruta al destino en forma de una secuencia de servidores. Un evento más común es el reenvío requerido a causa de que un usuario ha cambiado de dirección.

Es importante indicar que el protocolo SMTP se limita a la conversación que tiene lugar entre el emisor SMTP y el receptor SMTP. La función principal de SMTP es la transferencia de mensajes, aunque hay algunas funciones auxiliares para la verificación y tratamiento del destino del correo. El resto del sistema de tratamiento de correo mostrado en la Figura 19.7 está fuera del ámbito de SMTP y puede diferir de un sistema a otro.

Volvamos a la discusión de los elementos principales de SMTP.

Descripción general de SMTP

El funcionamiento de SMTP se realiza por medio de una serie de órdenes y respuestas intercambiadas entre el emisor y receptor SMTP. La iniciativa la lleva el SMTP emisor, que establece la conexión TCP. Una vez que se ha establecido la conexión, el emisor SMTP envía órdenes a través de la conexión al receptor. Cada orden genera exactamente una respuesta del receptor SMTP.

La Tabla 19.5 muestra las **órdenes SMTP**. Cada orden consta de una única línea de texto, comenzando con un código de orden de 4 letras seguido en algunos casos por un campo de argumentos. La mayoría de las respuestas son una única línea, aunque es posible respuestas de líneas múltiples. La tabla indica aquellas órdenes que todos los receptores deben ser capaces de reconocer.

Las **respuestas SMTP** se muestran en la Tabla 19.6. Cada respuesta comienza con un código de tres dígitos y puede ir seguido por información adicional. El primer bit indica la categoría de la respuesta:

- **Respuesta de finalización afirmativa:** la acción solicitada se ha completado satisfactoriamente. Se puede iniciar una nueva solicitud.
- **Respuesta intermedia positiva:** la orden ha sido aceptada pero la acción solicitada está suspendida, pendiente de recibir más información. El emisor SMTP debería enviar otra orden especificando está información. Esta respuesta se utiliza en grupos de secuencias de órdenes.
- **Respuesta de finalización negativa transitoria:** la orden no se aceptó y la acción solicitada no se realizó. Sin embargo, la condición de error es temporal y se puede solicitar la acción de nuevo.
- **Respuesta de finalización negativa permanente:** la orden no se aceptó y la acción solicitada no se realizó.

La operación básica de SMTP ocurre en tres fases: establecimiento de la conexión, intercambio de uno o más pares orden-respuesta, y cierre de la conexión. A continuación se examinan cada una de las fases.

Tabla 19.5. Órdenes SMTP.

Nombre	Formato de la orden	Descripción
HELO	HELO ⟨SP⟩ ⟨dominio⟩ ⟨CRLF⟩	Envía identificación
MAIL	MAIL ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Identifica al que origina el correo
RCPT	RCPT ⟨SP⟩ TO: ⟨camino destino⟩ ⟨CRLF⟩	Identifica al destino del correo
DATA	DATA ⟨CRLF⟩	Transfiere un texto de mensaje
RSET	RSET ⟨CRLF⟩	Aborta la transacción del correo actual
NOOP	NOOP ⟨CRLF⟩	No operación
QUIT	QUIT ⟨CRLF⟩	Cierra la conexión TCP
SEND	SEND ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal
SOML	SOML ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal si es posible; de otro modo al buzón
SAML	SAML ⟨SP⟩ FROM: ⟨camino inverso⟩ ⟨CRLF⟩	Envía correo al terminal y al buzón
VRFY	VRFY ⟨SP⟩ ⟨cadena⟩ ⟨CRLF⟩	Confirma el nombre del usuario
EXPN	EXPN ⟨SP⟩ ⟨cadena⟩ ⟨CRLF⟩	Devuelve el número de miembros de la lista de correo
HELP	HELP [⟨SP⟩ ⟨cadena⟩] ⟨CRLF⟩	Envía documentación específica del sistema
TURN	TURN ⟨CRLF⟩	Intercambia el rol del emisor y el receptor

⟨CRLF⟩ = retorno de carro, fin de línea
⟨SP⟩ = espacio
Los paréntesis cuadrados indican elementos opcionales.
Las órdenes sombreados son opcionales en una implementación que verifique SMTP.

Establecimiento de la conexión

Un emisor SMTP intentará establecer una conexión TCP con un computador destino cuando tiene uno o más mensajes de correo para entregar a ese computador. La secuencia es bastante sencilla:

1. El emisor abre una conexión TCP con el receptor.
2. Una vez que se ha establecido la conexión, el receptor se identifica a sí mismo con «220 Service Ready».
3. El emisor se identifica a sí mismo con la orden HELO.
4. El receptor acepta la identificación del emisor con «250 OK».

Si el servicio de correo no está disponible en el destino, el computador destino devuelve una respuesta «421 Service Not Available» en el paso 2 y finaliza el proceso.

Transferencia de correo

Una vez que se ha establecido la conexión, el emisor SMTP puede enviar uno o más mensajes al receptor SMTP. Hay tres fases lógicas en la transferencia de un mensaje:

1. Una orden MAIL identifica al que originó el mensaje.
2. Una o más órdenes RCPT identifican los destinos de este mensaje.
3. Una orden DATA transfiere el texto del mensaje.

Tabla 19.6. Respuestas SMTP.

Código	Descripción
	Respuesta de finalización positiva
211	Estado del sistema o respuesta de ayuda del sistema.
214	Mensaje de ayuda (información de cómo utilizar el receptor o el significado de una orden particular no estándar; esta respuesta es sólo útil al usuario humano)
220	⟨dominio⟩ Servicio preparado
221	⟨dominio⟩ Servicio cerrando el canal de transmisión
250	Acción de correo solicitada correcta, completada
251	Usuario no local; reenviar a ⟨camino-destino⟩
	Respuesta intermedia positiva
354	Comenzar la entrada de correo; acabar con ⟨CRLF⟩.⟨CRLF⟩
	Respuesta de finalización negativa transitoria
421	⟨dominio⟩ Servicio no disponible; perdido canal de transmisión. (Ésta podría ser la respuesta a cualquier orden si el servicio conoce que debe desconectarse)
450	Acción de correo solicitada no ejecutada; buzón de correo no disponible (p. ej. buzón ocupado)
451	Cancelada acción solicitada; error local en el procesamiento
452	Acción solicitada no ejecutada; almacenamiento del sistema insuficiente
	Respuesta de finalización negativa permanente
500	Error de sintaxis; orden no reconocida (esto puede incluir errores como línea de orden demasiado larga)
501	Error de sintaxis en los parámetros o los argumentos
502	Orden no implementada
503	Secuencia de órdenes incorrecta
504	Parámetro de orden no implementado
550	Acción solicitada no ejecutada; buzón de correo no disponible (p. ej. buzón no encontrado, no se accedió)
551	Usuario no local, por favor, intente ⟨camino-destino⟩
552	Acción de correo solicitada cancelada; excedida la asignación de espacio de almacenamiento
553	Acción solicitada no ejecutada; nombre del buzón de correos no permitido (p. ej. sintaxis de correo incorrecta)
554	Transacción fallida

La **orden MAIL** da el camino inverso que puede utilizarse para informar de errores. Si el receptor está preparado para aceptar mensajes, devuelve una respuesta «250 OK». De otra forma devuelve una respuesta indicando un fallo al ejecutar la orden (códigos 451, 452, 552) o un error en la orden (códigos 421, 500, 501).

La **orden RCPT** identifica un destino individual de los datos del correo; se pueden especificar destinos múltiples mediante el uso múltiple de esta orden. Se devuelve una respuesta separada por cada orden RCPT, con una de las siguientes posibilidades:

1. El receptor acepta el destino con una respuesta «250»; esto indica que ese buzón de correo destino está en el sistema receptor.
2. El destino requiere que se reenvíe y el receptor lo reenviará (251).
3. El destino requiere que se reenvíe pero el receptor no lo reenviará; el emisor debe reenviar a la dirección de reenvío (551).
4. No existe ese buzón de correo para ese destino en este computador (550).
5. El destino se rechaza debido a algún fallo de ejecución (códigos 450, 451, 452, 552) o a un error en la orden (códigos 421, 500, 501, 503).

La ventaja de utilizar fases separadas de RCPT es que el emisor no enviará el mensaje hasta que esté seguro que el receptor está preparado para recibir el mensaje para al menos un destino evitando, por tanto, el tiempo suplementario de enviar un mensaje entero para aprender que el destino es desconocido. Una vez que el receptor SMTP está de acuerdo en recibir el mensaje de correo para al menos un destino, el emisor SMTP utiliza la **orden DATA** para iniciar la transferencia del mensaje. Si el receptor SMTP sigue preparado para recibir el mensaje devuelve un mensaje «354»; de otro modo el receptor devuelve una respuesta indicando un fallo al ejecutar la orden (códigos 451, 554) o un error en la orden (códigos 421, 500, 501, 503). Si se devuelve la respuesta «354», el emisor SMTP procede a enviar el mensaje sobre la conexión TCP como una secuencia de líneas ASCII. El fin del mensaje se indica por una línea que contiene solamente un punto. El receptor SMTP responde con una respuesta «250 OK» si se acepta el mensaje o con el código de error apropiado (451, 452, 552, 554).

El siguiente ejemplo, tomado del RFC 821, muestra el proceso:

S: MAIL FROM: <Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO: <Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO: <Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO: <Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah ...
S: ... etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

El emisor SMTP está transmitiendo correo que se origina en el usuario Smith@Alpha.ARPA. El mensaje va dirigido a tres usuarios en la máquina Beta.ARPA, llamados Jones, Green y Brown. El receptor SMTP indica que tiene buzones de correo para Jones y Brown pero que no tiene información de Green. Ya que al menos uno de los usuarios destino ha sido verificado, el emisor procede a enviar el mensaje de texto.

Cierre de la conexión

El emisor SMTP cierra la conexión en dos pasos. Primero, el emisor envía una orden QUIT y espera una respuesta. El segundo paso es iniciar una operación de cierre TCP para la conexión TCP. El receptor inicia su cierre TCP después de enviar su respuesta en la orden QUIT.

RFC 822

El RFC 822 define un formato para los mensajes de texto que se envían utilizando el correo electrónico. El estándar SMTP adopta el RFC 822 como formato a utilizar en la construcción de mensajes a través SMTP. En el contexto del RFC 822, los mensajes se ven como compuestos de un sobre y un contenido. El sobre contiene cualquier información que sea necesaria para llevar a cabo la transmisión y la entrega. El contenido está compuesto del objeto que se va a entregar al destino. El estándar RFC 822 se aplica solamente al contenido. Sin embargo, el contenido estándar incluye un conjunto de campos de cabecera que se pueden utilizar por el sistema de correo para crear el sobre y el estándar está pensado para facilitar la adquisición de esa información por programas.

Un mensaje 822 consta de una secuencia de líneas de texto, y utiliza un marco de trabajo de notas. Esto es, un mensaje consta de algún número de líneas de cabecera, que siguen un formato rígido, seguido de una parte de cuerpo consistente en texto arbitrario.

Una línea de cabecera normalmente consta de una palabra clave, seguida por dos puntos (:) y el argumento de la palabra clave; el formato permite que una línea larga se rompa en varias líneas. Las palabras claves más frecuentes son From («de»), To («a»), Subject («asunto») y Date («fecha»). Aquí se muestra un ejemplo de mensaje:

```
Date: Tue, 16 Jan 1996 10:37:17 (EST)
From: «William Stalling» <ws@host.com>
Subject: La sintaxis en el RFC 822
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hola. Esta sección constituye el comienzo real del cuerpo del mensaje, que está separado de la cabecera del mensaje por una línea en blanco.
```

Otro campo que se encuentra a menudo en la cabecera RFC 822 es Message-ID. Este campo contiene un identificador único de este mensaje.

AMPLIACIÓN DE CORREO INTERNET MULTIOBJETIVO (MIME)

MIME es una ampliación del marco de trabajo del RFC 822 y está pensada para solventar algunos de los problemas y limitaciones en la utilización de SMTP y el RFC 822 para correo electrónico. [MURP95] indica las siguientes limitaciones del esquema SMTP/822:

1. SMTP no puede transmitir ficheros ejecutables u otros objetos binarios. Se utilizan una serie de esquemas para convertir ficheros binarios a formato texto de forma que se pueda utilizar el sistema de correo de SMTP, incluido el esquema popular de UNIX UUencode/UUdecode. Sin embargo ninguno de estos procedimientos de conversión es un estándar ni siquiera de facto.
2. SMTP no puede transmitir datos de texto que incluyan caracteres de un lenguaje nacional ya que éstos se representan por códigos de 8 bits con valores de 128 decimal o superiores, y SMTP está limitado a caracteres ASCII de 7 bits.
3. Los servidores SMTP pueden rechazar mensajes de correo a partir de un cierto tamaño.
4. Las pasarelas SMTP que traducen de caracteres ASCII a código EBCDIC no utilizan un conjunto consistente de correspondencias, lo que da lugar a problemas de traducción.
5. Las pasarelas SMTP a redes con correo electrónico X.400 no pueden gestionar datos que no son texto y que pueden estar incluidos en los mensajes X.400.
6. Algunas implementaciones no se adhieren completamente al estándar SMTP definido en el RFC 821. Algunos problemas comunes que aparecen son:

- Eliminación, incorporación o reordenamiento de caracteres retorno de carro y de fin de línea.
- Truncar o dividir líneas mayores de 76 caracteres.
- Eliminar espacios finales (caracteres tabuladores o blancos).
- Relleno de líneas en un mensaje para conseguir la misma longitud.
- Conversión de los caracteres tabuladores en múltiples caracteres de espacio.

MIME está pensado para resolver estos problemas de forma que resulte compatible con las implementaciones existentes de RFC 822. La especificación se encuentra en los RFC 2045 a 2049.

Descripción general

Las especificaciones MIME incluyen los siguientes elementos:

1. Se definen cinco campos nuevos de la cabecera del mensaje, que pueden ser incluidos en una cabecera RFC 822. Estos campos proporcionan información sobre el cuerpo del mensaje.
2. Se definen varios formatos de contenido, normalizando así las representaciones que dan soporte al correo electrónico multimedia.
3. Se definen esquemas de codificación de transferencia posibilitando así la conversión de cualquier formato de contenido a un formato que esté protegido por cambios del sistema de correo.

En esta subsección se introducen los cinco campos de cabecera de mensaje. En las dos siguientes se examinan los formatos de contenido y los esquemas de codificación de transferencia.

Los cinco campos de cabecera definidos en MIME son:

- **Versión MIME:** debe tener el valor de parámetro 1.0. Este campo indica que el mensaje cumple con los RFC.
- **Tipo de contenido:** describe los datos contenidos en el cuerpo con suficiente detalle de forma que el agente usuario receptor puede escoger un agente o un mecanismo adecuado para representar los datos al usuario o de otra forma tratar los datos de forma apropiada.
- **Codificación de transferencia del contenido:** indica el tipo de transformación que se ha utilizado para representar el cuerpo del mensaje de una forma aceptable para el transporte del correo.
- **Identificador del contenido:** utilizado para identificar de forma única entidades MIME en múltiples contextos.
- **Descripción del contenido:** una descripción en texto del objeto que acompaña al cuerpo; esto es útil cuando el objeto no se puede leer (por ejemplo, datos de audio).

Todos o alguno de estos campos pueden aparecer en una cabecera RFC 822 normal. Una implementación correcta debe permitir los campos versión MIME, tipo de contenido y codificación de transferencia de contenido; los campos identificador de contenido y descripción de contenido son opcionales y pueden ser ignorados por la implementación destino.

Tipos de contenido MIME

El núcleo de la especificación MIME está relacionado con la definición de varios tipos de contenidos. Esto refleja la necesidad de proporcionar formas normalizadas de tratar una gran variedad de representaciones de información en un entorno multimedia.

La Tabla 19.7 muestra los tipos de contenido especificados en el RFC 1521. Existen siete tipos de contenido principales diferentes y un total de 14 subtipos. En general, un tipo de contenido declara el tipo general de los datos y el subtipo especifica un formato particular para ese tipo de datos.

Para el **tipo texto** de cuerpo no se requiere software especial para obtener el significado completo del texto, aparte de permitir el conjunto de caracteres indicado. El único subtipo definido es texto nati-

Tabla 19.7. Tipos de contenido MIME.

Tipo	Subtipo	Descripción
Texto	Nativo	Texto no formateado; puede ser ASCII o ISO 8859
Multiparte	Mezclado	Las diferentes partes son independientes pero van a ser transmitidas juntas. Se deberían presentar al receptor en el mismo orden en que aparecen en el mensaje de correo.
	Paralelo	Difiere de mezclado solamente en que no se define orden para la entrega de las partes al receptor.
	Alternativo	Las diferentes partes son versiones alternativas de la misma información. Están ordenadas en exactitud creciente al original y el sistema de correo destino debería mostrar la mejor opción al usuario.
	Resumen	Similar a mezclado pero el tipo/subtipo por defecto para cada parte es mensaje/rfc822.
Mensaje	rfc822	El mismo cuerpo es un mensaje encapsulado que cumple con el RFC 822.
	Partial	Utilizado para permitir la fragmentación de correos grandes en una forma que es transparente al destino.
	Cuerpo-externo	Contiene un puntero a un objeto que existe en otra parte.
Imagen	jpeg	La imagen está en formato JPEG, codificación JFIF.
	gif	La imagen está en formato GIF.
Vídeo	mpeg	Formato MPEG.
Audio	Básico	Codificación en ley-mu de un canal único de 8 bits de la RDSI.
Aplicación	Postscript	Postscript de Adobe.
	flujo-octetos	Datos binarios generales consistente de bytes de 8 bits.

vo, que es simplemente una cadena de caracteres ASCII o caracteres ISO 8859. Una versión anterior de la especificación MIME incluía el subtipo *texto enriquecido* que permite una flexibilidad mayor en el formato. Se espera que este subtipo reaparezca en un RFC posterior.

El **tipo multiparte** indica que el cuerpo del mensaje contiene múltiples partes independientes. El campo de cabecera de tipo de contenido incluye un parámetro, llamado límite, que define los delimitadores entre las partes del cuerpo. Este límite no debería de aparecer en ninguna parte del mensaje. Cada límite comienza en una línea nueva y consta de dos guiones seguido por el valor del límite. El límite final, que indica el fin de la última parte, también tiene un sufijo de dos guiones. Dentro de cada parte, puede existir una cabecera opcional MIME ordinaria.

A continuación se muestra un ejemplo de mensaje multiparte, que consiste de dos partes cada una contiene texto simple:

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Subject: Mensaje de muestra
MIME-Version: 1.0
Content-type: multipart/mixed; boundary = «límite simple»
```

Esto es el preámbulo. Va a ser ignorado, aunque es un buen lugar para que los que componen el correo incluyan una nota explicatoria para los lectores que no siguen MIME.
--límite simple

Esto es implícitamente texto escrito ASCII. No termina con una ruptura de línea (*linebreak*).
--límite simple
Content-type: text/plain; charset = us-ascii

Esto es explícitamente texto escrito ASCII. Termina con una ruptura de línea.

--límite simple--
Éste es el epílogo. Va a ser ignorado.

Existen cuatro subtipos del tipo multiparte, que tienen la misma sintaxis general. El **subtipo multiparte/mezclado** se utiliza cuando existen múltiples partes de cuerpo independientes que necesitan estar en un orden particular. Para el **subtipo multiparte/paralelo,** el orden de las partes no es significativo. Si el sistema destino es apropiado, las partes múltiples se pueden presentar en paralelo. Por ejemplo, una parte de texto o imagen se podría acompañar por un comentario verbal que se reproduce cuando se muestra el texto o la imagen.

Para el **subtipo multiparte/alternativo**, las diferentes partes son representaciones diferentes de la misma información. Lo siguiente es un ejemplo:

From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Subject: Correo de texto formateado
MIME-Version: 1.0
Content-type: multipart/alternative; boundary = boundary42

--boundary42

Content-type: text/plain; charset = us-ascii

... el mensaje en versión texto va aquí...
--boundary42
Content-type: text/richtext

... la versión del mismo mensaje en texto enriquecido RFC 1341 va aquí...
--boundary42--

En este subtipo, las partes del cuerpo están ordenadas en términos crecientes de preferencia. Para este ejemplo, si el sistema destino es capaz de mostrar el mensaje en texto enriquecido, lo muestra; en caso contrario se utiliza el formato de texto propiamente dicho.

El **subtipo multiparte/resumen** se utiliza cuando cada parte del cuerpo se interpreta como un mensaje RFC 822 con cabecera. Este subtipo permite la construcción de un mensaje cuyas partes son mensajes individuales. Por ejemplo, el moderador de un grupo podría recoger mensajes de correo electrónico de los participantes, agrupar estos mensajes y enviarlos en un mensaje MIME encapsulado.

El **tipo mensaje** proporciona una serie de capacidades importantes en MIME. El **subtipo mensaje/rfc822** indica que el cuerpo es un mensaje entero, incluyendo cabecera y cuerpo. A pesar del nombre de este subtipo, el mensaje encapsulado puede no ser un mensaje RFC 822 simple, sino cualquier mensaje MIME.

El **subtipo mensaje/parcial** permite la fragmentación de un mensaje grande en varias partes, que se deben reensamblar en el destino. Para este subtipo se especifican tres parámetros en el campo Content-type: Message/Partial:

- **id:** un valor que es común a cada fragmento del mismo mensaje, de forma que se pueden identificar en el destino para poder reensamblarlos, pero que es único para mensajes diferentes.
- **número:** un número de secuencia que indica la posición del fragmento en el mensaje original. El primer fragmento se numera como 1, el segundo como 2, y así hasta el final.
- **total:** el número total de partes. El último fragmento se identifica por tener el mismo valor en los parámetros *número* y *total*.

El **subtipo mensaje/cuerpo-externo** indica que los datos reales que se van a transferir en este mensaje no están contenidos en el cuerpo. En lugar de eso, el cuerpo contiene información necesaria para acceder a los datos. Como con otros tipos de mensaje, el subtipo mensaje/cuerpo-externo tiene una cabecera externa y un mensaje encapsulado con su propia cabecera. El único campo necesario en la cabecera externa es el campo Content-type, que identifica este mensaje como del subtipo mensaje/cuerpo-externo. La cabecera interna es la cabecera del mensaje encapsulado.

El campo Content-type en la cabecera exterior debe incluir un parámetro de tipo de acceso, que tiene uno de los siguientes valores:

- **FTP:** el cuerpo del mensaje está accesible como fichero utilizando el protocolo de transferencia de ficheros (FTP). Para este tipo de acceso, son obligatorios los siguientes parámetros adicionales: *nombre*, el nombre del fichero; y *localización*, el nombre de dominio del computador donde reside el fichero. Los parámetros opcionales son: *directorio*, el directorio donde se sitúa el fichero; y *modo*, que indica como FTP debe recuperar el fichero (por ejemplo, ASCII, imagen). Antes de que tenga lugar la transferencia, el usuario necesita proporcionar un identificador y clave de acceso de usuario. Éstos no se transmiten con el mensaje por razones de seguridad.
- **TFTP:** el cuerpo del mensaje está accesible como fichero utilizando el protocolo trivial de transferencia de ficheros (TFTP). Se utilizan los mismos parámetros que para FTP y, de igual forma, se tiene que proporcionar un identificador y una clave de acceso de usuario.
- **FTP-anonymous:** es idéntico a FTP, excepto que no se solicita el identificador y la clave de acceso al usuario. El parámetro *nombre* proporciona el nombre del fichero.
- **fichero-local:** el cuerpo del mensaje está accesible como fichero en la máquina destino.
- **AFS:** el cuerpo del mensaje está accesible como fichero vía el AFS (*Andrew File System*) global. El parámetro *nombre* proporciona el nombre del fichero.
- **servidor de correo:** el cuerpo del mensaje está accesible enviando un mensaje de correo electrónico a un servidor de correo. El parámetro *servidor* se debe incluir para dar la dirección de correo electrónico del servidor. El cuerpo del mensaje original, conocido como cuerpo imaginario, debería contener la orden exacta que se va a enviar al servidor de correo.

El **tipo imagen** indica que el cuerpo contiene una imagen que se puede visualizar. El subtipo, jpeg o gif, especifica el formato de la imagen. En el futuro, se podrán incorporar más subtipos a esta lista.

El **tipo vídeo** indica que el cuerpo contiene una imagen con figuras que cambian con el tiempo, posiblemente con contenido de color y sonido coordinado. El único tipo especificado hasta ahora es mpeg.

El **tipo audio** indica que el cuerpo contiene datos de audio. El único subtipo, básico, se ajusta a un servicio RDSI conocido como «64 kbps, estructurado a 8 KHz, utilizable para información de voz», con un algoritmo de voz digitalizada conocido como *ley-μ* PCM (modulación por codificación de impulsos, *Pulse Code Modulation*). Este tipo general es la forma típica de transmitir señales de voz a través de una red digital. El término *ley-μ* se refiere a una técnica especifica de codificación; es una técnica estándar que se utiliza en Norteamérica y Japón. En Europa se utiliza el sistema estándar ley-A.

El **tipo aplicación** se refiere a otros tipos de datos, normalmente datos binarios sin interpretación, o información que se va a procesar por una aplicación basada en el correo. El **subtipo aplicación/flujo-de-octetos** indica datos binarios generales en una secuencia de octetos. El RFC 1521 recomienda que la

implementación receptora ofrezca almacenar los datos en un fichero o utilizarlos como entrada a un programa.

El **subtipo aplicación/Postscript** indica el uso de Postscript de Adobe.

Codificación de transferencia de MIME

El otro componente principal de la especificación MIME, además de la especificación del tipo de contenido, es la definición de la codificación de transferencia de los cuerpos de los mensajes. El objetivo es proporcionar una entrega segura a través del rango más grande de entornos.

El estándar MIME define dos métodos para codificar los datos. El campo Content-Transfer-Encoding en realidad puede tomar seis valores, mostrados en la Tabla 19.8. Sin embargo, tres de estos valores (7bit, 8bit y binario) indican que no se ha realizado codificación, pero proporciona alguna información sobre la naturaleza de los datos. Para la transferencia SMTP, es seguro utilizar la forma 7bit. Las formas 8bit y binaria se pueden utilizar en otros contextos de transporte de correo. Otro valor de Content-Transfer-Encoding es x-token, que indica que se utiliza algún otro esquema de codificación del que se proporcionará el nombre. Éste podría ser un esquema específico del vendedor o de una aplicación específica. Los dos esquemas de codificación reales definidos son imprimible textualmente (*quoted-printable*) y base64. Los dos esquemas se definen para proporcionar una elección entre una técnica de transferencia que es esencialmente legible por las personas y una que es segura para todos los tipos de datos en una forma razonablemente compacta.

La codificación de transferencia imprimible textualmente es útil cuando los datos son en buena parte octetos que corresponden a caracteres ASCII imprimibles (véase Tabla 3.1). En esencia, representa caracteres no seguros por medio de la representación hexadecimal de sus códigos e introduce rupturas de líneas reversibles (suaves) para limitar las líneas del mensaje a 76 caracteres. Las reglas de codificación son las siguientes:

1. Representación general de 8 bits: esta regla se va a utilizar cuando no se aplica ninguna de las otras reglas. Cualquier carácter se representa por un signo igual seguido por la representación hexadecimal de dos dígitos del valor del octeto. Por ejemplo, el carácter de cambio de línea ASCII, que tiene un valor de 8 bits decimal de 12 se representa por «=0C».
2. Representación literal: cualquier carácter en el rango decimal de 33 («!») hasta 126 («~»), excepto el decimal 61 («=»), se representa por ese carácter ASCII.
3. Espacio en blanco: los octetos con valor 9 y 32 se pueden representar como los caracteres ASCII tabulador y espacio, respectivamente, excepto al final de la línea. Cualquier espacio en blanco (tabulador o en blanco) al final de una línea se debe representar según la regla 1. Al decodifi-

Tabla 19.8. Codificación de transferencia MIME.

7 bit	Todos los datos se representan por líneas cortas de caracteres ASCII.
8 bit	Las líneas son cortas, pero podría haber caracteres no ASCII (octetos con el bit de orden más alto establecido).
Binario	A parte de que están presentes caracteres no ASCII, las líneas no son lo suficientemente cortas para el transporte SMTP.
Imprimible textualmente	Codifica los datos de tal forma que si la mayoría de los datos que se codifican son texto ASCII, el texto codificado permanece en gran medida reconocible por los usuarios humanos.
base64	Codifica los datos convirtiendo bloques de 6 bits en bloques de 8 bits, todos ellos caracteres ASCII imprimibles.
x-token	Una codificación no estándar.

car, se elimina cualquier espacio en blanco al final de la línea. Esto elimina cualquier espacio en blanco incorporado por agentes de transporte intermedios.

4. Ruptura de línea: cualquier ruptura de línea, independientemente de su representación inicial, se representa por la ruptura de línea del RFC 822, que es la combinación retorno de carro/cambio de línea.
5. Ruptura de línea suave: si una línea codificada va a tener una longitud mayor que 76 caracteres (excluyendo <CRLF>), se debe insertar una ruptura de línea suave antes o en la posición 75. Una ruptura de línea suave consiste en la secuencia hexadecimal 3D0D0A, que es el código ASCII para el signo igual seguido de <CRLF>.

La **codificación de transferencia base64,** también conocida como codificación radio-64, es una técnica común para codificar datos binarios arbitrarios de forma que sean invulnerables al procesamiento por programas de transporte de correo. Esta técnica convierte una entrada binaria arbitraria en una salida de caracteres imprimibles. Esta forma de codificación tiene las siguientes características relevantes:

1. El rango de la función es un conjunto de caracteres que es representable universalmente en todos los sitios, no una codificación binaria especifica de ese conjunto de caracteres. Así, los propios caracteres se pueden codificar en cualquier forma que sea necesaria por un sistema específico. Por ejemplo, el carácter «E» se representa en un sistema basado en ASCII por el valor hexadecimal 45 y en un sistema basado en EBCDIC por el valor hexadecimal C5.
2. El conjunto de caracteres consta de los 65 caracteres imprimibles, uno de los cuales se utiliza para relleno. Con $2^6 = 64$ caracteres disponibles, cada carácter se puede utilizar para representar 6 bits de entrada.
3. No se incluyen caracteres de control en el conjunto. Así, un mensaje codificado en base 64 puede atravesar sistemas de tratamiento de correo que comprueban el flujo de datos para encontrar caracteres de control.
4. El carácter de guión («-») no se utiliza. Este carácter tiene un significado en el formato RFC 822 y por lo tanto se debe evitar.

La Tabla 19.9 muestra la equivalencia de los valores de 6 bits de entrada con los caracteres. El conjunto de caracteres consta de los caracteres alfanuméricos más «+» y «/». El carácter «=» se utiliza como carácter de relleno.

Tabla 19.9. Codificación Radio-64.

Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter	Valor de 6 bits	Codificación del carácter
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(relleno)	=

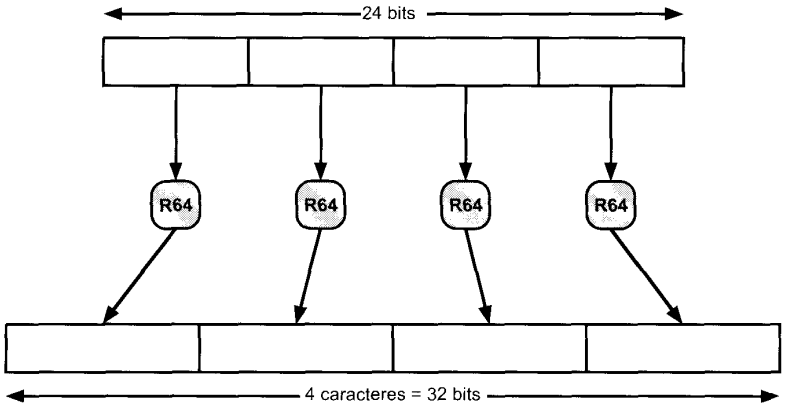


Figura 19.8. Codificación imprimible de datos binarios en formato radio 64.

La Figura 19.8 muestra un esquema de conversión sencillo. La entrada binaria se procesa en bloques de 3 octetos, o 24 bits. Cada conjunto de 6 bits en el bloque de 244 bits se convierte en un carácter. En la figura, los caracteres se muestran codificados como cantidades de 8 bits. En un caso típico, cada entrada de 24 bits se expande a una salida de 32 bits.

Por ejemplo, considere la secuencia de texto de 24 bits 00100011 0101110010 10010001, que expresado en hexadecimal es 235C91. Ordenando esta entrada en bloques de 6 bits se tiene

001000 110101 110010 010001

Los valores extraídos de 6 bits son 8, 53, 50, 17. Buscando estos valores en la Tabla 19.9 produce los siguientes caracteres con codificación radio-64: I1yR. Si estos caracteres se almacenan en formato ASCII de 8 bits con el bit de paridad puesto a cero, se tiene

01001001 00110001 01111001 01010010

En hexadecimal se expresa como 49317952. Para resumir:

Datos de entrada	
Representación binaria	00100011 01011100 10010001
Representación hexadecimal	235C91
Codificación radio-64 de los datos de entrada	
Representación en caracteres	I1yR
Código ASCII (8 bits paridad cero)	01001001 00110001 01111001 01010010
Representación hexadecimal	49317952

19.4. PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTOS (HTTP)

El protocolo de transferencia de hipertextos (HTTP) es el protocolo base del *world wide web* (WWW) y se puede utilizar en cualquier aplicación cliente-servidor que suponga la utilización de hipertextos. El

nombre es más bien confuso ya que HTTP no es un protocolo para transferir hipertexto; en lugar de eso es un protocolo para transmitir información con la eficiencia necesaria para hacer que el hipertexto salte. Los datos transferidos por el protocolo pueden ser texto propiamente dicho, hipertexto, audio, imágenes o cualquier información accesible a través de Internet.

Se comienza con una descripción general de los conceptos HTTP y el funcionamiento y después se examinan algunos de sus detalles, basando nuestra discusión en la versión más reciente incluida en la lista de estándares de Internet, HTTP 1.1 (RFC 2068). En la Tabla 19.10 se resume un número impor-

Tabla 19.10. Términos clave relacionados con HTTP.

Cache

Un almacenamiento local de un programa de mensajes de respuesta y el subsistema que controla el almacenamiento, recuperación y borrado de mensajes. Una cache almacena respuestas apropiadas para reducir el tiempo de respuesta y el consumo de ancho de banda en peticiones equivalente futuras. Cualquier cliente o servidor puede incluir una cache, aunque un servidor no puede utilizar una cache cuando actúa como túnel.

Cliente

Un programa de aplicación que establece conexiones con el propósito de enviar peticiones.

Conexión

Un circuito virtual de la capa de transporte establecido entre dos programas de aplicación para propósitos de comunicación.

Entidad

Una representación particular o interpretación de un recurso de datos, o una respuesta de un recurso de servicio, que puede estar incluido dentro de un mensaje de petición o respuesta. Una entidad consiste de cabeceras de entidad y un cuerpo de entidad.

Pasarela

Un servidor que actúa como intermediario para otros servidores. A diferencia de un representante, una pasarela recibe peticiones como si ella fuera el servidor original del recurso solicitado; el cliente solicitante podría no estar seguro si se está comunicando con una pasarela. Las pasarelas se utilizan a menudo como puertas del lado del servidor a través de cortafuegos de red y como traductores de protocolos para acceder a recursos en sistemas que no siguen HTTP.

Mensaje

La unidad básica de la comunicación HTTP, consistente en una secuencia estructurada de octetos transmitidos a través de la conexión.

Servidor original

El servidor en el que reside un recurso dado o donde se va a crear el recurso.

Representante

Un programa intermedio que actúa tanto como un servidor como un cliente con objeto de hacer las peticiones de parte de otros clientes. Las peticiones son servidas internamente o pasándolas, con la posible traducción, a otros servidores. Un representante debe interpretar y, si es necesario, reescribir un mensaje de petición antes de reenviarlo. Los representantes son utilizados a menudo como puertas del lado del cliente a través de cortafuegos de red y como aplicaciones de ayuda para tratar las peticiones a través de protocolos no implementados por el usuario agente.

Recurso

Un objeto de datos o un servicio de red que puede ser identificado por un URL.

Servidor

Un programa de aplicación que acepta conexiones para servir peticiones mediante respuestas.

Túnel

Un programa intermedio que está actuando como un retransmisor ciego entre dos conexiones. Una vez que está activo, no se considera como una parte de la comunicación HTTP, aunque puede ser iniciado por una petición HTTP. Un túnel finaliza cuando ambos extremos de la conexión retransmitida se cierran. Los túneles se utilizan como portal si es necesario y el intermediario no puede, o no debería, interpretar la comunicación retransmitida.

Agente de usuario

El cliente que inicia una petición. Entre éstos se incluyen los navegadores, editores, arañas («*spiders*») y otras herramientas del usuario final.

tante de términos definidos en las especificaciones HTTP; estos se irán introduciendo a medida que avance la discusión.

DESCRIPCIÓN GENERAL DE HTTP

HTTP es un protocolo cliente/servidor orientado a transacciones. El uso más común de HTTP es entre un navegador (*browser*) Web y un servidor Web. Para proporcionar seguridad, HTTP hace uso de TCP. Sin embargo, HTTP es un protocolo «sin estados»: cada transacción se trata independientemente. Por consiguiente, una implementación típica creará una conexión nueva entre el cliente y el servidor con cada transacción y después la cierra tan pronto como se completa la transacción, aunque la especificación no impone esta relación uno-a-uno entre la transacción y los tiempos de vida de la conexión.

La naturaleza de HTTP de ser un protocolo sin estados es la adecuada para su aplicación típica. Una sesión normal de un usuario con el cliente Web supone obtener una secuencia de páginas y documentos Web. La secuencia, idealmente, se obtiene rápidamente y las localizaciones de las distintas páginas y documentos Web pueden ser una serie de servidores distribuidos mundialmente.

Otra característica importante de HTTP es que es flexible en cuanto a los formatos que puede tratar. Cuando un cliente emite una solicitud a un servidor, puede incluir una lista de prioridades de formatos con los que puede operar, y el servidor responde con el formato adecuado. Por ejemplo, un navegador lynx no puede operar con imágenes, por lo tanto el servidor no necesita transmitir ninguna imagen de las páginas Web. Esta organización evita la transmisión de información innecesaria y proporciona la base para ampliar el conjunto de formatos de las nuevas especificaciones estándares y propietarias.

La Figura 19.9 muestra tres ejemplos de funcionamiento de HTTP. El caso más sencillo es aquel en el que un agente usuario establece una conexión directa con el servidor origen. El *agente de usuario* es el cliente que inicia la solicitud, como es el caso de un navegador Web actuando de parte de un usuario final. El *servidor origen* es el servidor donde reside el recurso de interés; un ejemplo lo constituye un servidor Web en el que reside la página central deseada. Para este caso, el cliente abre una conexión

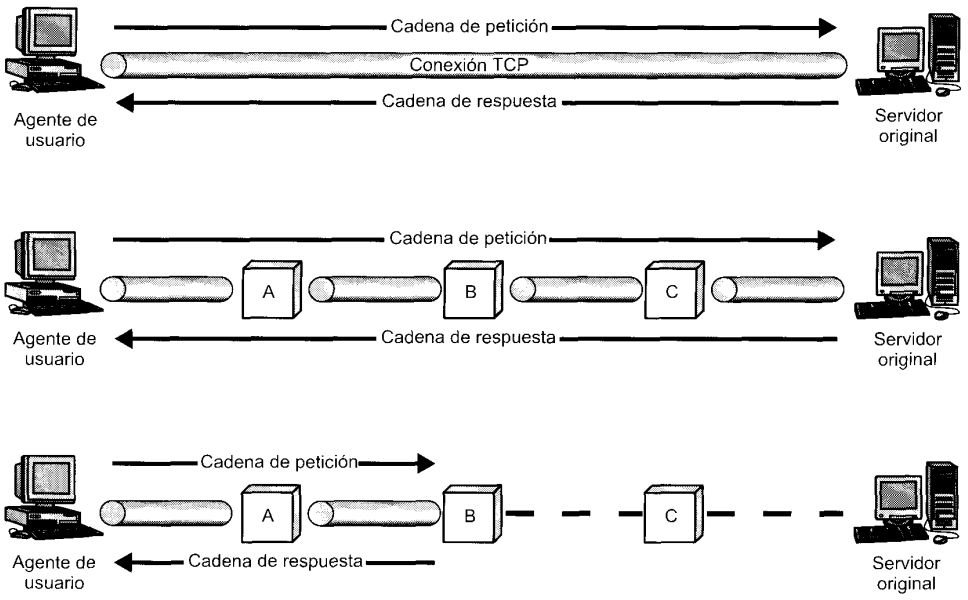


Figura 19.9. Ejemplos de operación HTTP.

TCP que es extremo-a-extremo entre el cliente y el servidor. El cliente emite una solicitud HTTP. La solicitud consta de la orden específica, referida a un método, un URL y un mensaje tipo MIME que contiene los parámetros de la solicitud, información sobre el cliente, y tal vez alguna información de contenido adicional.

Cuando el servidor recibe la solicitud, intenta llevar a cabo la acción solicitada y después devuelve una respuesta HTTP. La respuesta incluye información de estado, un código de éxito/error y un mensaje tipo MIME que contiene información sobre el servidor, información con la respuesta misma, y posiblemente contenido de cuerpo. A continuación se cierra la conexión TCP.

En la parte central de la Figura 19.9 se muestra un caso en que no existe una conexión TCP extremo-a-extremo entre el agente usuario y el servidor origen. En su lugar, existen uno o más sistemas intermedios con conexiones lógicas entre sistemas adyacentes. Cada sistema adyacente actúa como un retransmisor, para que una solicitud iniciada por el cliente se retransmita a través de los sistemas intermedios hasta el servidor, y la respuesta del servidor se retransmite de vuelta al cliente.

Se definen tres tipos de sistemas intermedios en la especificación HTTP: representante (*proxy*), pasarela (*gateway*), túnel (*tunnel*), los que se ilustran en la Figura 19.10.

Representante

Un representante actúa en nombre del cliente y presenta solicitudes de otros clientes a un servidor. El representante actúa como un servidor cuando interactúa con un cliente y como cliente cuando interactúa con un servidor. Existen varios escenarios que requieren el uso de un representante:

- **Intermediario de seguridad:** el cliente y el servidor pueden estar separados por un intermediario de seguridad, como es el caso de un cortafuegos, con el representante en el lado del cliente del cortafuegos. Normalmente, el cliente forma parte de una red protegida por un cortafuegos y el servidor es externo a esta red protegida. En este caso, el servidor se debe autentificar al corta-

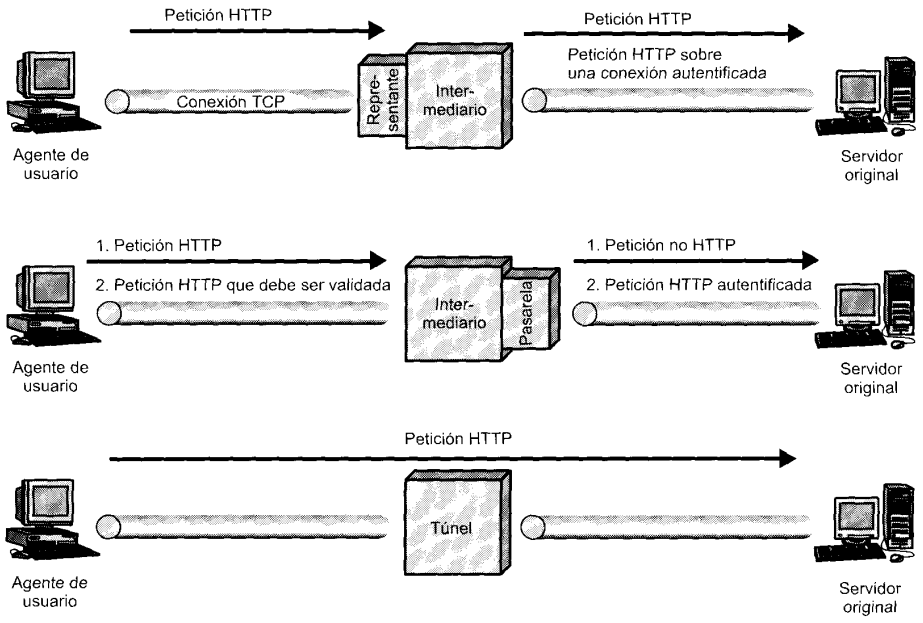


Figura 19.10. Sistemas HTTP intermedios.

fuegos para establecer una conexión con el representante. El representante acepta respuestas después de que hayan pasado por el cortafuegos.

- **Diferentes versiones de HTTP:** si el cliente y el servidor ejecutan diferentes versiones de HTTP, el representante puede implementar ambas versiones y realizar las traducciones requeridas.

En resumen, un representante es un agente de reenvío, recibiendo solicitudes para objetos URL, modificando las solicitudes y reenviándolas hacia el servidor identificado en el URL.

Pasarela

Una pasarela es un servidor que respecto al cliente actúa como si fuera un servidor original. Actúa en nombre de otros servidores que no son capaces de comunicarse directamente con un cliente. Existen varios escenarios en los que se pueden utilizar pasarelas:

- **Intermediario de seguridad:** el cliente y el servidor pueden estar separados por un intermediario de seguridad, como es el caso de un cortafuegos, con la pasarela en el lado del servidor del cortafuegos. Normalmente, el servidor está conectado a la red protegida por un cortafuegos y el cliente es externo a esta red protegida. En este caso, el cliente se debe autentificar a la pasarela, que puede pasar la solicitud al servidor.
- **Servidor no-HTTP:** los clientes Web se han construido con la capacidad de contactar con servidores de otros protocolos aparte de HTTP, como servidores FTP o Gopher. Esta capacidad también la puede proporcionar una pasarela. El cliente realiza una solicitud HTTP a un servidor pasarela. El servidor pasarela contacta con el servidor FTP o Gopher relevante para obtener el resultado deseado. Este resultado se convierte entonces en una forma adecuada para HTTP y se transmite de vuelta al cliente.

Túnel

A diferencia del representante y la pasarela, el túnel no realiza operaciones con las solicitudes y respuestas HTTP. Así es que un túnel simplemente es un punto de retransmisión entre dos conexiones TCP, y los mensajes HTTP se transfieren sin cambiarlos como si hubiera una única conexión HTTP entre el agente usuario y el servidor origen. Los túneles se utilizan cuando debe haber un sistema intermediario entre el cliente y el servidor pero no es necesario para ese sistema comprender el contenido de los mensajes. Un ejemplo es un cortafuegos en el que un cliente o un servidor externo a la red protegida puede establecer una conexión de autentificación y después se mantiene con objeto de realizar las transacciones HTTP.

Cache

Volviendo a la Figura 19.9, su parte inferior muestra un ejemplo de una cache. Una cache es un recurso que puede almacenar solicitudes y respuestas previas para tratar las nuevas solicitudes. Si llega una solicitud nueva que es igual a una solicitud almacenada, entonces la cache proporciona directamente la respuesta en lugar de acceder al recurso indicado en el URL. La cache puede operar en un cliente o en un servidor o en un sistema intermedio excepto un túnel. En la figura, el intermediario B ha almacenado una transacción solicitud/respuesta, para que la correspondiente solicitud nueva del cliente no necesite recorrer la cadena completa en el servidor origen, ya que es tratada por B.

No todas la transacciones se pueden almacenar y un cliente o un servidor puede indicar que ciertas transacciones se almacenen sólo durante un tiempo dado limitado.

MENSAJES

La mejor forma para describir la funcionalidad de HTTP es describir los elementos individuales del mensaje HTTP. HTTP consta de dos tipos de mensajes: solicitudes de los clientes a los servidores y

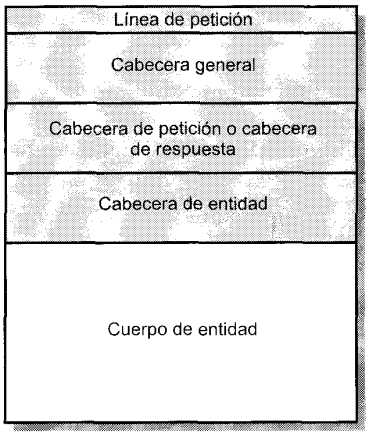


Figura 19.11. Estructura general de los mensajes HTTP.

respuestas de los servidores a los clientes. La estructura general de estos mensajes se muestra en la Figura 19.11. De una forma más formal, utilizando la notación BNF (Backus-Naur Form) (Tabla 19.11), tenemos:

Mensaje-HTTP = Solicitud-Sencilla | Respuesta-Sencilla | Solicitud-Completa | Respuesta-completa

Tabla 19.11. Notación BNF ampliada y utilizada en las especificaciones URL y HTTP

- Las palabras minúsculas representan variables o nombres de reglas.
- Una regla tiene la forma

  nombre = definición

- DIGIT es cualquier dígito decimal; CRLF es el retorno de carro, nueva línea; SP es uno o más espacios.
- Las comillas encierran texto literal
- Los ángulos «〈» «〉», se pueden utilizar dentro de una definición para delimitar un nombre de regla cuando su presencia facilita la claridad.
- Los elementos separados por una barra «|» son alternativos.
- Los paréntesis ordinarios se utilizan para indicar agrupaciones.
- El carácter «*» precediendo un elemento indica repetición. La forma completa es

  〈I〉*〈J〉elemento

  indicando al menos I y como mucho J ocurrencias del elemento. *elemento permite cualquier número, incluyendo 0; 1*elemento requiere al menos un elemento; 1*2elemento permite 1 o 2 elementos; 〈N〉elemento significa exactamente N elementos.
- Los paréntesis cuadrados «[» «]», encierran elementos opcionales.
- La construcción «#» se utiliza para definir, con el siguiente formato:

  〈I〉#〈J〉elemento

  indicando al menos I y como mucho J elementos, cada uno separado por una coma y espacios opcionales.
- Un punto y coma a la derecha de una regla indica el comienzo de un comentario que continúa hasta el final de la línea.

```
Solicitud-Completa = Línea-Solicitud
  *(Cabecera-General | Cabecera-Solicitada | Cabecera-Entidad)
  CRLF
  [Cuerpo-Entidad]
Respuesta-Completa = Línea-Estado
  *(Cabecera-General | Cabecera-Solicitada | Cabecera-Entidad)
  CRLF
  [Cuerpo-Entidad]
Solicitud-Sencilla = «GET» SP URL-Solicitado CRLF
Respuesta-Sencilla = [Cuerpo-Entidad]
```

Los mensajes Solicitud-Sencilla y Respuesta-Sencilla fueron definidos en HTTP/0.9. La solicitud es una orden sencilla GET con el URL solicitado; la respuesta es simplemente un bloque conteniendo la información identificada en URL. En HTTP/1.1 el uso de estas formas sencillas se desaconsejan ya que impiden al cliente utilizar negociación de contenido, y al servidor identificar el tipo de medio de la entidad devuelta.

Con solicitudes y respuestas completas, se utilizan los siguientes campos:

- **Línea-Solicitud:** identifica el tipo de mensaje y el recurso solicitado
- **Línea-Respuesta:** proporciona información de estado sobre esta respuesta.
- **Cabecera-General:** contiene campos que se aplican a los mensajes de solicitud y de respuesta, pero no se aplica a la entidad que está siendo transferida.
- **Cabecera-Solicitud:** contiene información sobre la solicitud y el cliente.
- **Cabecera-Respuesta:** contiene información sobre la respuesta.
- **Cabecera-Entidad:** contiene información sobre el recurso identificado por la solicitud e información sobre el cuerpo de la entidad.
- **Cuerpo-Entidad:** el cuerpo del mensaje.

Todas las cabeceras de HTTP constan de una secuencia de campos, siguiendo el mismo formato genérico del RFC 822 (descrito en la Sección 19.3). Cada campo comienza en una línea nueva y consiste en el nombre del campo seguido por dos puntos y el valor del campo.

Aunque el mecanismo de transacción básico es sencillo, existe un gran número de campos y parámetros definidos en HTTP; éstos se muestran en la Tabla 19.12. En el resto de esta sección se describen las cabeceras de solicitud, las cabeceras de respuesta y las entidades.

Campos de la cabecera general

Los campos de la cabecera general se pueden utilizar en los mensajes de solicitud y de respuesta. Estos campos se aplican en ambos tipos de mensajes y contienen información que no se aplica directamente a la entidad que se está transfiriendo. Los campos son:

- **Cache-Control (Control de Cache):** especifica directivas que se deben cumplir por cualquier mecanismo de implementación de cache a lo largo de la cadena solicitud/respuesta. El propósito es prevenir a una cache de interferencias adversas con esta solicitud o respuesta particular.
- **Connection (Conexión):** contiene una lista de palabras clave y nombres de campos de cabecera que solamente se aplican a esta conexión TCP entre el que envía y el destino más cercano que no sea un túnel.
- **Date (Fecha):** día y hora en la que se originó el mensaje.
- **Forwarded (Reenvío):** utilizado por las pasarelas y representantes para indicar pasos intermedios a lo largo de la cadena de solicitud o respuesta. Cada pasarela o representante que trata un mensaje puede incorporar un campo Reenvío que da su URL.

Tabla 19.12. Elementos HTTP.

TODOS LOS MENSAJES			
Campos de la cabecera general		**Campos de la cabecera de entidad**	
Cache-Control	Keep-Alive	Allow	Derived-From
Connection	MIME-Version	Content-Encoding	Expires
Data	Pragma	Content-Language	Last-Modified
Forwarded	Upgrade	Content-Length	Link
		Content-MD5	Title
		Content-Range	Transfer-Encoding
		Content-Type	URI-Header
		Content-Version	extension-header
MENSAJES DE PETICIÓN			
Métodos de solicitud		**Campos de la cabecera de petición**	
OPTIONS	MOVE	Accept	If-Modified-Since
GET	DELETE	Accept-Charset	Proxy-Authorization
HEAD	LINK	Accept-Encoding	Range
POST	UNLINK	Accept-Language	Referer
PUT	TRACE	Authorization	Unless
PATCH	WRAPPED	From	User-Agent
COPY	extension-method	Host	
MENSAJES DE RESPUESTA			
Códigos de estado de respuesta			**Campos de la cabecera de respuesta**
Continue	Moved Temporarily	Request Timeout	Location
Switching Protocols	See Other	Conflict	Proxy-Authenticate
OK	Not Modified	Gone	Public
Created	Use Proxy	Lengh Required	Retry-After
Accepted	Bad Request	Unless True	Server
Non-Authoritative	Unauthorized	Internal Server Error	WWW-Authenticate
Information	Payment Required	Not Implemented	
No Content	Forbidden	Bad Gateway	
Reset Content	Not Found	Service Unavailable	
Partial Content	Method Not Allowed	Gateway Timeout	
Multiple Choices	None Acceptable	extensión coce	
Moved Permanently	Proxy Authentication Required		

- **Keep-Alive (Mantener vivo):** puede estar presente si existe la palabra clave *keep-alive* en un campo Conexión entrante, y proporciona información al solicitante de la duración de la conexión persistente. Este campo puede indicar un tiempo máximo durante el que el emisor mantendrá abierta la conexión esperando la siguiente solicitud, o el máximo número de solicitudes adicionales que se le permitirán a la actual conexión persistente.
- **Versión MIME:** indica que el mensaje sigue las instrucciones de la versión indicada de MIME.
- **Pragma:** contiene directivas específicas de la implementación que se pueden aplicar a cualquier destino a lo largo de la cadena de solicitud/respuesta.
- **Upgrade (Actualización):** se utiliza en una solicitud para especificar los protocolos adicionales que admite el cliente y cuál de ellos le gustaría utilizar; se utiliza en respuestas para indicar que protocolo será utilizado.

MENSAJES DE PETICIÓN

Un mensaje de petición completo consta de una línea de estado seguida por una o más cabeceras generales de entidad seguídas por un cuerpo de entidad opcional.

Métodos de petición

Un mensaje de petición completo siempre comienza con una Línea-Petición, que tiene el siguiente formato:

Línea-Petición = Método SP URL-Petición SP Version-HTTP CRLF

El parámetro Método contiene el orden de petición real, llamada método en HTTP. URL-Petición es el URL del recurso solicitado y Version-HTTP es el número de versión de HTTP utilizado por el emisor.

Se definen los siguientes métodos de petición en HTTP/1.1:

- **OPTIONS (opciones):** una petición de información sobre las opciones disponibles para la cadena petición/respuesta identificada por este URL.
- **GET (obtener):** una petición para recuperar la información identificada en el URL y devuelta en el cuerpo de entidad. Un GET es opcional si el campo de cabecera If-Modified-Since está incluido, y es parcial si el campo de cabecera Range está incluido.
- **HEAD (cabeza):** esta petición es idéntica a GET, excepto que la respuesta del servidor no debe incluir un cuerpo de entidad; todos los campos de cabecera en la respuesta son los mismos como si el cuerpo de la entidad estuviera presente. Esto permite a un cliente obtener información sobre un recurso sin transferir el cuerpo de la entidad.
- **POST (correo):** una petición para aceptar la entidad incorporada como una nueva subordinada al URL identificado. La entidad enviada está subordinada a ese URL de la misma forma que un fichero está subordinado al directorio que lo contiene, un artículo nuevo está subordinado a un grupo de noticias al que se envía o un registro está subordinado a una base de datos.
- **PUT (poner):** petición para aceptar la entidad incorporada y almacenarla bajo el URL proporcionado. Éste puede ser un nuevo recurso con un nuevo URL o una reposición del contenido de un recurso existente con un URL existente.
- **PATCH (parche):** similar a PUT, excepto que la entidad contiene una lista de diferencias con respecto al contenido del recurso original identificado en el URL.
- **COPY (copiar):** solicita que una copia del recurso identificado por el URL en Línea-Petición se copie a la(s) localización(es) dada(s) en el campo Cabecera-URL en la Cabecera-Entidad de este mensaje.
- **MOVE (mover):** solicita que el recurso identificado por el URL en Línea-Petición se transfiera a la(s) localización(es) dada(s) en el campo Cabecera-URL en la Cabecera-Entidad de este mensaje. Es equivalente a COPY seguido de DELETE.
- **DELETE (suprimir):** solicita que el servidor origen suprima el recurso identificado por el URL en la Línea-Solicitud.
- **LINK (enlace):** establece una o más relaciones de enlace entre recursos identificados en Línea-Solicitud. Los enlaces se definen en el campo Link de la Cabecera-Entidad.
- **UNLINK (enlace roto):** elimina una o más relaciones de enlace entre recursos identificados en Línea-Solicitud. Los enlaces se definen en el campo Link de la Cabecera-Entidad.
- **TRACE (trazar):** solicita que el servidor devuelva todo lo que reciba como cuerpo de entidad de la respuesta. Esto se puede utilizar con objetivos de comprobación y diagnóstico.

- **WRAPPED (envolver):** permite a un cliente enviar una o más solicitudes encapsuladas. Las solicitudes pueden estar encriptadas o haber sufrido otro tipo de procesamiento. El servidor debe quitar la envoltura y procesar de acuerdo a esto.
- **Extension-method (método-de-extensión):** permite definir métodos adicionales sin cambiar el protocolo, pero no se puede suponer que estos métodos se vayan a reconocer por el destino.

Campos de la cabecera de petición

Los campos de la cabecera de petición actúan como modificadores de petición, proporcionando información adicional y parámetros relacionados con la petición. En HTTP/1.1 están definidos los siguientes campos:

- **Accept (aceptado):** una lista de tipos de medio y rangos que son aceptables como respuesta a esta petición.
- **Accept-Charset (conjunto de caracteres aceptado):** una lista de conjuntos de caracteres aceptables para la respuesta.
- **Accept-Encoding (codificación aceptada):** lista de los esquemas de codificación de contenido aceptable para el cuerpo de la entidad. La codificación del contenido se utiliza principalmente para permitir que un documento se comprima o se encripte. Normalmente el recurso se almacena con esta codificación y solamente se decodifica antes de su uso real.
- **Accept-Languaje (lenguaje aceptado):** restringe el conjunto de lenguajes naturales que se prefiere para la respuesta.
- **Authorization (autorización):** contiene un valor de campo, conocido como credencial, utilizado por un cliente para autentificarse el mismo ante el servidor.
- **From (de):** la dirección de correo electrónico en Internet para el usuario humano que controla el agente de usuario solicitante.
- **Host (computador):** especifica el computador Internet del recurso solicitado.
- **If-Modified-Since (si ha sido modificado desde):** utilizado con el método GET. Esta cabecera incluye un parámetro de fecha/hora; el recurso se va a transferir solamente si ha sido modificado desde la fecha/hora especificada. Esta característica permite actualizaciones eficientes de la cache. Un mecanismo que implemente la cache puede emitir periódicamente mensajes GET a un servidor origen y sólamente recibirá pequeños mensajes de respuesta a menos que sea necesario una actualización.
- **Proxy-Authorization (autorización de representante):** permite que un cliente se autorice el mismo a un representante que requiere autentificación.
- **Range (rango):** para estudios futuros. La intención es que, en un mensaje GET, un cliente pueda solicitar solamente una parte del recurso identificado.
- **Referer (remite):** el URL de un recurso del que se obtuvo el URL solicitado. Esto permite a un servidor generar una lista de enlaces hacia atrás.
- **Unless (no útil):** similar en funcionamiento al campo If-Modified-Since, con dos diferencias: (1) no se restringe al método GET, y (2) la comparación se realiza en el valor del campo Entity-Header en lugar del valor fecha/hora.
- **User-Agent (agente de usuario):** contiene información sobre el agente usuario que origina la solicitud. Esto se utiliza con objetivos estadísticos, para hacer un seguimiento de las violaciones de protocolo y para el reconocimiento automático de agentes usuarios con objeto de confeccionar respuestas que evitan limitaciones de agentes usuarios particulares.

MENSAJES DE RESPUESTA

Un mensaje de respuesta completo consta de una línea de estado seguida por una o más cabeceras generales de entidad de respuesta, seguida por un cuerpo de entidad opcional.

Códigos de estado

Un mensaje de respuesta completo siempre comienza con una Línea-de-Estado, que tiene el siguiente formato:

Línea-de-estado = Versión-HTTP SP Código-Estado SP Frase-de-Razón CRLF

El valor de Versión-HTTP es el número de versión del HTTP utilizado por el que envía. El Código-Estado es un entero de 3 dígitos que indica la respuesta a una solicitud recibida y la Frase-de-Razón proporciona una explicación corta textual del código de estado.

Existe una gran cantidad de códigos de estado definidos en HTTP/1.1; éstos se muestran en la Tabla 19.13 junto con una breve explicación. Los códigos se organizan en las siguientes categorías:

- **De información:** la solicitud se ha recibido y el procesamiento continúa. No se acompaña un cuerpo de entidad en la respuesta.
- **De éxito:** la solicitud se recibió con éxito, se entendió y aceptó. La información devuelta en el mensaje de respuesta depende del método de solicitud, como sigue:

  GET: el contenido del cuerpo de entidad corresponde al recurso solicitado.
  HEAD: no se devuelve cuerpo de entidad.
  POST: la entidad describe o contiene el resultado de la acción.
  TRACE: la entidad contiene el mensaje de solicitud.
  Otros métodos: la entidad describe el resultado de la acción.
- **De redirección:** se requieren acciones adicionales para completar la solicitud.
- **De error del cliente:** la solicitud contiene un error de sintaxis o la solicitud no se puede llevar a cabo.
- **De error del servidor:** el servidor falló al llevar a cabo una solicitud aparentemente válida.

Campos de cabecera de respuesta

Los campos de cabecera de respuesta proporcionan información adicional relacionada con la respuesta y que no se puede situar en la Línea-de-Estado. En HTTP/1.1 se definen los siguientes campos:

- **Location (localización):** define la localización exacta del recurso identificado por el URL-Request.
- **Proxy-Authenticate (autentificación del representante):** incluido con una respuesta que tiene un código de estado de la solicitud de autentificación del representante. Este campo contiene un «reto» que indica el esquema de autentificación y los parámetros requeridos.
- **Public (público):** indica los métodos no normalizados que admite este servidor.
- **Retry-After (intentar después):** incluido en una respuesta que tiene un código de estado de Service Unavailable (servicio no disponible) e indica cuánto tiempo se espera que el servicio esté no disponible.
- **Server (servidor):** identifica el producto software utilizado por el servidor origen para tratar la solicitud.
- **WWW-Authenticate (autentificación WWW):** incluida en una respuesta que tiene el código de estado Unauthorized (no autorizado). Este campo contiene un «reto» que indica el esquema de autentificación y los parámetros requeridos.

Tabla 19.13. Códigos de estado HTTP.

De información	
Continue	Recibida la parte inicial de la solicitud; el cliente puede continuar con la solicitud.
Switching Protocol	El servidor conmutará a los nuevos protocolos de aplicación solicitados.
De éxito	
OK	La solicitud ha tenido éxito y la información de respuesta apropiada se incluye.
Created	La solicitud se ha completado y se ha creado un recurso nuevo; se incluye el URL(s).
Accepted	La solicitud se ha aceptado pero el procesamiento no ha terminado. La solicitud podría o no ser finalizada finalmente.
Non-Authoritative Information	Los contenidos devueltos de la cabecera de entidad no son el conjunto definitivo disponible en el servidor origen, pero están recogidos en una copia local o en una tercera parte.
No Content	El servidor ha completado la solicitud pero no se tiene información que devolver.
Reset Content	La solicitud ha tenido éxito y el usuario agente debería inicializar la vista de documento que causó la solicitud a ser generada.
Partial Content	El servidor ha completado la solicitud GET parcial y la información correspondiente se incluye.
Redirección	
Multiple Choices	El recurso solicitado está disponible en varias localizaciones y no se puede determinar la localización preferida.
Moves Permanently	Al recurso solicitado le ha sido asignado un URL permanente nuevo; las referencias futuras se deben hacer a este URL.
Moved Temporarily	El recurso solicitado reside temporalmente en un URL diferente.
See Other	La respuesta a la solicitud se puede encontrar en un URL diferente y se debería obtener utilizando un GET en ese recurso.
Not Modified	El cliente ha realizado un GET condicional, el acceso está permitido, y el documento no se ha modificado desde la fecha/tiempo especificada en la solicitud.
Use Proxy	El recurso solicitado se debe acceder a través de un representante indicado en el campo Location.
Error de Cliente	
Bad Request	Sintaxis incorrecta en la solicitud.
Unauthorized	La solicitud requiere autorización al usuario.
Payment Required	Reservado para usos futuros.
Forbidden	El servidor rechaza completar la solicitud; utilizado cuando el servidor no desea revelar porque se rechazó la solicitud.
Not Found	URL solicitado no encontrado.
Method Not Allowed	Método (orden) no permitido para el recurso solicitado.
Proxy Authentication Required	El cliente se debe autentificar con el representante.
Conflict	La solicitud no se puede completar debido a un conflicto con el estado actual del recurso.
Gone	El recurso solicitado no está ya disponible en el servidor y no se conoce la dirección de reenvío.
Length Required	El servidor rechaza aceptar solicitudes sin una longitud de contenido definida.
Unless True	La condición dada en el campo Unless era verdadera cuando se comprobó en el servidor.
Error de Servidor	
Internal Server Error	El servidor encontró una condición no esperada que le impide completar la solicitud.
No Implemented	El servidor no soporta la funcionalidad requerida para completar la solicitud.
Bad Gateway	El servidor, mientras actuaba como pasarela o representante, recibió una respuesta inválida del servidor en la dirección del flujo al que accede para completar la solicitud.
Server Unavailable	El servidor es incapaz de gestionar la solicitud debido a una sobrecarga temporal o a mantenimiento del servidor.
Gateway Timeout	El servidor, mientras actuaba como pasarela o representante, no recibió una respuesta a tiempo del servidor en la dirección del flujo al que accede para completar la solicitud.

ENTIDADES

Una entidad consta de una cabecera de entidad y un cuerpo de entidad en un mensaje de solicitud o de respuesta. Una entidad puede representar un recurso de datos o puede constituir otra información proporcionada con una solicitud o una respuesta.

Campos de la cabecera de entidad

Los campos de la cabecera de entidad proporcionan información opcional sobre el cuerpo de la entidad o, si el cuerpo no está presente, sobre el recurso identificado por la solicitud. En HTTP/1.1 se definen los siguientes campos:

- **Allow (permitir):** indica los métodos admitidos por el recurso identificado en el URL-Request. Este campo se debe incluir con una respuesta que tiene un código de estado Method-Not-Allowed y se puede incluir en otras respuestas.
- **Content-Encoding (codificación del contenido):** indica qué codificación del contenido se ha aplicado al recurso. La única codificación actualmente definida es la compresión zip.
- **Content-Language (lenguaje del contenido):** identifica el lenguaje(s) natural de la audiencia destino de la entidad indicada.
- **Content-length (longitud del contenido):** el tamaño del cuerpo de la entidad en octetos.
- **Content-MD5 (contenido MD5):** para estudios futuros. MD5 se refiere a la función de código de mezcla (*hash*) MD5, descrita en el Capítulo 18.
- **Content-Range (rango del contenido):** para estudios futuros. La intención es que indicará una parte del recurso identificado que se incluye en esta respuesta.
- **Content-Type (tipo de contenido):** indica el tipo de medio del cuerpo de la entidad.
- **Content-Version (versión del contenido):** una marca de versión asociada con una entidad en desarrollo.
- **Derived-From (derivada de):** indica la marca de versión de un recurso del que se derivó esta entidad antes de que se hicieran las modificaciones por el emisor. Este campo y el campo Content-Version se pueden utilizar para tratar múltiples actualizaciones por un grupo de usuarios.
- **Expires (expirar):** fecha/hora después de la cual la entidad se debería considerar obsoleta.
- **Last-Modified (última modificación):** fecha/hora de la última modificación del recurso que supone el emisor.
- **Link (enlace):** define enlaces a otros recursos.
- **Title (título):** un título textual de la entidad.
- **Transfer-Encoding (codificación de transferencia):** indica qué tipo de transformación se ha aplicado al cuerpo del mensaje para realizar una transferencia segura entre el emisor y el destino. La única codificación definida en el estándar es *chunked*. Esta opción define un procedimiento para romper un cuerpo de entidad en fragmentos etiquetados que se transmiten por separado.
- **URL-header (cabecera de URL):** informa al destino de otros URL por los que se puede identificar el recurso.
- **Extension-header (ampliación de cabecera):** permite definir campos adicionales sin cambiar el protocolo, pero se supone que estos campos se van a reconocer por el destino.

Cuerpo de la entidad

Un cuerpo de entidad consta de una secuencia arbitraria de octetos. HTTP está diseñado para ser capaz de transferir cualquier tipo de contenido, incluyendo texto, datos binarios, imágenes y vídeo. Cuando

está presente un cuerpo de entidad en un mensaje, la interpretación de los octetos en el cuerpo se determina por los campos de la cabecera de entidad Content-Encoding, Content-Type y Transfer-Encoding. Estos definen un modelo de codificación ordenado en tres capas:

cuerpo-entidad : = Transfer-Encoding(Content-Encoding(Content-Type(datos)))

Los datos es el contenido del recurso identificado por el URL. El campo Content-Type determina la forma en que se interpretan los datos. Se puede aplicar una codificación de contenido a los datos y almacenarlos en el URL en lugar de los datos. Finalmente, en la transferencia, se puede aplicar una codificación de transferencia para formar el cuerpo de entidad del mensaje.

19.5. LECTURAS RECOMENDADAS Y PÁGINAS WEB

Una presentación rigurosa de ASN.1 se encuentra en [STEE90]. Dos documentos bastantes útiles son [KALI91] y [GAUD89]. [STAL96] proporciona un examen comprensivo y detallado de SNMP, SNMPv2 y SNMPv3; el texto también proporciona una descripción general de la tecnología de gestión de red. [ROSE93] proporciona un tratamiento del correo electrónico con la longitud de un libro, incluyendo alguna información de SMTP y MIME.

GAUD89 Gaudette, P. *A Tutorial on ASN.1*. Technical Report NCSL/SNA-89/12. Gaithersburg, MD: National Institute of Standards and Technology, 1989.

KALI91 Kaliski, B. *A. Layman's Guide to a Subset of ASN.1, BER, and DER*. Report SEC-SIC-91-17, Redwood City, CA: RSA Data Security Ind. 1991.

ROSE93 Rose, M. *The Internet Message: Closing the Book with Electronic Mail*. Englewood Cliffs, NJ: Prentice Hall, 1993.

STAL99 Stalling, W. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Reading, MA: Addison-Wesley, 1999.

STEE90 Steedman, D. *ASN.1: The Tutorial and Reference*. London: Technology Appraisals, 1990.

SITIOS WEB RECOMENDADOS

- **Página Web Simple:** mantenida por la Universidad de Twente. Es una buena fuente de información sobre SNMP, incluyendo enlaces a muchas implementaciones de dominio público y listas de libros y artículos.
- **Consorcio WWW:** contiene información actualizada sobre HTTP y tópicos relacionados.
- **Página Web de ASN.1:** contiene tutoriales, enlaces a herramientas software, aplicaciones y productos basados en ASN.1 e información sobre estándares.

19.6. PROBLEMAS

19.1. **a)** Considere la siguiente definición:

```
ExpeditedDataAcknowledgement ::= SET {
desRef          [0]     Reference,
yr-tu-nr        [1]     TPDUnumber,
checkSum        [2]     CheckSum OPTIONAL
```

```
NormalEA ::= ExpeditedDataAcknowledgement
(WITH COMPONENTS {
 desRef,
 yr-tu-nr (0..127) }
```

Encuentre una expresión equivalente para definir NormalEA.

b) Considere la siguiente definición:

```
ExtenderEA ::= ExpeditedDataAcknowledgement
  (WITH COMPONENTS {..., checkSum PRESENT })
```

Encuentre una expresión equivalente para definir NormalEA.

c) Defina un nuevo tipo, EA, basado en ExpeditedDataAcknowledgement, con la restricción de que la suma de comprobación está ausente, en cuyo caso yr-tu-nr debe estar en el rango de 0 a 127, o la suma de comprobación está presente, en cuyo caso no existe ninguna restricción adicional en yr-tu-nr.

19.2. Considere la definición siguiente:

```
TypH ::= SEQUENCE {
=r              INTEGER,
s               BOOLEAN,
t               INTEGER OPCIONAL }
```

¿Cuáles de los valores siguientes son válidos?

```
valH1 TypH ::= { r −5, s TRUE, t 0}
valH2 TypH ::= {10, FALSE}
valH3 TypH ::= { t 1, r 2, s TRUE }
```

19.3. Dada la definición siguiente:

```
T1 ::= SEQUENCE { X1,
  b BOOLEAN }
X1 ::= CHOICE {y INTEGER, z REAL }
```

¿Serían y, z, b identificadores de T1?

19.4. Defina un tipo IA5String-based que contenga solamente los caracteres «A» o «B» y está restringido a una longitud máxima de 10 caracteres.

19.5. La especificación original (versión 1) de SNMP tiene la definición siguiente de un tipo nuevo:

```
Gauge ::= [APPLICATION 2] IMPLICIT INTEGER (0..4294967295)
```

El estándar incluye la siguiente explicación de la semántica de este tipo:

> Este tipo de aplicación de uso amplio representa un entero no negativo, que se puede incrementar o decrementar, pero se fija («latch») a un valor máximo. Este estándar especifica un valor máximo de $2^{32} - 1$ (4294967295 en decimal) para Gauge.

Desafortunadamente, la palabra «latch» no está definida y ha dado lugar a dos interpretaciones diferentes. El estándar SNMPv2 clarifica esta ambigüedad con la siguiente definición:

> El valor de Gauge es máximo siempre que la información que se está modelando es menor o igual que ese valor máximo; si la información que se está modelando se decrementa debajo del valor máximo, Gauge también se decrementa.

a) ¿Cuál es la interpretación alternativa?

b) Discuta los pros y los contras de las dos interpretaciones.

19.6. Los sistemas de correo electrónico difieren en la manera en la que se tratan los recipientes múltiples. En algunos sistemas, el agente usuario origen o emisor de correo hace todas las copias necesarias y éstas se envían de forma independiente. Un enfoque alternativo es determinar primero la ruta de cada destino. Después se envía un único mensaje en la parte común de la ruta y se hacen solamente copias cuando las rutas divergen; este proceso se conoce como empaquetamiento de correo (*mail-bagging*). Discuta las ventajas y desventajas relativas de los dos métodos.

APÉNDICE A

RDSI y RDSI de banda ancha

- Más allá de las alternativas tradicionales de servicios de conmutación de paquetes y de conmutación de circuitos, está surgiendo rápidamente una alternativa nueva de red de área ancha fácilmente disponible: Red Digital de Servicios Integrados (RDSI).
- Los servicios de la RDSI se basan en el concepto de proporcionar un conjunto de canales con una única interfaz. El canal B, a 64 kbps, es el canal principal usado para conmutación de circuitos, conmutación de paquetes y circuitos dedicados (alquilados). El canal D se usa para la señalización de control (llamada de inicio) y también puede transmitir algunos datos. Para usuarios en casa y pequeñas empresas existe un servicio de acceso básico de dos canales, uno B y otro D. Para clientes con PBX digital o instalaciones LAN, se utiliza un servicio de acceso primario de 23 canales B o 30 canales B y un canal D.
- La RDSI de banda ancha es una especificación de segunda generación de la RDSI que proporciona altas velocidades de datos digitales. La tecnología básica de la interfaz de usuario es ATM.

Los rápidos avances en las tecnologías de computadores y de comunicaciones han dado lugar a la fusión de estos dos campos. Las fronteras entre computación, conmutación y equipos de transmisión digital se han difuminado, y se usan las mismas técnicas digitales para transmisión de datos, voz e imagen. La evolución y fusión de las tecnologías, junto con la creciente demanda de recogida, procesamiento y diseminación de la información eficientes y oportunos, nos llevan al desarrollo de sistemas integrados que transmitan y procesen todo tipo de datos. El objetivo final de esta evolución es la red digital de servicios integrados (RDSI; en inglés ISDN, Integrated Services Digital Network).

La RDSI pretende ser una red pública mundial de telecomunicaciones que reemplace a las redes de telecomunicaciones existentes y ofrezca una amplia variedad de servicios. La RDSI está definida por la normalización de interfaces de usuario y se implementa como un conjunto de conmutadores digitales y caminos admitiendo un amplio rango de tipos de tráfico y suministrando servicios de procesamiento de valor añadido. En la práctica, hay muchas redes implementadas dentro de las fronteras nacionales, pero desde el punto de vista del usuario, habrá una red única, mundial, uniformemente accesible.

El impacto de la RDSI, tanto en usuarios como en vendedores, ha sido profundo. Para controlar la evolución y el impacto de la RDSI, se está haciendo un esfuerzo masivo de normalización. Aunque las normalizaciones RDSI están todavía evolucionando, se comprende bien tanto la tecnología como la incipiente estrategia de implementación.

A pesar del hecho de que la RDSI no ha conseguido todavía el despliegue universal esperado, está ya en su segunda generación. La primera generación, a veces denominada **RDSI de banda estrecha,** se basa en el uso de un canal de 64 kbps como unidad básica de conmutación, orientada a conmutación de circuitos. La mayor contribución técnica de la RDSI de banda estrecha ha sido la retransmisión de tramas («frame relay»). La segunda generación, denominada **RDSI de banda ancha (RDSI-BA),** admite velocidades muy altas (cientos de Mbps) y está orientada a conmutación de paquetes. La mayor contribución técnica de la RDSI de banda ancha ha sido el modo de transferencia asíncrono (ATM), también conocido como de «retransmisión de celdas».

Este apéndice muestra una visión general de la RDSI de banda estrecha y de la RDSI de banda ancha.

A.1 VISIÓN GENERAL DE LA RDSI

CONCEPTO DE RDSI

El concepto de RDSI se introduce mejor considerándola desde distintos puntos de vista:

- Principios de la RDSI
- La interfaz de usuario
- Objetivos

Principios de la RDSI

Las normalizaciones para RDSI se han definido en la ITU-T (antiguamente CCITT), tema que exploraremos más adelante en esta sección. La Tabla A.1, que es el texto completo de una de las normalizaciones relacionadas con la RDSI, establece los principios de la RDSI desde el punto de vista de la ITU-T. Veamos cada uno de estos puntos.

1. **Soporte de aplicaciones con voz y sin voz usando un conjunto limitado de prestaciones normalizadas.** Este principio define tanto los objetivos de la RDSI así como los medios para lograrlos. La RDSI proporciona varios servicios relacionados con las comunicaciones de voz (llamadas telefónicas) y comunicaciones sin voz (intercambio de datos digitales). Estos servicios se realizan conforme las normalizaciones (recomendaciones ITU-T) que especifican un pequeño número de interfaces y dispositivos de transmisión de datos.
2. **Soporte para aplicaciones conmutadas y no conmutadas.** RDSI admite tanto conmutación de circuitos como conmutación de paquetes. Además, RDSI proporciona servicios no conmutados con líneas dedicadas a ello.
3. **Dependencia de conexiones de 64 kbps.** RDSI proporciona conexiones de conmutación de circuitos y de conmutación de paquetes a 64 kbps. Éste es el bloque de construcción fundamental de la RDSI. Se eligió esta velocidad porque, en esa época, se hizo el estándar de velocidad para voz digitalizada, y así se estaba introduciendo en las redes digitales integradas (RDI) que se estaban desarrollando. A pesar de que esta razón de datos es útil, es muy restrictivo apoyarse sólo en ella. Futuros desarrollos en RDSI permitirán mayor flexibilidad.
4. **Inteligencia en la red.** Se espera que la RDSI pueda proporcionar servicios sofisticados superiores a la sencilla situación de una llamada de circuito conmutado.
5. **Arquitectura con protocolo en capas.** Los protocolos para acceso del usuario a RDSI presentan una arquitectura en capas que se puede hacer corresponder con el modelo OSI. Esto tiene una serie de ventajas:

   Se pueden usar las normalizaciones ya desarrolladas para aplicaciones relacionadas con OSI en RDSI. Un ejemplo es el nivel 3 de X.25 para acceso a servicios de conmutación de paquetes en RDSI.

   Las nuevas normalizaciones relacionadas con RDSI se pueden basar en normalizaciones ya existentes, reduciéndose el coste de nuevas implementaciones. Un ejemplo es LAPD, que se basa en LAPB.

   Se pueden desarrollar e implementar normalizaciones independientes para varias capas y para varias funciones en una capa. Esto permite la implementación gradual de los servicios de RDSI a un ritmo apropiado para un suministrador dado o una base dada de clientes.
6. **Variedad de configuraciones.** Es posible más de una configuración física para implementar RDSI. Esto permite diferencias en políticas nacionales (monopolio frente a competencia), en el estado de la tecnología, y en las necesidades y equipos existentes de la base de clientes.

Tabla A.1. Recomendación ITU-T I.120 (1993).

1. Principios de la RDSI

1.1. La principal característica del concepto RDSI es la capacidad de admitir un amplio rango de aplicaciones con voz y sin voz en la misma red. Un elemento clave en la integración de un servicio en la RDSI es la oferta de un rango de servicios usando un conjunto limitado de tipos de conexión y disposiciones de interfaz usuario-red multipropósito.

1.2. RDSI admite diversas aplicaciones incluyendo tanto conexiones de circuitos conmutados como de paquetes conmutados. En RDSI, las conexiones conmutadas incluyen tanto conexiones de circuitos conmutados como de paquetes conmutados y sus concatenaciones.

1.3. En cuanto estén disponibles, los nuevos servicios introducidos en la RDSI deberían ser compatibles con las conexiones digitales conmutadas de 64 kbits/s.

1.4. Una RDSI tendrá inteligencia con el fin de proporcionar características de servicio, funciones de mantenimiento y de gestión de red. Puede que esta inteligencia no sea suficiente para algunos de los nuevos servicios y puede que tenga que ser suplementada con alguna inteligencia adicional dentro de la red o posiblemente con inteligencia compatible en los terminales de usuario.

1.5. Se debería usar una estructura de protocolos en capas, para especificar un acceso a la RDSI. El acceso de un usuario a los recursos RDSI, puede variar dependiendo del servicio solicitado y del estado de implementación de las RDSI nacionales.

1.6. Está reconocido que se pueden implementar RDSI con distintas configuraciones según las situaciones nacionales específicas.

2. Evolución de las RDSI

2.1. Las RDSI se basarán en los conceptos para telefonía RSI y podrán evolucionar incorporando progresivamente funciones adicionales y características de red incluyendo aquéllas de cualquier otra red dedicada, como conmutación de circuitos y conmutación de paquetes para datos de forma que se suministren servicios ya existentes o nuevos.

2.2. La transición de una red existente a una red RDSI de gran alcance, puede requerir un periodo de tiempo de una a varias décadas. Durante este periodo, la adaptación debe desarrollarse de forma que queden interconectados servicios de RDSI y servicios de otras redes.

2.3. En la evolución hacia una RDSI, la conectividad de extremo a extremo digital se obtendrá con plataforma y equipos usados en las redes ya existentes, tales como transmisión digital, conmutación múltiple por división en el tiempo y/o conmutación múltiple por división en el espacio. Las recomendaciones más relevantes existentes para estos elementos constitutivos se encuentran en las oportunas series de recomendaciones de CCITT y de CCIR.

2.4. En las primeras etapas de la evolución de las RDSI, en ciertos países es necesario adoptar algunos dispositivos usuario-red intermedios, para facilitar la pronta incorporación de los servicios digitales. Dispositivos correspondientes a variantes nacionales pueden cumplir parcial o totalmente las recomendaciones de las Series-I. Sin embargo, la intención es que no estén específicamente incluidos en las Series-I.

2.5. La evolución de la RDSI puede también incluir, en etapas posteriores, conexiones conmutadas a velocidades superiores e inferiores a 64 kbits.

La interfaz de usuario

La Figura A.1 es una visión conceptual de la RDSI desde el punto de vista del usuario o cliente. El usuario tiene acceso a la RDSI mediante una interfaz local a un «cauce digital» con una cierta razón de bits. Hay disponibles cauces de varios tamaños para satisfacer diferentes necesidades. Por ejemplo, un cliente residencial puede requerir sólo capacidad suficiente para gestionar un teléfono o un terminal de videotexto. Una oficina querrá sin duda conectarse a la RDSI vía PBX digital local, y requerirá un cauce de mucha más capacidad.

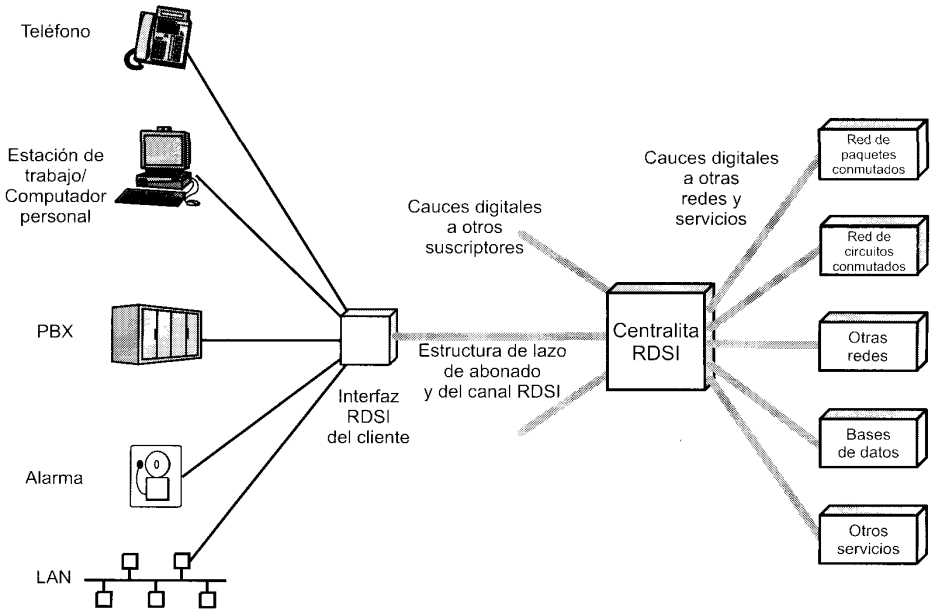


Figura A.1. Visión conceptual de las características de conexión de RDSI.

En cualquier momento, el cauce hacia las instalaciones del usuario tiene una capacidad fija, pero en el tráfico del cauce puede haber una mezcla variable hasta el límite de su capacidad. Así, un usuario puede acceder a los servicios de conmutación de circuitos y de conmutación de paquetes, así como a otros servicios, en una mezcla dinámica de tipos de señales y velocidades. Para suministrar estos servicios, la RDSI utiliza señales de control bastante complejas para indicar cómo ordenar los datos multiplexados en el tiempo y proporcionar los servicios solicitados. Estas señales de control están también multiplexadas en el mismo cauce digital.

Objetivos

El esfuerzo de la RDSI implica a gobiernos nacionales, compañías de comunicación y de procesamiento de datos, organizaciones de normalizaciones, y otras entidades. Algunos objetivos comunes son, en general, compartidos por estos grupos dispares. Enumeramos aquí los objetivos clave:

- **Normalización:** es esencial que se consiga un único conjunto de normalizaciones de RDSI para permitir un acceso universal y el desarrollo de equipos rentables.
- **Transparencia:** el servicio más importante que hay que proporcionar es un servicio de transmisión transparente. Esto permite a los usuarios desarrollar aplicaciones y protocolos con la confianza de que no se verán afectados por la RDSI subyacente.
- **Separación de funciones competitivas:** debe ser posible separar las funciones que pueden ser suministradas por el mercado libre y competitivo frente a aquellas que forman parte fundamental de la RDSI. En muchos países, una única entidad propiedad del gobierno suministra todos los servicios. Algunos países desean (en el caso de los Estados Unidos, se exige) que ciertos servicios suplementarios se ofrezcan competitivamente (por ej.; videotexto, correo electrónico).
- **Servicios alquilados y conmutados:** la RDSI debería proporcionar servicios punto a punto así como servicios conmutados. Esto permite al usuario optimizar la implementación de técnicas de enrutamiento y conmutación.

- **Tarifas relacionadas con el coste:** el precio de los servicios RDSI debería estar relacionado con el coste, y ser independiente del tipo de datos que se vayan a transportar. Un tipo de servicio no debería subvencionar a otros.
- **Adaptación paulatina:** la conversión a RDSI será gradual, y la evolución de la red debe coexistir con los equipos y sistemas existentes. Por tanto, las interfaces RDSI deberían evolucionar a partir de las interfaces actuales, y proporcionar vías de adaptación para los usuarios.
- **Soporte multiplexado:** además de proporcionar un soporte de baja capacidad para usuarios individuales, el soporte multiplexado debe adaptarse al PBX del usuario y a los equipos de red local.

Hay, por supuesto, otros objetivos que podríamos citar. Los que acabamos de enumerar están, ciertamente, entre los más importantes y ampliamente aceptados, y ayudan a definir el carácter de la RDSI.

ARQUITECTURA

La Figura A.2 es el diagrama de bloques de RDSI. RDSI contempla un nuevo conector físico para los usuarios, un bucle de abonado (unión entre el usuario final y la central u oficina terminal), y modificaciones para todos los equipos de la oficina central.

Se ha definido una interfaz física común para proporcionar, esencialmente, una conexión DTE-DCE. Se podría usar la misma interfaz para teléfono, computador, y videotexto. Se necesitan protocolos para el intercambio de información de control entre el usuario y la red. Se deben prever interfaces de alta velocidad para, por ejemplo, un PBX digital o una LAN.

La parte del bucle de abonado de la red telefónica actual consiste en enlaces de pares trenzados entre el abonado y la oficina central, llevando señales analógicas a 4 kHz. Bajo la RDSI de uno o dos pares trenzados se suele ofrecer un enlace básico de comunicación digital full-duplex.

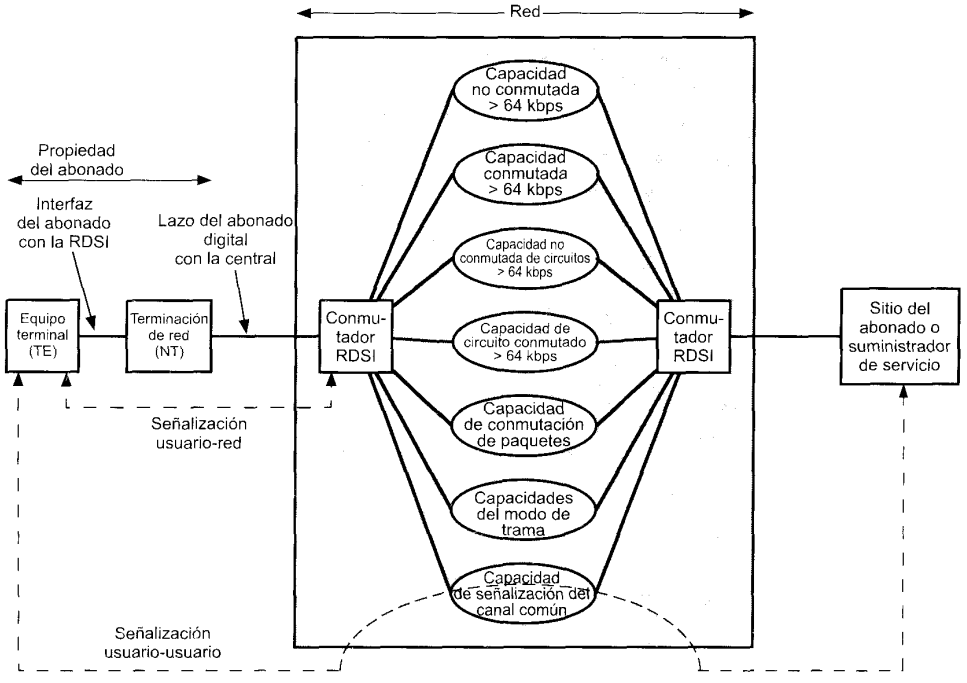


Figura A.2. Arquitectura RDSI.

La central digital conecta las numerosas señales del bucle de abonado RDSI con la red digital. Además de proporcionar un acceso a la red de conmutación de circuitos, la central proporciona acceso de abonado a líneas especiales, redes de conmutación de paquetes, y servicios de computadores orientados a transacción y a tiempo compartido. También debe adaptarse al acceso multiplexado vía PBX digital y LAN.

NORMALIZACIONES

El desarrollo de la RDSI está gobernado por un conjunto de recomendaciones dadas por la RDSI, llamadas series-I de recomendaciones. Estas recomendaciones o normalizaciones, se formularon por primera vez en 1984. En 1988, se hizo un conjunto más completo. La mayoría de las recomendaciones se han puesto al día, a intervalos irregulares, desde 1988. La mayor parte de la descripción de la RDSI se encuentra en las series-I de recomendaciones, con algún tema relacionado cubierto en otras recomendaciones. La caracterización de la RDSI contenida en estas recomendaciones se centra en tres áreas principales:

1. La normalización de servicios ofrecidos a los usuarios, así como la capacidad de los servicios de ser internacionalmente compatibles.
2. La normalización de las interfaces entre usuario y red, así como la capacidad de los equipos terminales para ser portátiles, y ayudar a (1).
3. La normalización de la capacidad de la RDSI hasta el grado necesario para permitir el trabajo entre usuario-red y red-red, y por tanto lograr (1) y (2).

Las series-I de recomendaciones se descomponen en seis grupos principales, llamados I.100 hasta I.700.

Serie I.100—Conceptos generales

La serie I.100 sirve como introducción general a la RDSI. La estructura general de las recomendaciones RDSI se presenta como un glosario de términos. I.120 proporciona una descripción general de la RDSI y la evolución esperada de las RDSI. I.130 introduce terminología y conceptos que se usan en la serie I.200 para especificar servicios.

Serie I.200—Capacidad de los servicios

La serie I.200 es en cierto sentido la parte más importante de las recomendaciones de la ITU-T RDSI. Aquí se especifican los servicios que se van a ofrecer a los usuarios. Podemos ver esto como un conjunto de requisitos que la RDSI debe satisfacer. En el glosario de la RDSI (I.112), el término *servicio* se define como:

> Lo que ofrece una administración o un ente privado reconocido (RPOA, Recognized Private Operating Agency) a sus clientes para satisfacer una demanda de telecomunicación específica.

Aunque ésta es una definición muy general, el término *servicio* ha pasado a tener un significado muy específico en ITU-T, un significado que es en cierto modo diferente al uso de este término en un contexto OSI. Para ITU-T, un servicio normalizado se caracteriza por:

- Compatibilidad, de un extremo a otro, completa y garantizada.
- Terminales normalizados ITU-T, incluyendo procedimientos.
- Listado de los servicios subscritos en un directorio internacional.
- Procedimientos de mantenimiento y verificación normalizados ITU-T.
- Reglas de cobro y contabilidad.

Hay tres servicios ITU-T completamente normalizados: telegrafía, telefonía, y datos. Hay cuatro servicios *telemáticos* adicionales en proceso de normalización: teletexto, fax, videotexto, y gestión de men-

sajes. El objetivo con todos estos servicios es asegurar telecomunicaciones internacionales de alta calidad para el usuario final, sin importar la forma del equipo terminal y el tipo de red usados nacionalmente para soportar estos servicios.

Serie I.300—Aspectos de la red

Mientras que la serie I.200 se centra en el usuario, en términos de los servicios ofrecidos al usuario, la serie I.300 se centra en la red, en términos de cómo la red proporciona esos servicios. Un modelo de referencia de un protocolo se presenta de forma que, además de seguir el modelo OSI de 7 capas, intenta hacer frente a la complejidad de una conexión que pueda implicar a dos o más usuarios (por ejemplo, una conferencia telefónica) más un diálogo de señalización en un canal común relacionado. Se cubren temas tales como numeración y direccionamiento. Incluye también una discusión de los tipos de conexiones RDSI.

Serie I.400—Interfaces usuario-red

La serie I.400 se ocupa de la interfaz entre el usuario y la red. Se consideran tres temas principales:

- **Configuraciones físicas:** la manera en que se configuran las funciones RDSI en los equipos. La normalización especifica grupos funcionales y define puntos de referencia entre esos grupos.
- **Velocidades de transmisión:** las velocidades de los datos y las combinaciones de velocidades de datos que se van a ofrecer al usuario.
- **Especificaciones de protocolo:** los protocolos de las capas OSI del 1 al 3 que especifican la interacción usuario-red.

Serie I.500—Interfaces entre redes

RDSI contiene servicios que también proporcionaban las antiguas redes de conmutación de circuitos y de conmutación de paquetes. Así, es necesario que haya interconexión entre RDSI y otros tipos de redes para permitir la comunicación entre terminales pertenecientes a servicios equivalentes ofrecidos a través de distintas redes. La serie I.500 se ocupa de varios temas de la red que surgen al intentar definir interfaces entre RDSI y otros tipos de redes.

Serie I.600—Principios de mantenimiento

Esta serie proporciona una guía para el mantenimiento de la instalación del abonado a RDSI, la parte de la red de accesos básicos, accesos primarios y servicios de datos de velocidad más alta de RDSI. Los principios y funciones de mantenimiento están relacionados con la configuración y arquitectura general de RDSI. Una función clave identificada en la serie es la de bucle realimentado. En general, los tests de bucle realimentado se usan para localización y verificación de fallos.

Serie I.700—Aspectos de los equipos RDSI-BA

Esta serie fue introducida por primera vez en 1996. Cubre el funcionamiento y las características de equipo ATM y varios aspectos de gestión.

A.2. CANALES RDSI

El cauce digital entre la central y el usuario RDSI se usa para aportar varios canales de comunicación. La capacidad del cauce, y por tanto el número de canales incluidos, puede variar de un usuario a otro.

La estructura de la transmisión de cualquier punto de acceso se construye según los siguientes tipos de canales:

- **Canal B:** 64 kbps
- **Canal D:** 16 o 64 kbps
- **Canal H:** 384 (H0), 1536 (H11), y 1920 (H12) kbps

El **canal B** es el canal básico del usuario. Se puede usar para transferir datos digitales, voz digital codificada PCM, o una mezcla de tráfico de baja velocidad, incluyendo datos digitales y voz digitalizada decodificada a una velocidad de 64 kbps. En el caso de tráfico mixto, se debe destinar todo el tráfico al mismo punto final. En un canal B se pueden establecer cuatro tipos de conexiones:

- **Circuito conmutado:** es el equivalente al servicio digital conmutado disponible actualmente. El usuario hace una llamada y se establece una conexión de circuito conmutado con otro usuario de la red. Una característica interesante es que el diálogo de establecimiento de la llamada no tiene lugar en el canal B, sino en el D, como explicaremos a continuación.
- **Paquetes conmutados:** el usuario se conecta a un nodo de conmutación de paquetes, y los datos se intercambian con otros usuarios vía X.25.
- **Modo de trama:** el usuario se conecta a un nodo de retransmisión de tramas, y los datos se intercambian con otros usuarios vía LAPF.
- **Semipermanente:** es una conexión con otro usuario establecida anteriormente, y no requiere un protocolo de establecimiento de llamada. Es equivalente a una línea alquilada.

La designación de 64 kbps como velocidad estándar del canal de usuario destaca la contradicción fundamental en las actividades de normalización. Se escogió esta velocidad como la más efectiva para voz digitalizada, a pesar de que la tecnología ha progresado hasta el punto de que a 32 kbps o incluso menos se consigue una reproducción de la voz igualmente satisfactoria. Para que sea efectiva, una normalización debe considerar («congelar») la tecnología en una situación temporal concreta. Por eso, en el momento en que la normalización se aprueba, puede estar ya obsoleta.

El **canal D** tiene dos finalidades. Primero, lleva información de señalización para controlar las llamadas de circuitos conmutados asociadas con los canales B en la interfaz de usuario. Además, el canal D puede usarse para conmutación de paquetes o telemetría de baja velocidad (por ej.: 100 bps) mientras no haya esperando información de señalización. La Tabla A.2 resume los tipos de tráfico de datos que pueden admitir los canales B y D.

Los **canales H** están para información de usuario a altas velocidades. El usuario puede usar este canal como una línea de alta velocidad o subdividir el canal de acuerdo con el propio esquema TDM del usuario. Ejemplos de aplicaciones incluyen fax rápido, vídeo, datos a alta velocidad, audio de alta calidad, y flujos múltiples de información con velocidad de datos inferior.

Tabla A.2. Funciones del canal RDSI.

Canal B (64 kbps)	Canal D (16 kbps)
Voz digital PCM a 64 kbps Velocidad baja (32 Kbps)	**Señalización** Básica Mejorada
Velocidad de datos alta Circuito conmutado Paquete conmutado	**Velocidad de datos baja** Videotexto Teletexto Terminal
Otros Facsímil Vídeo de barrido lento	**Telemetría** Servicios de emergencia Gestión de energía

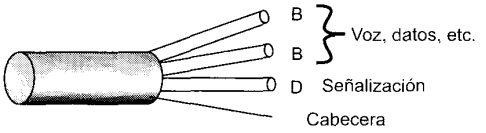
Estos tipos de canales se agrupan en estructuras de transmisión que se ofrecen como paquetes al usuario. Las estructuras mejor definidas en este momento son la estructura de canal básico (acceso básico) y la estructura de canal primario (acceso primario), que se muestran en la Figura A.3.

El **acceso básico** consiste en dos canales B full-duplex de 64 kbps y dos canales D full-duplex de 16 kbps. La razón de bits total, por simple aritmética, es 144 kbps. Sin embargo, la división en tramas, la sincronización, y otros bits adicionales dan una velocidad total a un punto de acceso básico de 192 kbps. La estructura de la trama para un acceso básico se mostró en la Figura 8.10. Cada trama de 48 bits incluye 16 bits en cada canal B y 4 bits en el canal D.

El servicio básico intenta satisfacer las necesidades de la mayoría de los usuarios individuales, incluyendo viviendas y pequeñas oficinas. Esto permite el uso simultáneo de voz y varias aplicaciones de datos, como acceso a conmutación de paquetes, conexión al servicio de alarma central, fax, videotexto, etc. Se puede acceder a estos servicios a través de un terminal multifunción único o de varios terminales separados. En ambos casos, se proporciona una interfaz física única. La mayoría de los enlaces locales de dos pares pueden admitir esta interfaz.

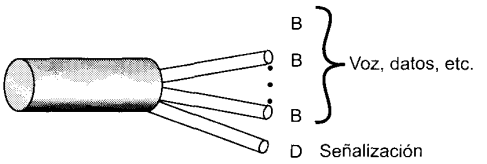
En algunos casos uno o ambos canales B permanecen sin usarse. Esto da lugar a una interfaz B + D o D, en lugar de una interfaz 2B + D. Sin embargo, para simplificar la implementación de la red, la velocidad de los datos en la interfaz permanece a 192 kbps. No obstante, para aquellos abonados con requisitos de transmisión más modestos, puede haber un ahorro en el coste usando una interfaz básica reducida.

El **acceso primario** está destinado a usuarios con requisitos de capacidad mayores, tales como oficinas con PBX digital o red local. Debido a las diferencias en las jerarquías de transmisión digital usadas en distintos países, no es posible lograr un acuerdo en una única velocidad de los datos. Estados Unidos, Canadá y Japón usan una estructura de transmisión basada en 1,544 Mbps; esto corresponde a la transmisión T1 usando el formato de transmisión DS-1. En Europa, la velocidad estándar es de 2,048 Mbps.



Composición: 192 kbps: 2 canales B a 64 kbps cada uno
1 canal D a 16 kbps
Bits de sincronización y delimitación de tramas

(a) Servicio básico



Composición: 2,048 Mbps: 30 canales B a 64 kbps cada uno
1 canal D a 64 kbps
1,544 Mbps: 23 canales B a 64 kbps cada uno
1 canal D a 64 kbps

(b) Servicio primario

Figura A.3. Estructura de canal RDSI.

Ambas velocidades se proporcionan como un servicio de interfaz primaria. Generalmente, la estructura para el canal de 1,544 Mbps es 23 canales B más un canal D de 64 kbps y, para velocidades de 2,048 Mbps, 30 canales B más un canal D de 64 kbps. De nuevo, es posible para un cliente con menos requerimientos, emplear menos canales B, en cuyo caso la estructura del canal es nB + D, donde n varía entre 1 y 23 o entre 1 y 30 para los dos servicios primarios. También, a un cliente con demanda de altas velocidades de datos se le puede proporcionar más de una interfaz física primaria. En este caso, puede ser suficiente un único canal D en una de las interfaces, para satisfacer todas las necesidades de señalización, y las otras interfaces pueden constar solamente de canales B (24 B o 31 B). La estructura de la trama para acceso primario se muestra en la Figura 8.11.

La interfaz primaria también se puede usar para soportar canales H. Algunas de estas estructuras incluyen un canal D de 64 kbps para señalización de control. Cuando no hay presente un canal D, se supone que un canal D en otra interfaz primaria, en la misma posición del abonado, proporcionará cualquier señalización que se requiera. Se reconocen las siguientes estructuras:

- **Estructuras del canal H0 con interfaz de velocidad primaria:** esta interfaz admite canales H0 a 384 kbps múltiples. Las estructuras son 3H0 + D y 4H0 para la interfaz a 1,544 Mbps y 5H0 + D para la interfaz a 2,048 Mbps.
- **Estructuras del canal H1 con interfaz de velocidad primaria:** la estructura del canal H11 consiste en un canal H11 a 1536 kbps. La estructura del canal H12 consta de un canal H12 a 1920 kbps y un canal D.
- **Estructuras con interfaz de velocidad primaria para mezcla de canales B y H0:** consta de uno o ningún canal D más cualquier combinación posible de canales B y H0 hasta el límite de la capacidad de la interfaz física (por ej.: 3H0 + 5B + D y 3H0 + 6B).

A.3. ACCESO DEL USUARIO

Para definir los requisitos de acceso del usuario a RDSI, es muy importante comprender la configuración anticipada de los equipos del usuario y de las interfaces normalizadas necesarias. El primer paso es agrupar funciones que pueden existir en el equipo del usuario. La Figura A.4 muestra la aproximación CCITT de esta tarea, usando:

- **Agrupaciones funcionales:** ciertas disposiciones finitas de equipos físicos o combinaciones de equipos.
- **Puntos de referencia:** puntos conceptuales usados para separar grupos de funciones.

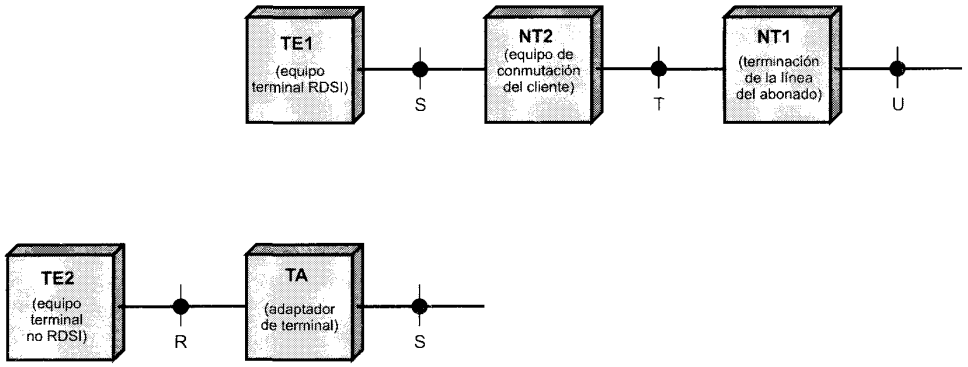


Figura A.4. Puntos de referencia RDSI y grupos funcionales.

La arquitectura del equipo de abonado se divide funcionalmente en grupos separados por puntos de referencia. Esto permite a las interfaces normalizadas desarrollarse en cada punto de referencia. Esto organiza eficazmente el trabajo sobre normalizaciones y proporciona una guía a los suministradores de equipos. Una vez que existe una normalización estable de interfaz, se pueden hacer mejoras técnicas en ambos lados de la interfaz sin impacto en los grupos funcionales adyacentes. Finalmente, con interfaces estables, el abonado es libre de conseguir equipos de diferentes suministradores para varios grupos funcionales, siempre que el equipo se ajuste a las normalizaciones de interfaz apropiadas.

La **Terminación de red 1 (NT1)** incluye funciones asociadas a la terminación física y eléctrica de la RDSI en los equipos del usuario; éstas corresponden a la capa 1 de OSI. La NT1 puede ser controlada por el suministrador RDSI y constituye una frontera en la red. Esta frontera aísla al usuario de la tecnología de transmisión del lazo de abonado y presenta una interfaz de conexión física para la conexión al dispositivo del usuario. Además, la NT1 realiza funciones de mantenimiento de línea, como la verificación de bucle realimentado, y controla la ejecución. La NT1 soporta canales múltiples (por ej.; 2B + D); en el nivel físico, el flujo de bits de estos canales se multiplexa conjuntamente, usando multiplexación por división del tiempo síncrona. Finalmente, la interfaz NT1 puede soportar dispositivos múltiples en una distribución multiconexión. Por ejemplo, una interfaz personal podría incluir un teléfono, un computador personal, y un sistema de alarma, todo ello conectado a una única interfaz NT1 vía línea multiconexión.

La **Terminación de red 2 (NT2)** es un dispositivo inteligente que realiza funciones de concentración y conmutación; puede incluir las funciones consideradas en el modelo OSI, hasta la capa 3. Ejemplos de NT2 son un PBX digital, un controlador de terminal, y una LAN. Un ejemplo de función de conmutación es la construcción de una red privada usando circuitos semipermanentes entre una serie de sitios. Cada sitio puede incluir un PBX que actúa como circuito de conmutación o un computador huésped que actúa como conmutador de paquetes. La función de concentración simplemente significa que varios dispositivos, conectados a un PBX digital, LAN, o controlador de terminal, puede transmitir datos a través de RDSI.

La **Terminación de red 1, 2 (NT12)** es una sola pieza de un equipo que contiene funciones combinadas de NT1 y NT2. Esto señala uno de los temas normativos asociados con el desarrollo de la interfaz RDSI. En muchos países, el suministrador RDSI poseerá el NT12 y proporcionará un servicio completo al usuario. En Estados Unidos, es necesario que haya una terminación de red con un número limitado de funciones para permitir un mercado competitivo de equipos de usuarios. Por tanto, las funciones de red de los equipos del usuario se reparten entre la NT1 y la NT2.

El equipo terminal es el equipo del abonado que usa RDSI. Se definen dos tipos. El **equipo terminal de tipo 1 (TE1)** son dispositivos que soportan la interfaz RDSI normalizada. Como ejemplos tenemos teléfonos digitales, terminales de voz/datos integrados, y equipos de fax digitales. El equipo terminal de tipo 2 (TE2) contempla la existencia de equipos no RDSI. Por ejemplo, tenemos terminales con una interfaz física tal como EIA-232-F y computadores huésped con una interfaz X.25. Tal equipo requiere un adaptador de terminal (TA) para conectarse a la interfaz RDSI.

Las definiciones de las agrupaciones funcionales también definen, por implicación, puntos de referencia. El **punto de referencia T** (terminal) corresponde a la mínima terminación de red RDSI del equipo del cliente. Separa el equipo del proveedor de red del equipo del usuario. El **punto de referencia S** (sistema) corresponde a la interfaz de terminales individuales RDSI. Separa el equipo terminal del usuario de las funciones de comunicación relacionadas con la red. El **punto de referencia R** (velocidad) proporciona una interfaz no RDSI entre el equipo del usuario, que no es RDSI compatible, y el equipo adaptador. Normalmente, esta interfaz cumplirá con la normalización de interfaz más antigua, tal como EIA-232-E.

A.4. PROTOCOLOS RDSI

ARQUITECTURA DEL PROTOCOLO RDSI

La Figura A.5 ilustra, en el contexto del modelo OSI, los protocolos que se definen o a los que se hace referencia en los documentos RDSI. Como una red, RDSI es esencialmente indiferente a las capas de usuario de la 4 a la 7. Son capas de extremo a extremo empleadas por el usuario para intercambio de información. El acceso a red concierne únicamente a las capas de la 1 a la 3. La capa 1, definida en I.430 e I.431, especifica la interfaz física tanto para el acceso básico como primario. Como los canales B y D están multiplexados en la misma interfaz física, estas normalizaciones se aplican a ambos tipos de canales. Encima de esta capa, la estructura del protocolo difiere para los dos canales.

Para el canal D, se ha definido una nueva normalización de capa de enlace de datos, LAPD (protocolo de acceso de enlace, «Link Access Protocol», canal D). Esta normalización se basa en HDLC, modificado para cumplir los requisitos RDSI. Toda transmisión en el canal D se da en forma de tramas LAPD que se intercambian entre el equipo abonado y un elemento de conmutación RDSI. Se consideran tres aplicaciones: señalización de control, conmutación de paquetes, y telemetría. Para **señalización de control,** se define un protocolo de llamada (I.451/Q.931). Este protocolo se usa para establecer, mantener y finalizar conexiones en canales B. Por tanto, es un protocolo entre el usuario y la red. Sobre la capa 3, existe la posibilidad de funciones de capas más altas asociadas con la señalización de control usuario a usuario. Esto es tema para un estudio posterior. El canal D puede usarse también para proporcionar servicios de **conmutación de paquetes** para el abonado. En este caso, se usa el protocolo del nivel 3 de X.25, y los paquetes X.25 se transmiten en tramas LAPD. El protocolo del nivel 3 de X.25 se usa para establecer circuitos virtuales en el canal D para otros usuarios y para intercambiar datos empaquetados. La última área de aplicación, **telemetría,** es tema para estudio posterior.

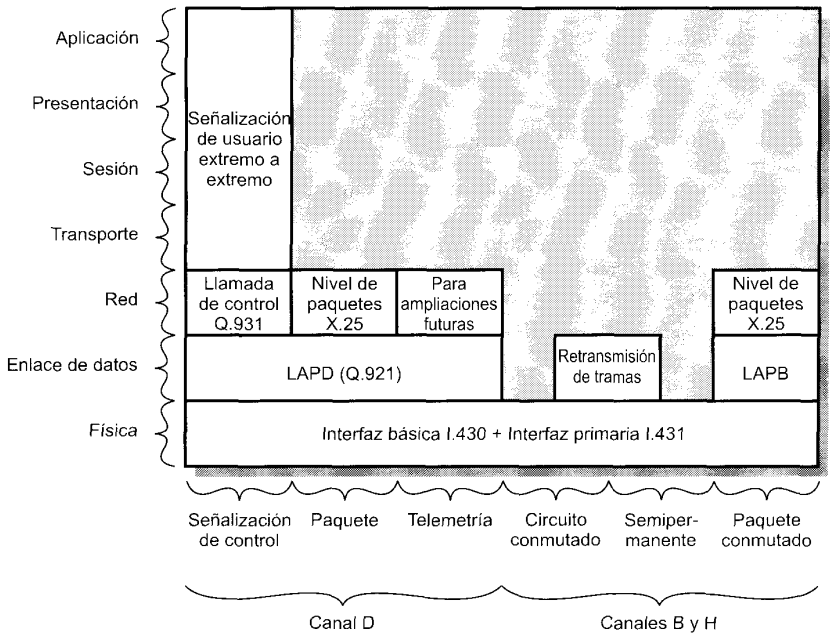


Figura A.5. Protocolos RDSI en la interfaz usuario-red.

El canal B se puede usar para conmutación de circuitos, circuitos semipermanentes, y conmutación de paquetes. Para **conmutación de circuitos,** se construye un circuito en un canal B bajo demanda. El protocolo de control de llamada del canal D se usa para este fin. Una vez establecido el circuito, se puede usar para transferencia de datos entre usuarios. Un **circuito semipermanente** es un circuito canal B que se ha establecido previo acuerdo entre los usuarios conectados y la red. Como con una conexión de circuito conmutado, proporciona un camino transparente de datos entre sistemas terminales.

Tanto con una conexión de circuito conmutado como con de circuito semipermanente, las estaciones conectadas intercambian información como si se hubiese establecido un enlace directo full-duplex. Son libres para usar sus propios formatos, protocolos y sincronización de tramas. Por tanto, desde el punto de vista de RDSI, las capas del 2 al 7 no son visibles o no están especificadas.

En el caso de **conmutación de paquetes,** se establece una conexión de circuito conmutado en un canal B entre el usuario y el nodo del paquete conmutado usando el protocolo de control del canal D. Una vez que el circuito se establece en el canal B, el usuario puede emplear X.25 en las capas 2 y 3 para establecer un circuito virtual con otro usuario del canal e intercambiar datos en paquetes. Como alternativa, se puede usar el servicio de retransmisión de tramas. La retransmisión de tramas se puede usar también en canales H y D.

Algunos de los protocolos mostrados en la Figura A.5 se resumen en lo que queda de esta sección. Primero, veremos la forma en la que se establecen las conexiones de paquetes conmutados y circuitos conmutados. Después, examinaremos el protocolo de señalización de control y luego LAPD. Finalmente, revisaremos las especificaciones de la capa física.

CONEXIONES RDSI

RDSI proporciona cuatro tipos de servicios para comunicación de un extremo a otro:

- Celdas de circuitos conmutados en un canal B.
- Conexiones semipermanentes en un canal B.
- Llamadas de paquetes conmutados en un canal B.
- Llamadas de paquetes conmutados en el canal D.

Llamadas de circuitos conmutados

La configuración de red y protocolos para conmutación de circuitos implican tanto al canal B como al D. El canal B se usa para el intercambio transparente de datos del usuario. Los usuarios que se comunican pueden usar cualquier protocolo que deseen para comunicación de extremo a extremo. El canal D se usa para intercambiar información de control entre el usuario y la red para establecimiento y finalización de llamadas, y para acceso a las instalaciones de la red.

El canal B es mantenido por un NT1 o NT2 usando sólo funciones de la capa 1. En el canal D, se usa un protocolo de acceso a la red de tres capas que se explica a continuación. Finalmente, el proceso de establecimiento de un circuito a través de RDSI implica la cooperación de conmutadores internos a RDSI para establecer la conexión. Estos conmutadores interactúan usando un protocolo interno, sistema de señalización número 7.

Conexiones semipermanentes

Una conexión semipermanente entre puntos predeterminados, se puede proporcionar para un periodo de tiempo indefinido después de la suscripción, para un periodo fijo, o para periodos predeterminados durante un día, semana u otro intervalo. Como con conexiones de conmutación de circuitos, la interfaz de red proporciona sólo la Capa 1. El protocolo de control de llamada no se necesita porque la conexión ya existe.

Llamadas de paquetes conmutados a través de un canal B

La RDSI debe también permitir acceso al usuario a servicios de paquetes conmutados para tráfico de datos (por ej.: interactivo) que se mantiene de la mejor forma con conmutación de paquetes. Hay dos posibles implementaciones de este servicio: o una red diferente proporciona la capacidad de conmutación de paquetes, llamada red pública de datos de paquetes conmutados (PSPDN), o la capacidad de conmutación de paquetes se integra en RDSI. En el primer caso, el servicio se da sobre un canal B. En el último caso, el servicio se puede dar sobre un canal B o D. Primero examinaremos el uso del canal B para paquetes conmutados.

Cuando una PSPDN proporciona el servicio de conmutación de paquetes, el acceso a tal servicio se hace vía canal B. Tanto el usuario como el PSPDN deben, por tanto, estar conectados como abonados a RDSI. En el caso de PSPDN, uno o más de los nodos de red de conmutación de paquetes, llamados gestores de paquetes, están conectados a RDSI. Podemos concebir cada uno de estos nodos como un DCE X.25 tradicional más la lógica necesaria para acceder a RDSI. Es decir, el abonado RDSI desempeña el papel de un DTE X.25, el nodo en el PSPDN al que está conectado funciona como un DCE X.25, y la RDSI simplemente proporciona la conexión del DTE al DCE. Cualquier abonado a RDSI puede entonces comunicarse, vía X.25, con cualquier otro usuario conectado al PSPDN, incluyendo:

- Usuarios con una conexión directa, permanente a PSPDN.
- Usuarios de RDSI que actualmente disfruten de una conexión, a través de RDSI, en PSPDN.

La conexión entre el usuario (vía un canal B) y el gestor de paquetes con el que se comunica puede ser tanto semipermanente como de circuito conmutado. En el primer caso, la conexión está siempre ahí y el usuario puede libremente llamar al X.25 para establecer un circuito virtual con otro usuario. En el otro caso, está implicado el canal D, y tienen lugar los siguientes pasos (Figura A.6):

1. El usuario pide, vía protocolo de llamada del canal D (I.451/Q.931), una conexión de circuito conmutado en un canal D al gestor de paquetes.

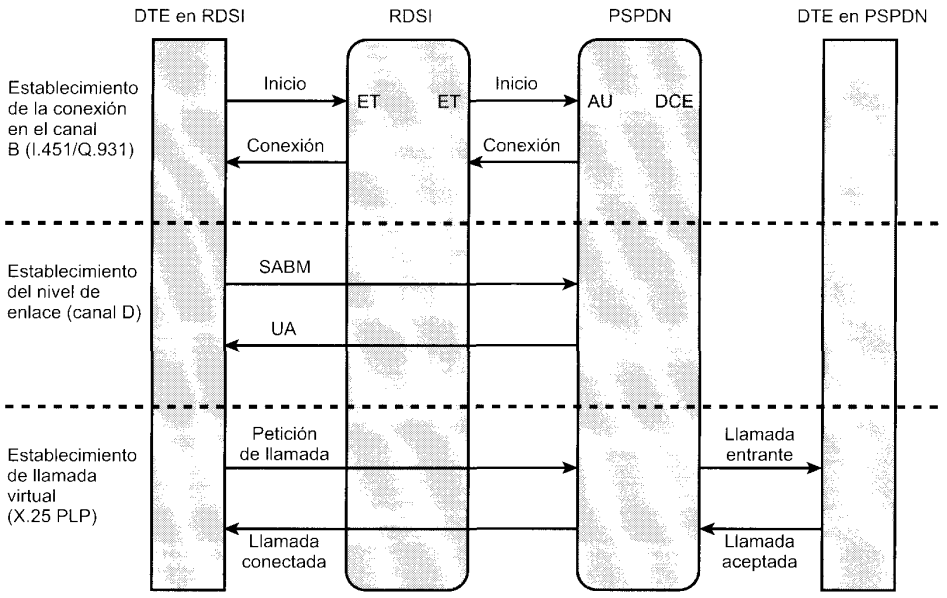
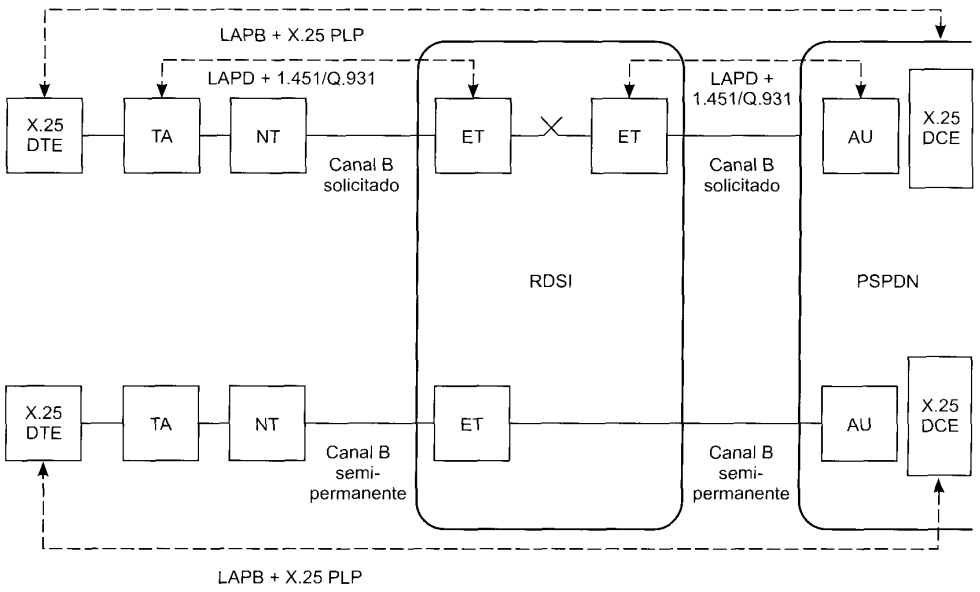


Figura A.6. Inicio de llamada virtual.

2. La conexión la establece RDSI y se le notifica al usuario vía protocolo de llamada del canal D.
3. El usuario establece un circuito virtual con otro usuario vía procedimiento de establecimiento de llamada X.25 en canal B (descrito en la Sección A.4). Esto requiere que primero se establezca una conexión de enlace de datos, usando LAPB, entre el usuario y el gestor de paquetes.
4. El usuario cancela el circuito virtual usando X.25 en el canal B.
5. Después de una o más llamadas virtuales en el canal B, el usuario está servido y señala vía canal D que termina la conexión de circuito conmutado al nodo de conmutación de paquetes.
6. RDSI termina la conexión.

La Figura A.7 muestra la configuración implicada en la realización de este servicio. En la figura, al usuario se le muestra cómo usar un dispositivo DTE que cuenta con una interfaz con un DCE X.25. Por tanto, se requiere un adaptador de terminal. Por otra parte, la capacidad del X.25 puede ser una función integrada de un dispositivo RDSI TE1, prescindiendo de la necesidad de un TA separado.

Cuando RDSI proporciona un servicio de conmutación de paquetes, la función de manipulación del paquete se hace dentro de la RDSI, ya sea con un equipo independiente o como parte de un equipo de intercambio. El usuario puede conectarse al gestor de paquetes tanto por un canal B como D. En un canal B, la conexión al gestor de paquetes puede ser conmutada o semipermanente, y se aplican los mismos procedimientos descritos anteriormente para conexiones conmutadas. En este caso, en lugar de establecer una conexión canal B con otro abonado RDSI que es un gestor de paquetes PSPDN, la conexión se hace a un elemento interno de RDSI que es un gestor de paquetes.



Leyenda:

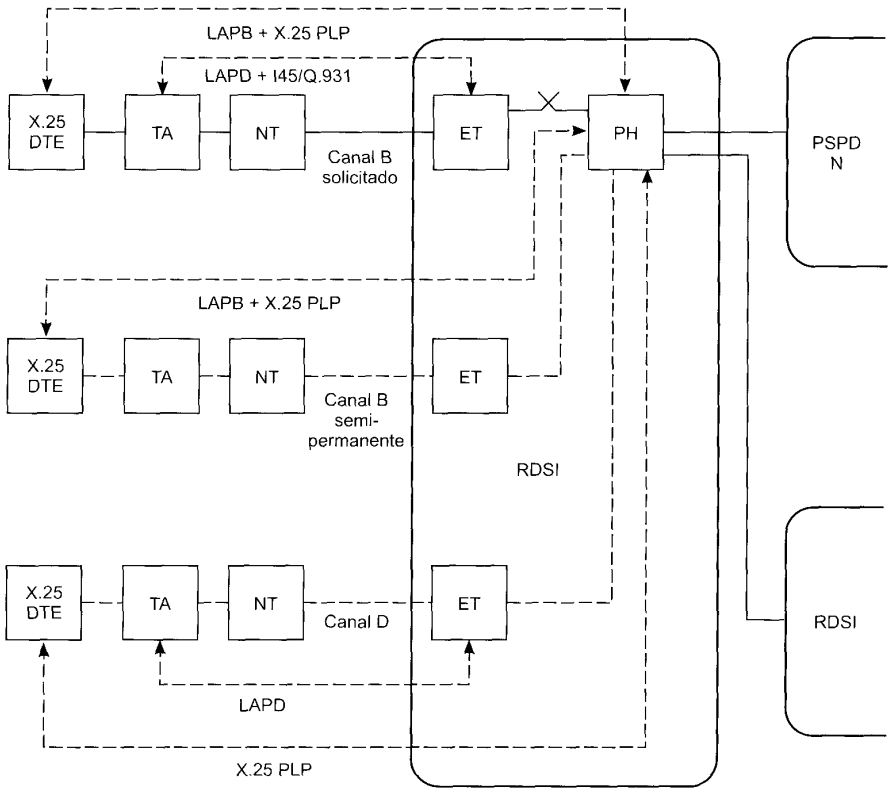
AU = Unidad de acceso RDSI
TA = Adaptador de terminal
NT = Terminación de red 2 y/o 1
ET = Terminación de intercambio
PLP = Procedimiento a nivel de paquete
PSPDN = Red pública de datos de paquetes conmutados

Figura A.7. Acceso a PSPDN del servicio en modo paquete.

Llamadas de paquetes conmutados a través de un canal D

Cuando se proporciona un servicio de conmutación de paquetes interno a RDSI, también se puede acceder a él a través del canal D. Para el acceso al canal D, RDSI proporciona una conexión semipermanente a un nodo de conmutación de paquetes dentro de RDSI. El usuario emplea el protocolo de nivel 3 de X.25 como se hizo en el caso de una llamada virtual canal B. Aquí, las tramas LAPD llevan el protocolo de nivel 3. Como el canal D se usa también para señalización de control, hay que distinguir de alguna forma entre el tráfico de paquetes X.25 y el tráfico de control RDSI. Éste se lleva a cabo mediante el esquema de direccionamiento de la capa de enlace, como se explicó anteriormente.

La Figura A.8 muestra la configuración para conseguir conmutación de paquetes en RDSI. El servicio de conmutación de paquetes proporcionado internamente a RDSI sobre canales B y D es lógicamente suministrado por una única red de conmutación de paquetes. Entonces, se pueden establecer llamadas virtuales entre dos usuarios de canal D, dos usuarios de canal B, y entre un usuario de canal B y otro de D. Además, es usual dar acceso a los usuarios X.25 en otros RDSI y PSPDN mediante procedimientos de interconexión de redes apropiados.



Leyenda:

TA = Adaptador de terminal
NT = Terminación de red 2 y/o 1
ET = Terminación de intercambio
PLP = Procedimiento a nivel de paquete
PSPDN = Red pública de datos de paquetes conmutados
PH = Función de gestión de paquetes

Figura A.8. Acceso a RDSI para servicios modo paquete.

SEÑALIZACIÓN DE CANAL COMÚN EN LA INTERFAZ RED-USUARIO RDSI

ITU-T ha desarrollado una normalización, Q.931, para señalización de canal común. La aplicación primaria de esta normalización es para la red digital de servicios integrados (RDSI). En términos OSI, Q.931 es una capa 3, o un protocolo de capa de red. Como la Figura A.9 indica, Q.931 se basa en el protocolo de nivel de enlace para transmitir mensajes a través del canal D. Q.931 especifica procedimientos para establecer conexiones en canales B que compartan la misma interfaz física que RDSI con el canal D. También proporciona señalización de control usuario-usuario a través del canal D.

El proceso de establecimiento, control y finalización de una llamada se produce como resultado de los mensajes de señalización de control intercambiados entre el usuario y la red a través del canal D. Se usa un formato común para todos los mensajes definidos en Q.931, como se ilustra en la Figura A.10a. Todos los mensajes tienen tres campos en común:

- **Discriminador de protocolos:** usado para distinguir mensajes de control de llamada usuario-red de otros tipos de mensajes. Otros tipos de protocolos pueden compartir un canal de señalización común.
- **Referencia de llamada:** identifica la llamada usuario-canal a la que el mensaje se refiere. Como con números de circuitos virtuales X.25, sólo tiene significado local. El campo de referencia de llamada tiene 3 subcampos. El subcampo de longitud especifica la longitud del resto del campo en octetos. Esta longitud es un octeto para una interfaz de velocidad básica, y dos octetos para una interfaz de velocidad primaria. El indicador especifica qué extremo de la conexión lógica LAPD inició la llamada.
- **Tipo de mensaje:** identifica qué mensaje Q.931 se está enviando. El contenido del resto del mensaje depende del tipo de mensaje.

Siguiendo estos tres campos comunes, el resto del mensaje consiste en una secuencia de ceros o más elementos de información o parámetros. Éstos contienen información adicional que va con el mensaje. Por tanto, el tipo de mensaje especifica una orden o respuesta, y los elementos de información proporcionan los detalles. Algunos elementos de información deben incluirse siempre con un mensaje dado (obligatorios), y otros son opcionales (adicionales). Se usan tres formatos para los elementos de información, como se indica en las Figuras de A.10b a d.

La Tabla A.3 enumera los mensajes Q.931. Los mensajes se pueden agrupar en dos dimensiones. Los mensajes valen para una de estas cuatro aplicaciones: control modo circuito, control de conexión de acceso modo paquete, señalización usuario-usuario no asociada con llamadas de circuitos conmutados, y mensajes usados con referencia de llamada global. Además, los mensajes llevan a cabo funciones de una de estas cuatro categorías: establecimiento de llamada, información de llamada, finalización de llamada, y varios.

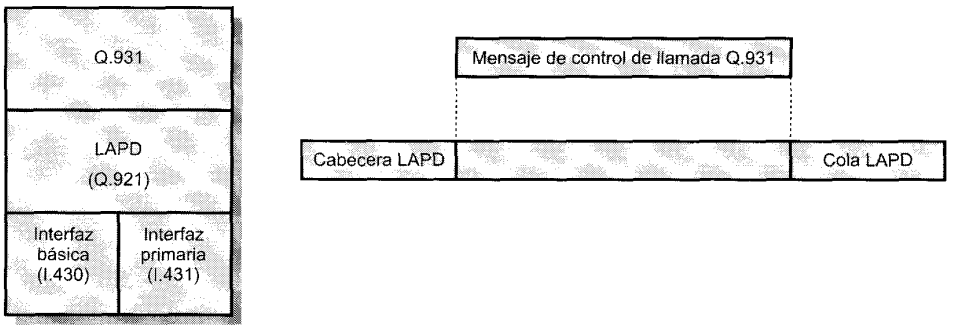


Figura A.9. Arquitectura del protocolo de control de llamadas.

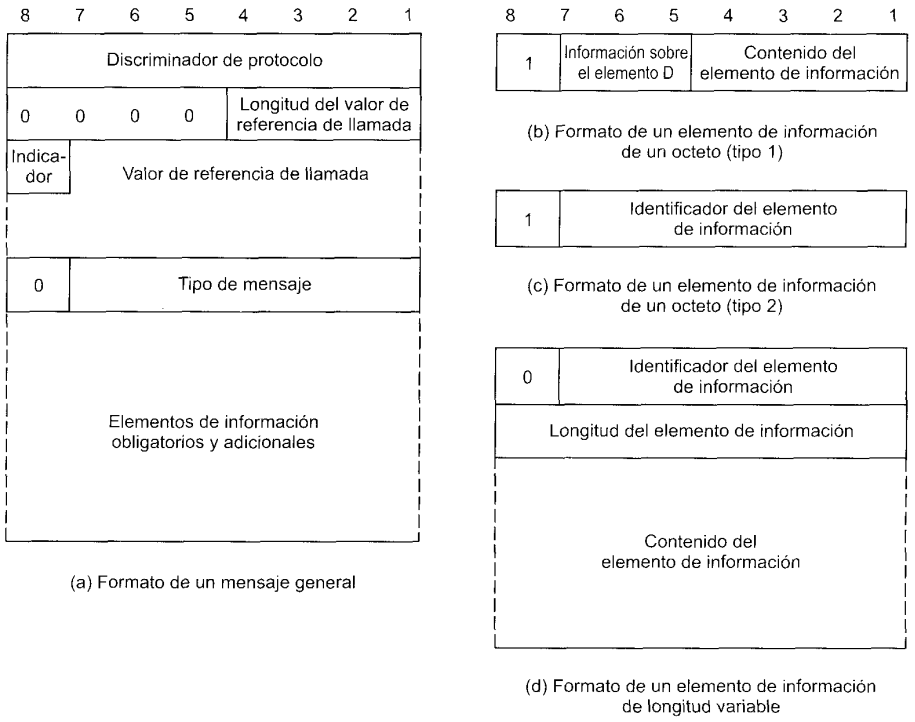


Figura A.10. Formatos Q.931.

Control modo circuito son las funciones que se necesitan para establecer, mantener, y terminar una conexión de circuito conmutado en un canal de usuario. Esta función corresponde al control de llamada redes de telecomunicaciones de conmutación de circuitos existentes. **Control de conexión de acceso modo paquete** son las funciones que se necesitan para establecer una conexión de circuito conmutado (llamado una conexión de acceso en este contexto) en un nodo de conmutación de paquetes RDSI; éste conecta el usuario a la red de conmutación de paquetes proporcionada por el proveedor RDSI. Los mensajes de **señalización usuario-usuario** permiten a dos usuarios comunicarse sin establecer una conexión de circuito conmutado. Una conexión de señalización temporal se establece y termina de forma similar al control de una conexión de circuito conmutado. La señalización tiene lugar a través del canal de señalización y no consume recursos del canal de usuario. Finalmente, una referencia a llamada global son las funciones que habilitan al usuario o a la red a devolver uno o más canales a la condición de desocupados.

Los mensajes de establecimiento de llamada se usan para iniciar una llamada. Este grupo incluye mensajes entre el terminal de llamada y la red y entre la red el terminal al que se llama. Estos mensajes soportan los siguientes servicios:

- Establecimiento de una llamada usuario-canal en respuesta a una petición del usuario.
- Suministro de recursos de red particulares para esta llamada.
- Información al usuario que llama sobre el avance del proceso del establecimiento de la llamada.

Una vez establecida una llamada, pero antes de la fase de desestablecimiento (terminación), los mensajes de la fase de **información de llamada** se envían entre usuario y red. Uno de los mensajes de este grupo permite a la red retransmitir, sin modificación, la información entre los dos usuarios de la

Tabla A.3. Mensajes I.451/Q.931 para control de conexiones en modo circuito.

Mensaje	Significado	Dirección	Funcionamiento
Mensajes de establecimiento de llamada			
ALERTA	global	ambos	Indica que la alerta del usuario ha empezado
LLAMADA EN CURSO	local	ambos	Indica que se ha iniciado el establecimiento de la llamada
CONEXIÓN	global	ambos	Indica aceptación de llamada por el TE llamado
RECONOCIMIENTO DE CONEXIÓN	local	ambos	Indica que se le ha concedido la llamada al usuario
PROGRESO	global	ambos	Informa del progreso de una llamada
INICIO	global	ambos	Indica el establecimiento de una llamada
RECONOCIMIENTO DE INICIO	local	ambos	Indica que se ha iniciado el establecimiento de la llamada pero pide más información
Mensajes de la fase de información de llamada			
REANUDA llamada pendiente	local	u → n	Pide la reanudación de una llamada previamente suspendida
REANUDA RECONOCIMIENTO	local	n → u	Indica que la llamada pedida se ha restablecido
RECHAZA RECONOCIMIENTO	local	n → u	Indica fallo al reanudar la llamada suspendida
SUSPENDIDO	local	u → n	Pide la suspensión de una llamada
RECONOCIMIENTO SUSPENDIDO	local	n → u	La llamada ha sido suspendida
RECHAZO SUSPENDIDO	local	n → u	Indica fallo en la suspensión de la llamada solicitada
Mensajes de cierre de llamada			
DESCONECTAR	global	ambos	Enviado por el usuario para pedir el fin de una conexión; enviado por la red para indicar fin de conexión
LIBERAR referencia de llamada	local	ambos	Indica la intención de liberar el canal y la referencia de la llamada
LIBERACIÓN COMPLETA	local	ambos	Indica la liberación del canal y la referencia de llamada
INFORMACIÓN	local	ambos	Proporciona información adicional
NOTIFICACIÓN	acceso	ambos	Indica información perteneciente a una llamada
ESTADO	local	ambos	Enviada en respuesta a una PETICIÓN DE ESTADO o en cualquier momento para informar de un error
PETICIÓN DE ESTADO	local	ambos	Solicita un mensaje de ESTADO

llamada. La naturaleza de esta información está más allá del alcance de la normalización, pero se supone que la información de señalización de control la que no puede o no debe ser enviada directamente a través del circuito usuario-canal. El resto de los mensajes permite a los usuarios pedir la suspensión y posterior reanudación de la llamada. Cuando una llamada se suspende, la red recuerda la identidad de las partes llamadas y las instalaciones de la red que soportan la llamada, pero desactiva la llamada para que no se contraigan costes adicionales y para que el canal de usuario correspondiente se libere. Presumiblemente, la reanudación de la llamada es más rápida y barata que el inicio de una nueva llamada.

Los mensajes de **terminación de llamada** se envían entre el usuario y la red para finalizar una llamada. Finalmente, hay mensajes **varios** que pueden enviarse entre el usuario y la red en varios estados de la llamada. Algunos se pueden enviar durante el establecimiento de la llamada; otros pueden enviarse incluso si no existen llamadas. La función primaria de estos mensajes es negociar las características de la red (servicios suplementarios).

PROTOCOLO DE LA CAPA DE ENLACE: LAPD

Todo el tráfico sobre el canal D utiliza un protocolo de capa de enlace conocido como LAPD («Link Acces Protocol-D channel», protocolo del nivel de acceso al canal D).

Servicios LAPD

La normalización LAPD proporciona dos formas de servicios a los usuarios LAPD: el servicio de transferencia de información sin reconocimiento y el servicio de transferencia de información con reconocimiento. El servicio de **transferencia de información sin reconocimiento** sencillamente se proporciona para la transferencia de tramas que contienen datos del usuario sin reconocimiento. El servicio no garantiza que los datos presentados por un usuario vayan a llegar a otro usuario, ni tampoco informa al que envía si el intento de envío falla. El servicio no proporciona ningún flujo de control o mecanismo de control de errores. Este servicio admite tanto la modalidad punto a punto (entrega a un usuario) como la multipunto (entrega a varios usuarios). El servicio permite la transferencia de datos rápida y es útil para gestión de procedimientos tales como mensajes de alarma y mensajes que no necesitan ser emitidos a varios usuarios.

El servicio de **transferencia de información con reconocimiento** es el más común, y similar al servicio ofrecido por LAP-B y HDLC. Con este servicio, se establece una conexión lógica entre dos usuarios LAPD antes el intercambio de datos.

Protocolo LAPD

El protocolo LAPD se basa en HDLC. Tanto la información de usuario y la información de control de protocolo y los parámetros se transmiten en tramas. Correspondiendo a los dos tipos de servicios ofrecidos por LAPD, hay dos tipos de operaciones:

- **Operación sin reconocimiento:** la información de la Capa 3 se transfiere en tramas no numeradas. La detección de errores se usa para descartar tramas dañadas, pero no hay un control de errores o control de flujo.
- **Operación con reconocimiento:** la información de la Capa 3 se transfiere en tramas que incluyen una secuencia de números que son reconocidos. Los procedimientos de control de errores y control de flujo están incluidos en el protocolo. Este tipo también se menciona en la normalización como operación multitrama.

Estos dos tipos de operaciones pueden coexistir en un único canal D. Ambos tipos de operaciones hacen uso del formato de trama ilustrado en la Figura A.11. Este formato es idéntico al de HDLC (Figura 7.10) con excepción del campo de dirección.

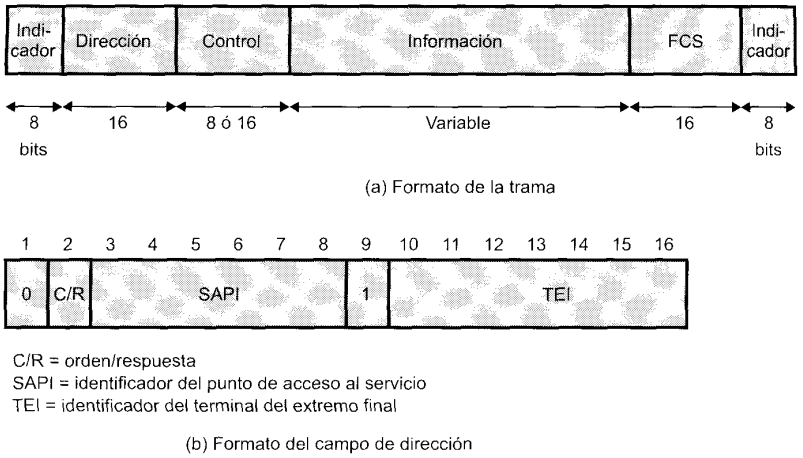


Figura A.11. Formato LAPD.

Para explicar el campo de dirección, necesitamos considerar que LAPD tiene que ocuparse de los dos niveles de multiplexación. Primero, en el sitio del abonado, puede haber varios dispositivos de usuario compartiendo la misma interfaz física. Segundo, en cada dispositivo de usuario, puede haber varios tipos de tráfico: específicamente, datos de paquetes conmutados y señalización de control. Para adaptar estos niveles de multiplexación, LAPD emplea una dirección con dos partes, que consiste en un identificador de punto final de terminal (TEI) y un identificador de punto de acceso al servicio (SAPI).

Normalmente, a cada dispositivo de usuario se le da un único **identificador de punto final de terminal (TEI).** También es posible para un único dispositivo, asignarle más de un TEI. Esto puede darse para un concentrador de terminales. La asignación TEI tiene lugar tanto automáticamente cuando el equipo se conecta por primera vez a la interfaz, como manualmente por el usuario. En el último caso, se debe tener cuidado cuando varios equipos conectados a la misma interfaz no tienen el mismo TEI. La ventaja del procedimiento automático es que permite al usuario cambiar, añadir o eliminar equipos sin notificación anterior a la administración de la red. Sin esta característica, la red estaría obligada a gestionar una base de datos para cada abonado que tendría que ser puesta al día manualmente. La Tabla A.4a muestra la asignación de números TEI.

Tabla A.4. Asignaciones SAPI y TE1.

(a) Asignaciones TE1

Valor del TE1	Tipo de usuario
0-63	Equipo de usuario con asignación de TE1 no automática
64-126	Equipo de usuario con asignación de TE1 automática
127	Usado durante una asignación de TE1 automática

(b) Asignaciones SAPI

Valor del SAPI	Protocolo relacionado o entidad de gestión
0	Procedimientos de control de llamadas
16	Comunicación de paquetes conforme del nivel 3 de X.25
32-61	Comunicación con Retransmisión de Tramas («Frame Relay»)
63	Procedimientos de gestión de la Capa 2
Todas las demás	Reservado para futuras normalizaciones

El **identificador de punto de acceso al servicio (SAPI)** identifica al usuario de la capa 3 de LAPD, y por tanto corresponde a una entidad de protocolo de la capa 3 en un dispositivo de usuario. Se han asignado cuatro valores específicos, como se muestra en la Tabla A.4b. Un SAPI de 0 se usa para procedimientos de control de llamadas para gestión de circuitos de canal B; el valor 16 está reservado para comunicación modo paquete en el canal D usando nivel 3 de X.25; y el valor 63 se usa para el intercambio de información de gestión de la capa 2. Finalmente, los valores comprendidos entre 32 y 61 están reservados para conexiones de retransmisión de tramas.

Para la operación con reconocimiento, LAPD sigue esencialmente los mismos procedimientos descritos para HDLC en el Capítulo 7. Para operaciones sin reconocimiento, la trama de información de usuario (UI) se usa para transmitir datos del usuario. Cuando un usuario LAPD desea enviar datos, pasa los datos a su entidad LAPD, que pasa los datos al campo de información de una trama UI. Cuando esta trama es recibida, el campo de información se pasa al usuario destinatario. No se devuelve reconocimiento a la otra parte. Sin embargo, se realiza la detección de errores y se descartan tramas erróneas.

Capa física

La capa física de RDSI se presenta al usuario bien en el punto de referencia S o en el T (Figura A.4). La interfaz mecánica se describió en el Capítulo 6.

La especificación eléctrica depende de la interfaz específica. Para la interfaz de acceso básico, se usa un código pseudoternario (Figura 5.2). Recordemos que con pseudoternario, la señal de línea puede tomar uno de tres niveles. Éste no es tan eficiente como un código de dos niveles, pero es razonablemente sencillo y barato. Es un código adecuado para la relativamente modesta velocidad de los datos de la interfaz de acceso básico.

Para la interfaz de acceso primario de alta velocidad, se necesita un esquema de codificación más eficiente. Para una velocidad de 1,544 Mbps, se usa un código B8ZS, mientras que para una velocidad de 2,048 Mbps, se usa un código HDB3 (Figura 5.6). No hay ventajas particulares de uno sobre otro; la especificación refleja un uso histórico.

La especificación funcional de la capa física incluye las siguientes funciones:

- Transmisión full-duplex de datos del canal B
- Transmisión full-duplex de datos del canal D
- Transmisión full-duplex de señales de temporización
- Activación y desactivación de circuitos físicos
- Alimentación de potencia de la terminación de red al terminal
- Identificación de terminal
- Aislamiento de terminales defectuosos
- Acceso al canal D de contención

La función final se requiere cuando varios terminales TE1 comparten una única interfaz física (por ejemplo, una línea multipunto). En este caso, no se necesita funcionalidad adicional para el control de acceso a los canales B, ya que cada canal se dedica a un circuito particular en un momento dado. Sin embargo, el canal D está disponible para uso de todos los dispositivos, tanto para señalización de control como para transmisión de paquetes. Para datos de llegada, el esquema de direccionamiento LAPD es suficiente para elegir el destino adecuado de cada unidad de datos. Para datos de salida, se necesitan algunos tipos de protocolos de resolución de contención para asegurar que sólo un dispositivo a la vez intenta transmitir. Los algoritmos de resolución de contención del canal D se describieron en el Capítulo 8.

A.5. RDSI DE BANDA ANCHA

En 1988, como parte de las series I de recomendaciones de RDSI, CCITT publicó la primera de dos recomendaciones relacionadas con RDSI de banda ancha (RDSI-BA): I.113, «vocabulario de términos relacionados con la RDSI de banda ancha», e I.121, «aspectos de la RDSI de banda ancha». Estos documentos proporcionan una descripción preliminar y una base para un futuro trabajo de desarrollo y normalización, y a partir de estos documentos se ha desarrollado un rico conjunto de recomendaciones. En la Tabla A.5 se presentan algunas de las importantes nociones desarrolladas en estos documentos.

La ITU-T define modestamente RDSI-BA como «un servicio que requiere canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria». Detrás de esta frase inocua yace un plan para una red y un conjunto de servicios que tendrán mucho más impacto en empresas y en clientes particulares que la RDSI. Con RDSI-BA estarán disponibles, servicios, especialmente servicios de vídeo, que requieren velocidades de un orden de magnitud más allá de las que ofrece RDSI. Para contrastar esta nueva red y estos nuevos servicios con el concepto original de RDSI, este concepto original se denomina ahora RDSI de banda estrecha.

ARQUITECTURA DE LA RDSI DE BANDA ANCHA

RDSI-BA difiere de RDSI de banda estrecha de diferentes modos. Para reunir los requisitos para vídeo de alta resolución, se necesita una velocidad de canal superior, más o menos de 150 Mbps. Para admitir simultáneamente uno o más servicios interactivos y distribuidos, se necesita una velocidad de línea de abonado total de alrededor de 600 Mbps. En términos del parque de teléfonos instalado hoy día, es una excelente velocidad a apoyar. La única tecnología apropiada para sustento general de estas velocidades de datos, es la fibra óptica. Por tanto, la introducción de RDSI-BA depende del ritmo de introducción del bucle de abonado de fibra.

Interno a la red, está el tema de la técnica de conmutación que se va a usar. El dispositivo de conmutación tiene que ser capaz de manejar un amplio rango de velocidades diferentes y de parámetros de tráfico (por ejemplo, transmisión en ráfagas). A pesar de la creciente potencia del hardware de circuitos digitales de conmutación y del creciente uso de líneas de fibra óptica, es difícil gestionar la gran cantidad y variedad de requisitos de RDSI-BA con tecnología de conmutación de circuitos. Por esta razón, hay un interés creciente en algunos tipos de paquetes de conmutación rápidos como la técnica de conmutación básica para RDSI-BA. Esta forma de conmutación admite fácilmente un ATM en la interfaz usuario-red.

Tabla A.5. Declaraciones notables de I.113 e I.121.

Banda ancha: servicio o sistema que requiere canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria.
El término RDSI-BA se usa por conveniencia, para referirse y enfatizar los aspectos de banda ancha de la RDSI. La intención es, sin embargo, ofrecer una noción comprensible de una RDSI que proporciona banda ancha y otros servicios RDSI.
El modo de transferencia asíncrona (ATM) es el modo de transferencia que implementa RDSI-BA y es independiente del significado del transporte en la capa física.
RDSI-BA estará basada en los conceptos desarrollados para la RDSI y puede evolucionar incorporando progresiva y directamente a la red funciones RDSI-BA adicionales que habiliten servicios nuevos y avanzados.
Puesto que la RDSI-BA se basa generalmente en conceptos RDSI, la configuración de referencia de acceso a RDSI es también la base de la configuración de referencia de la RDSI-BA.

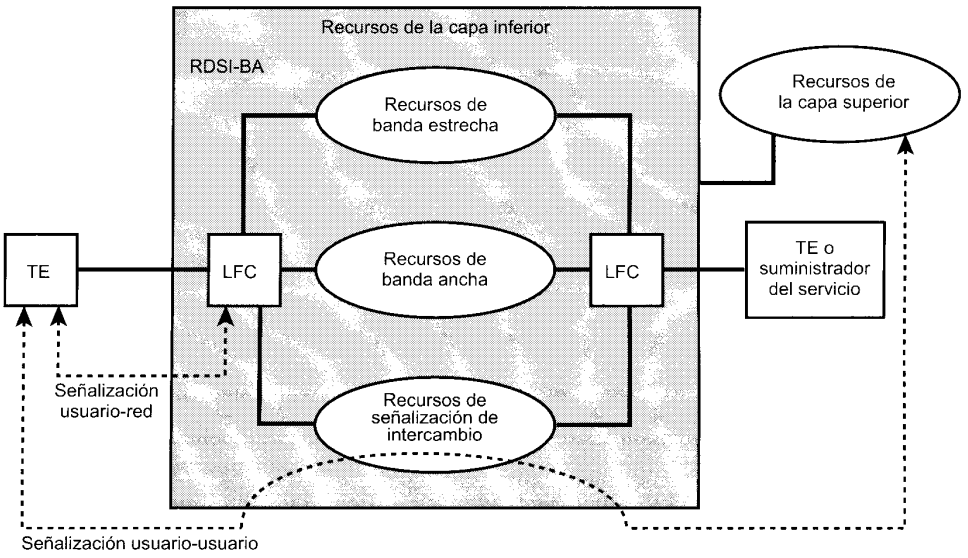


Figura A.12. Arquitectura RDSI-BA.

Arquitectura funcional

La Figura A.12 muestra la arquitectura funcional de RDSI-BA. Como con RDSI de banda estrecha, el control de RDSI-BA se basa en señalización de canal común. En la red, se usa un SS7, mejorado para soportar capacidades suplementarias de red de mayor velocidad. Igualmente, el protocolo de señalización de control usuario-red es una versión mejorada de I.451/Q.931.

RDSI-BA debe, por supuesto, soportar todos los servicios de transmisión a 64 kbps, tanto de conmutación de circuitos como de conmutación de paquetes, que son admitidos por RDSI de banda estrecha. Esto protege la inversión del usuario y facilita la emigración de RDSI de banda estrecha a banda ancha. Además, las capacidades de banda ancha se proporcionan para servicios de transmisión a mayores velocidades. En la interfaz usuario-red, estas capacidades se proporcionarán con el modo de transferencia asíncrono orientado a conexión (ATM).

Interfaz usuario-red

La configuración de referencia definida para RDSI de banda estrecha se considera lo bastante general como para ser usada en RDSI-BA. La Figura A.13, casi idéntica a la Figura A.4, muestra la configuración de referencia para RDSI-BA. Para ilustrar más claramente los aspectos de banda ancha, las notaciones para los puntos de referencia y las agrupaciones funcionales, se indican con la letra B (por ej.: B-NT1, T_B). Los grupos funcionales de banda ancha son equivalentes a los grupos funcionales definidos para RDSI de banda estrecha que se discuten más adelante. Las interfaces en el punto de referencia R pueden o no tener capacidades de banda ancha.

Estructura de la transmisión

En términos de velocidades disponibles para los abonados RDSI-BA, se definen tres servicios de transmisión nuevos. El primero de ellos consiste en un servicio full-duplex a 155,52 Mbps. El segundo servi-

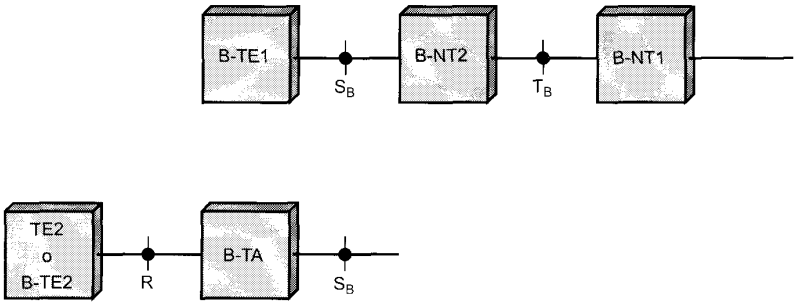


Figura A.13. Puntos de referencia RDSI-BA y grupos funcionales.

cio definido es asimétrico, proporciona transmisión desde el abonado a la red a 155,52 Mbps y en la otra dirección a 622,08 Mbps. Y el servicio de mayor capacidad ya definido es el servicio full-duplex a 622,08 Mbps.

La velocidad de 155,52 Mbps puede admitir ciertamente todos los servicios de RDSI de banda estrecha. Es decir, admite fácilmente la mayoría de los servicios RDSI-BA. A esta velocidad, se pueden admitir uno o varios canales de vídeo dependiendo de la resolución del vídeo y de la técnica de codificación usada. Entonces, el servicio full-duplex a 155,52 Mbps será probablemente el servicio RDSI-BA más común.

Se necesitan velocidades mayores de 622,08 Mbps para gestionar la distribución de vídeo múltiple, como la que se puede requerir cuando un organismo lleva a cabo videoconferencias simultáneas múltiples. Esta velocidad tiene sentido en la dirección red a abonado. El abonado típico no iniciará los servicios de distribución y entonces podrá usar todavía el servicio menor, 155,52 Mbps. El servicio full-duplex a 622,0 Mbps sería apropiado para un suministrador de distribución de vídeo.

PROTOCOLOS DE LA RDSI DE BANDA ANCHA

La arquitectura del protocolo para RDSI-BA introduce algunos elementos nuevos que no se encontraban en la arquitectura RDSI, como se vio en la Figura 11.1. Para RDSI-BA se supone que la transferencia de información a través de la interfaz usuario-red usará ATM.

La decisión de usar ATM para RDSI-BA es destacable. Esto implica que RDSI-BA será una red basada en paquetes, ciertamente en la interfaz y casi ciertamente en términos de su conmutación interna. Aunque la recomendación también afirma que RDSI-BA admitirá aplicaciones modo circuito, esto se hará sobre un mecanismo de transporte basado en paquetes. Por tanto, la RDSI que empezó como una evolución de la red de teléfono de conmutación de circuitos, se transformará en una red de conmutación de paquetes ya que contiene servicios de banda ancha.

El modelo de referencia de protocolo hace referencia a tres planos separados:

- **Plano del usuario:** proporciona al usuario transferencia de información, junto con el control asociado (por ej.: control de flujo, control de errores).
- **Plano de control:** realiza control de llamadas y funciones de control de conexión.
- **Plano de gestión:** incluye un plano de gestión, que realiza funciones de gestión relacionadas con el sistema como un todo y proporciona coordinación entre todos los planos, y la capa de gestión, que realiza funciones de gestión relacionadas con recursos y parámetros que residen en sus entidades de protocolo.

La Tabla A.6 destaca las funciones que realiza cada subcapa.

Tabla A.6. Funciones de las capas RDSI-BA.

	Funciones de capas superiores	Capas superiores	
Gestión de capa	Convergencia	CS	AAL
	Segmentación y resamblado	SAR	
	Control genérico de flujo Generación/extracción de la celda de cabecera Traslación de celda VPI/VCI Multiplexación y demultiplexación de celdas	ATM	
	Velocidad de desacoplo de celdas Generación/verificación de secuencias de cabecera HEC Delineación de celdas Adaptación de tramas de transmisión Generación/recuperación de tramas de transmisión	TC	Capa física
	Temporización de bit Medio físico	PM	

CS = Subcapa de convergencia
SAR = Subcapa de segmentación y resamblado
AAL = Capa de adaptación ATM
ATM = Modo de transferencia asíncrono
TC = Subcapa de control de transmisión
PM = Subcapa del medio físico

A.6. LECTURAS RECOMENDADAS

Se puede encontrar un tratamiento técnico detallado de RDSI y RDSI de banda ancha en [STAL99]. Otros tratamientos excelentes con amplitud de libro son [KESS99] y [BLAC97].

BLAC97 Black, U. *ISDN and SS7: Architectures for Digital Signaling Networks.* Upper Saddle River, NJ: Prentice Hall, 1997.

KESS99 Kessler, G., y Southwick, P. *ISDN: Concepts, Facilities, and Services.* New York: McGraw-Hill, 1999.

STAL99 Stallings, W. *ISDN and Broadband ISDN, with Frame Relay and ATM.* Upper Saddle River, NJ: Prentice Hall, 1990.

A.7. PROBLEMAS

A.1. Se ha mencionado que las líneas multiconexión implementadas de usuario y los multiplexores pueden desaparecer. Explique por qué.

A.2. Un cliente RDSI tiene delegaciones en varios lugares. A una delegación típica se le ofrecen dos cauces digitales de 1,544 Mbps. Uno proporciona acceso de circuito conmutado a RDSI; el otro es una línea alquilada de conexión a otro lugar. El equipo de premisas consiste en un PBX enlazado con un nodo lógico de conmutación de paquetes. El usuario tiene tres requisitos:

- Servicio de teléfono
- Una red privada de paquetes conmutados para datos
- Vídeo teleconferencia a 1,544 Mbps

¿Cómo puede el usuario distribuir óptimamente la capacidad para satisfacer estos requisitos?

A.3. Una trama de acceso básico RDSI tiene 32 bits B y 4 bits D. Supongamos que se han usado más bits, digamos 160 bits B y 20 bits D por trama. ¿Reduciría esto el porcentaje de costes fijos y por consiguiente la velocidad de acceso básico? En caso afirmativo discutir las desventajas potenciales.

A.4. ¿Bajo qué circunstancias la capa 3 de usuario del canal B no sería nula?

A.5. Comparar los esquemas de direccionamiento en HDLC, LLC y LAPD:

a) ¿Son lo mismo SAPI de LAP-D y SAP de LLC?

b) ¿Son lo mismo TEI de LAP-D y la dirección del nivel MAC de IEEE 802?

c) ¿Por qué se necesitan dos niveles de direccionamiento en LAP-D y LLC, y sólo un nivel en HDLC?

d) ¿Por qué LLC necesita una dirección fuente, pero LAP-D y HDLC no?

A.6. ¿Cuál es el porcentaje de costes fijos de la estructura del canal básico?

A.7. En la Figura A.5, ¿podría parecer que las capas de la 4 a la 7 del modelo OSI están poco afectadas por RDSI? ¿Es éste un resultado esperado? ¿Por qué sí o por qué no?

A.8. El X.25 y la mayoría de los protocolos de la capa 3 proporcionan técnicas para control de flujo y control de errores. ¿Por qué no se proporcionan estas características en I.451?

APÉNDICE B

RFCS citados en este libro

RFC Número	Título	Fecha
768	Protocolo de datagrama de usuario (UDP).	Agosto 1980
791	Protocolo Internet (IP).	Septiembre 1981
792	Protocolo de mensajes de control Internet (ICMP).	Septiembre 1981
793	Protocolo de control de transmisión (TCP).	Septiembre 1981
821	Protocolo de transferencia de correo sencillo (SMTP).	Agosto 1982
822	Normalización para el formato de mensajes de texto Internet ARPA.	Agosto 1982
1112	Ampliaciones de computadores (hosts) para multidifusión.	Agosto 1989
1122	Requisitos de los computadores de Internet-Capas de comunicación.	Octubre 1989
1633	Servicios integrados en la arquitectura de Internet: visión general.	Junio 1994
1636	Seguridad en la arquitectura de Internet.	Junio 1994
1752	Recomendación para el protocolo IP de próxima generación.	Enero 1995
1771	Protocolo 4 de pasarela frontera (BGP-4).	Marzo 1995
1812	Requisitos para los encaminadores de la versión IP.	Junio 1995
1901	Introducción a SNMPv2 basado en comunidad.	Enero 1996
1902	Estructura de la información de gestión en SNMPv2.	Enero 1996
1903	Reglas textuales para SNMPv2.	Enero 1996
1904	Declaraciones de conformación para SNMPv2.	Enero 1996
1905	Operaciones de protocolo para SNMPv2.	Enero 1996
1906	Mapas de transporte para SNMPv2.	Enero 1996
1907	Base de información de gestión para SNMPv2.	Enero 1996
1908	Coexistencia entra la versión 1 y la versión 2 de la normalización de Internet.	Enero 1996
2001	Inicio lento de TCP, prevención de la congestión, retransmisión rápida y algoritmos de recuperación rápida.	Enero 1997
2026	Proceso de normalización de Internet-Revisión 3.	Octubre 1996
2045	Ampliaciones de correo en Internet multipropósito (MIME) Parte uno: formato del cuerpo de mensaje en Internet.	Noviembre 1996
2046	Ampliaciones de correo en Internet multipropósito (MIME) Parte dos: tipos de medios.	Noviembre 1996
2047	MIME (Ampliaciones de correo en Internet multipropósito) Parte tres: ampliaciones de la cabecera del mensaje para texto no ASCII.	Noviembre 1996
2048	Ampliaciones de correo en Internet multipropósito (MIME) Parte cuatro: procedimientos de registro.	Noviembre 1996

RFC Número	Título	Fecha
2049	Ampliaciones de correo en Internet multipropósito (MIME) Parte cinco: criterios de conformidad y ejemplos.	Noviembre 1996
2068	Protocolo de transferencia de hipertexto-HTTP/1.1	Enero 1997
2205	Protocolo de reserva de fuente (RSVP)- Versión 1 Especificación funcional.	Septiembre 1997
2328	Primer camino más corto abierto (OSPF) Versión 2.	Abril 1998
2373	Arquitectura de direccionamiento IP, versión 6.	Julio 1998
2401	Arquitectura de seguridad para el protocolo de Internet.	Noviembre 1998
2402	Cabecera de autentificación IP.	Noviembre 1998
2406	Sobrecarga de la seguridad de encapsulación IP (ESP).	Noviembre 1998
2408	Asociación de seguridad en Internet y protocolo de gestión de claves.	Noviembre 1998
2460	Protocolo de Internet, especificación de la versión 6.	Diciembre 1998
2474	Definición del campo de servicios diferenciados en las cabeceras Ipv4 e Ipv6.	Diciembre 1998
2475	Una arquitectura para servicios diferenciados.	Diciembre 1998
2570	Introducción a la versión 3 de la normalización en Internet de tramas de gestión de red.	Abril 1999
2571	Arquitectura para describir tramas de gestión de SNMP.	Abril 1999
2572	Procesamiento y gestión de mensajes SNMP.	Abril 1999
2573	Aplicaciones SNMP.	Abril 1999
2574	Modelo de seguridad basado en usuario para SNMPv3.	Abril 1999
2575	Modelo de control de acceso «view-based» (VACM) para SNMP.	Abril 1999

APÉNDICE C

Proyectos para enseñanza de comunicaciones de datos y computadores

Muchos profesores creen que los proyectos de investigación o de implementación son cruciales para entender con claridad los conceptos de comunicaciones y redes de computadores. Sin proyectos, puede ser difícil que los estudiantes capten algunos conceptos básicos y las interacciones entre componentes. Los proyectos refuerzan los conceptos introducidos en el libro, dan al estudiante una mejor apreciación de cómo funcionan los protocolos y los esquemas de transmisión, y pueden motivarle y darle confianza para que entiendan adecuadamente el texto.

En este texto, he tratado de presentar los conceptos tan claro como me ha sido posible y he propuesto alrededor de 250 problemas para reforzar dichos conceptos. Muchos profesores desearían complementar este material con proyectos. Este apéndice proporciona una guía en esta línea y describe el material de ayuda disponible en el manual del profesor. El material de ayuda abarca cuatro tipos de proyectos:

- Proyectos de simulación
- Proyectos de modelos de prestaciones
- Proyectos de investigación
- Asignación de lecturas/trabajos

C.1. PROYECTOS DE SIMULACIÓN

Una forma excelente de obtener una adecuada comprensión de los protocolos de comunicación y su funcionamiento y de las configuraciones de red, y de estudiar y apreciar algunos de las condiciones de diseño e implicaciones de las prestaciones, es simulando los elementos clave. Una herramienta útil para este propósito es *cnet*.

Comparado con las implementaciones hardware/software reales, la simulación proporciona varias ventajas tanto en investigación como en educación:

- Con la simulación, es fácil modificar varios elementos de una configuración de red, o varias características de un protocolo, variar las características de funcionamiento de varios componentes y, por tanto, analizar los efectos de tales modificaciones.
- La simulación ofrece conjuntos estadísticos de prestaciones, que se pueden usar para entender los requisitos de prestaciones.

El simulador de redes *cnet* [MCDO91] permite experimentar con varias capas de enlace de datos, capas de red, protocolos de las capas de encaminamiento y transporte, y con varias configuraciones de red. Se ha diseñado específicamente para cursos de redes de computadores dirigidos a estudiantes universitarios no graduados, y ha sido utilizado en todo el mundo por cientos de estudiantes desde 1991.

El simulador *cnet* fue desarrollado por el profesor Chris McDonald de la Universidad de Western Australia. El profesor McDonald ha desarrollado un manual del estudiante y un conjunto de proyectos específico para usar en comunicaciones y redes de computadores y está disponible para los profesores que lo soliciten.

El simulador *cnet* se puede ejecutar en distintas plataformas UNIX y se ha adaptado recientemente a una plataforma con Win-32. Está en desarrollo una versión para Macintosh. El software se puede copiar desde un sitio Web. Está disponible gratis para uso no comercial.

C.2. MODELADO DE PRESTACIONES

Una alternativa a la simulación para evaluar las prestaciones de un sistema de comunicaciones o protocolo de red es un modelado analógico. En este contexto, un modelado analógico se refiere a herramientas para hacer análisis de cola, así como herramientas para hacer sencillos tests estadísticos del tráfico de la red y herramientas para generar series temporales para analizar.

El profesor Kenneth Christensen de la Universidad del sur de Florida ha desarrollado un conjunto de herramientas potentes y fáciles de usar. Su página de *herramientas* contiene programas principalmente relacionadas con la evaluación de prestaciones de redes de computadores y con la programación de conectores TCP/IP. Cada herramienta está escrita en ANSI C. El formato de cada herramienta es el mismo, en la cabecera del programa se describe la finalidad de la herramienta, las notas generales, una muestra de entrada, una muestra de salida, instrucciones de construcción, instrucciones de ejecución e información para contactar con el autor. El código está documentado con muchos comentarios y bloques de cabecera en todas las funciones. La finalidad de cada herramienta es que pueda servir como medio de enseñanza del concepto implementado (y como modelo de una buena práctica de programación). Por tanto, lo destacable es su sencillez y claridad. Se supone que el estudiante tiene acceso a un compilador de C y que dispone, al menos, de una experiencia moderada en programación en C.

El profesor Christensen ha desarrollado un manual del estudiante y un conjunto de proyectos específicos para comunicaciones y redes de computadores, que está disponible para los profesores que lo soliciten. El software se puede copiar desde su página Web de *herramientas*. Está disponible gratis para uso no comercial.

C.3. PROYECTOS DE INVESTIGACIÓN

Una forma efectiva de reforzar los conceptos básicos del curso, y de enseñar a los estudiantes experiencias en investigación es asignarles proyectos. Uno de este tipo podría implicar una búsqueda bibliográfi-

ca así como la localización en la Web de productos, actividades de laboratorios de investigación, y normalizaciones. Los proyectos se podrían asignara a equipos o, si los proyectos son pequeños, a individuos. En cualquier caso, es mejor solicitar al propio alumno algún tipo de propuesta de proyecto pronto, para dar al profesor tiempo para evaluar la propuesta con objeto de que tenga contenidos y nivel adecuados. Los proyectos de investigación a proponer a los alumnos deben incluir:

- Formato para la propuesta
- Formato para el informe final
- Esquema con fechas de entrega intermedias y finales
- Lista de posibles temas de proyectos

Los estudiantes podrán seleccionar uno de los temas de la lista o idear su propio proyecto. El manual del profesor incluye una sugerencia de formato para el informe propuesto y final más una lista de posibles temas de investigación.

C.4. ASIGNACIÓN DE LECTURAS/INFORMES

Otra forma excelente de reforzar conceptos del curso y dar a los estudiantes experiencia en investigación es asignarles artículos para leerlos y analizarlos. El manual del profesor incluye una lista de artículos sugeridos. Todos los artículos están disponibles tanto en Internet como en las bibliotecas de los centros docentes buenos. El manual también incluye sugerencias para la asignación de estos trabajos.

Glosario

Algunas de las definiciones en este glosario proceden del *National Standard Dictionary of Information Technology* (*Diccionario estándar nacional de tecnología de la información*), normalización ANSI X3.172, 1995. Estas definiciones están marcadas con un asterisco.

Acceso múltiple por demanda/asignación Técnica para asignar capacidad adicional, basada en FDM o en TDM, en la que la capacidad se concede según demanda.

Aloha Una técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación transmite siempre que tiene datos para enviar. Se repiten las transmisiones que no son reconocidas.

Amplitud El tamaño o magnitud de una onda de tensión o de corriente.

Ancho de banda Diferencia entre las frecuencias límite de un espectro de frecuencia continuo.

Anillo Topología de red local en la que las estaciones están conectadas a repetidores conectados en un lazo cerrado. Los datos se transmiten en una dirección alrededor del anillo, y pueden ser leídos por todas las estaciones conectadas a la red.

Arquitectura de comunicaciones Las estructuras hardware y software que implementan las funciones de comunicación.

Atenuación Disminución en magnitud de la corriente, tensión o potencia de una señal durante su transmisión entre puntos.

Autentificación Proceso usado para verificar la integridad de los datos transmitidos, especialmente mensajes.

Banda ancha Uso de cable coaxial para proporcionar una transferencia de datos mediante señales analógicas (de radio frecuencia). Las señales digitales se adaptan en un modem y se transmiten en una de las bandas de frecuencia del cable.

Banda base Transmisión de señales sin modulación. En una red local de banda base, las señales digitales (unos y ceros) se insertan directamente en el cable como pulsos de tensión. Todo el espectro del cable es ocupado por la señal. Este esquema no permite multiplexación por división de frecuencia.

Baudio Unidad de velocidad de la señal, dada por el número de valores discretos o eventos de una señal por segundo, o la inversa del tiempo de duración del elemento de señal más corto.

Bit de paridad* Un bit de comprobación añadido a un conjunto de dígitos binarios para hacer al conjunto de todos los dígitos binarios de valor uno, incluyendo el bit de comprobación, siempre par o impar.

Bits de relleno La inserción de bits extra en una cadena de datos para evitar la aparición de secuencias de control no deseadas.

Bucle local Camino de transmisión, generalmente par trenzado, entre el abonado individual y el centro de conmutación más cercano de la red pública de telecomunicaciones.

Bus* Uno o más conductores que sirven como conexión común para un grupo de dispositivos relacionados.

Cabecera Información de control de un sistema definido que precede a los datos del usuario.

Cable coaxial Cable que contiene un conductor, usualmente un tubo o hilo de cobre, en su interior aislado por otro conductor de mayor diámetro, usualmente un tubo de cobre o cobre trenzado.

Capa* Grupo de servicios, funciones, y protocolos que se definen totalmente desde un punto de vista conceptual, que constituye uno de entre conjunto de grupos dispuestos jerárquicamente, y que se extiende a través de todos los sistemas que conforman la arquitectura de la red.

Capa de adaptación ATM (AAL, ATM Adaptation Layer) Capa que transforma los protocolos de transferencia de información en ATM.

Capa de aplicación Capa 7 del modelo OSI. Esta capa determina la interfaz del sistema con el usuario.

Capa de enlace de datos* En OSI, la capa que proporciona el servicio de transferencia de datos entre entidades de la capa de red, usualmente en nodos adyacentes. La capa de enlace de datos detecta y posibilita la corrección de errores que puedan ocurrir en la capa físico.

Capa de presentación* Capa 6 del modelo OSI. Proporciona la selección de una sintaxis común para representar datos y para transformar datos de aplicación en y desde una sintaxis común.

Capa de red Capa 3 del modelo OSI. Responsable del enrutamiento de los datos a través de la red de comunicación.

Capa de sesión Capa 5 del modelo OSI. Gestiona una conexión lógica (sesión) entre dos procesos o aplicaciones que se comunican.

Capa de transporte Capa 4 del modelo OSI. Proporciona una transferencia de datos fiable y transparente entre puntos extremos.

Capa física Capa 1 del modelo OSI. Relacionado con aspectos eléctricos, mecánicos y de temporización de la transmisión de una señal en un medio.

CATV (Community Antenna Television) Antena de televisión comunitaria. El cable CATV se usa para redes locales de banda ancha, y para distribución de emisiones de TV.

Cifrado Convertir textos puros o datos en una forma ininteligible mediante el uso de un código de forma que posteriormente se pueda hacer la reconversión a la forma original.

Cifrado asimétrico Un método de cifrado en el que el cifrado y descifrado se realizan usando dos claves diferentes, una de ellas llamada clave pública y la otra clave privada. También se conoce como cifrado de clave pública.

Cifrado convencional Cifrado simétrico.

Cifrado de clave pública Cifrado asimétrico.

Cifrado simétrico Un tipo de sistema criptográfico en el que el cifrado y descifrado se realizan usando la misma clave. También se conoce como cifrado convencional.

Circuito virtual Servicio de conmutación de paquetes en el que se establece una conexión (circuito virtual) entre dos estaciones al comienzo de la transmisión. Todos los paquetes siguen la misma ruta, no necesitan llevar una dirección completa y llegan secuencialmente.

Clave privada Una de las dos claves usadas en un sistema de cifrado asimétrico. Para una comunicación segura, el creador de la clave privada debe ser el único que la conozca.

Clave pública Una de las dos claves usadas en un sistema de cifrado asimétrico. La clave pública se hace pública, para ser usada junto con su correspondiente clave privada.

Codec (codificador-decodificador) Transforma datos analógicos en un flujo digital de bits (codificador), y señales digitales en datos analógicos (decodificador).

Codificación diferencial Un tipo de codificación de datos digitales en una señal digital tal que el valor binario se determina por un cambio de la señal en lugar de por el nivel de la señal.

Codificación Manchester Técnica de señalización digital en la que hay una transición en medio de cada intervalo de duración de un bit. Se codifica un 1 con nivel alto durante la primera mitad del bit; se codifica un 0 con nivel bajo durante la primera mitad del bit.

Código de detección de errores* Código en el que cada secuencia se ajusta a reglas de construcción específicas, para que si ocurren ciertos errores en ella, la secuencia resultante no se ajuste a las reglas de construcción y por tanto se pueda detectar la presencia de errores.

Colisión Situación en la que dos paquetes transmiten a través de un medio al mismo tiempo. Su interferencia hace a ambos ininteligibles.

Competición Situación que se produce cuando dos o más estaciones intentan usar el mismo canal al mismo tiempo.

Comprobación de suma (checksum) Código de detección de errores basado en la suma de los bits que se van a comprobar.

Conmutación de circuitos Método de comunicación en el que se establece un camino de comunicación entre dos dispositivos a través de uno o más nodos de conmutación intermedios.

Conmutación de paquetes Método de transmisión de mensajes a través de una red de comunicación, en la que los mensajes largos se subdividen en pequeños paquetes. Los paquetes se transmiten después como en conmutación de mensajes.

Conmutación por división del espacio Técnica de conmutación de circuitos en la que cada conexión a través del conmutador toma un camino físicamente separado y exclusivo.

Conmutación por división del tiempo Técnica de conmutación de circuitos en la que los intervalos de tiempo asignados a un flujo de datos multiplexado se corresponden con el paso de los mismos de la entrada a la salida.

Conmutador digital Una red local con topología de estrella. Usualmente se refiere a un sistema que maneja sólo datos, no voz.

Contador de saltos (hop count) El número de saltos a lo largo de un camino desde una fuente dada a un destino dado, y es igual al número de nodos de la red (nodos de conmutación de paquetes, conmutadores ATM, enrutadores, etc.) que un paquete se encuentra a lo largo de dicho camino.

Control de acceso al medio (MAC, Medium Access Control) Para redes de difusión, método de determinación del dispositivo que tiene acceso al medio de transmisión en cada momento. Son métodos de acceso al medio CSMA/CD y paso de testigo.

Control de flujo Función realizada por una entidad receptora para limitar la cantidad o velocidad de los datos que una entidad transmisora envía.

CSMA (Carrier Sense Multiple Access, acceso múltiple por detección de portadora) Técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación que desee transmitir, primero detecta el medio y sólo transmite si el medio está desocupado.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Acceso múltiple sensible a portadora con detección de colisiones) Un refinamiento de CSMA en el que una estación cesa la transmisión si detecta una colisión.

Datagrama* En conmutación de paquetes, un paquete, independiente de los otros paquetes, que lleva información suficiente para enrutar desde el equipo terminal de datos (DTE) de origen hasta el DTE de destino sin la necesidad de establecer una conexión entre los DTE y la red.

Datos analógicos* Datos representados por una magnitud física que varía continuamente, y cuya magnitud es directamente proporcional al dato o a la función que se ajusta a los datos.

Datos digitales* Datos que consisten en una secuencia de valores discretos.

Decibelio Medida de la intensidad relativa de dos señales. El número de decibelios es 10 veces el logaritmo del cociente de la potencia de dos señales, o 20 veces el logaritmo del cociente de tensión de dos señales.

Densidad espectral de potencia (PSD, Power Spectral Density) La PSD de una señal es una función de la frecuencia que representa la potencia por unidad de ancho de banda de los componentes espectrales para cada frecuencia.

Descifrado La traducción de un texto o datos cifrados (o texto encriptado) al texto o datos originales (o texto puro). También se llama desencriptado.

Diafonía (crosstalk) Fenómeno por el que una señal transmitida en un circuito o canal de un sistema de transmisión crea un efecto indeseado en otro circuito o canal.

Difusión Transmisión simultánea de datos a varias estaciones.

Digitalizar* Convertir una señal analógica en una señal digital.

Dirección de difusión Una dirección que designa todas las entidades en un dominio (por ejemplo: red Internet).

Dirección multidestino Una dirección que designa a un grupo de entidades en un dominio (por ejemplo: red, Internet).

Dispositivo de encaminamiento (router) Dispositivo de red que conecta dos redes de computadores. Usa un protocolo de internet y asume que todos los dispositivos conectados a la red usan la misma arquitectura y protocolos de red. Un dispositivo de encaminamiento opera en la capa 3 de OSI.

Distorsión de retardo Distorsión de una señal que ocurre cuando el retardo de propagación del medio de transmisión no es constante en el rango de frecuencia de la señal.

Encaminamiento o enrutamiento Determinación del camino o ruta que las unidades de datos (tramas, paquetes, mensajes) atravesarán desde la fuente al destino.

Encapsulado Adición de información de control mediante una entidad de protocolo con datos obtenidos de un protocolo de usuario.

Equipo de terminación de red Agrupación de funciones RDSI en la frontera entre RDSI y el abonado.

Equipo terminal de circuito de datos (DCE, Data Circuit-terminating Equipment) En una estación de datos, el equipo que proporciona la conversión de señales y la codificación entre el equipo terminal de datos (DTE, Data Terminal Equipement) y la línea. El DCE puede ser un equipo independiente o una parte integrada en el DTE o en un equipo intermedio. El DCE puede realizar otras funciones que normalmente se realizan en el extremo de la red de la línea.

Equipo terminal de datos (DTE, Data Terminal Equipment)* Equipo consistente en instrumentos finales digitales que convierten la información del usuario en señales de datos para transmisión, o reconvierten las señales de datos recibidas en información de usuario.

Espectro Se refiere a un rango absoluto de frecuencias. Por ejemplo, el espectro del cable CATV, en la actualidad, comprende de 5 a 400 MHz.

Estrella Topología en la que todas las estaciones están conectadas a un conmutador central. Dos estaciones se comunican por medio de conmutación de circuitos.

Fase Posición relativa en el tiempo dentro de un periodo individual de la señal.

Fibra óptica Filamento fino de cristal u otro material transparente a través del que se puede transmitir, mediante reflexión total interna, un haz de luz de una señal codificada.

Firma digital Mecanismo de autentificación que habilita al creador de un mensaje a adjuntar un código que actúa como firma. La firma garantiza la fuente y la integridad del mensaje.

Frecuencia Velocidad de oscilación de la señal en hertzios.

Función de dispersión (Hash) Función que asigna a un bloque de datos de longitud variable o a un mensaje, un valor de longitud fija llamado código de dispersión (hash). La función se diseña de forma que, cuando está protegida, proporciona una autentificación de los datos o de los mensajes.

HDLC (High-level Data Link Control, control de enlace de datos de alto nivel) Protocolo de enlace de datos (capa 2 de OSI) orientado a bits, muy común, usado por ISO. Los protocolos LAPB, LAPD, y LLC son similares.

Incorporación de confirmación (Piggybacking) La inclusión de un reconocimiento de un paquete previamente recibido en un paquete de datos que sale.

Información de control de protocolo* Información intercambiada entre entidades de una capa dada, por medio del servicio proporcionado por la capa inmediata inferior, para coordinar su funcionamiento conjunto.

Interconexión de redes (internetworking) Comunicación entre dispositivos a través de varias redes.

Medio de transmisión Camino físico entre transmisores y receptores en un sistema de comunicación.

Microondas Ondas electromagnéticas en el rango de frecuencias entre 2 y 40 GHz.

Modelo de referencia de interconexión de sistemas abiertos (OSI, Open Systems Interconnection) Modelo de comunicación entre dispositivos que cooperan. Define una arquitectura de siete capas de funciones de comunicación.

Modem (modulador/demodulador) Transforma un flujo de bits digitales en una señal analógica (modulador) y viceversa (demodulador).

Modo de transferencia asíncrono (ATM, Asynchronous Transfer Mode) Un método de transmisión de paquetes usando un tamaño de paquete fijo, llamado celda. ATM es la interfaz de trasferencia de datos para RDSI-BA. A diferencia de X.25, ATM no proporciona mecanismos de control de errores y de control de flujo.

Modulación* Proceso, o resultado del proceso, de variación de algún parámetro de una señal, llamada portadora, de acuerdo con una señal mensaje.

Modulación angular* Modulación en la que se varía el ángulo de una onda portadora senoidal. La modulación en fase y en frecuencia son formas particulares de modulación angular.

Modulación de fase Modulación en la que el ángulo de fase de una portadora es el parámetro que se varía.

Modulación en amplitud Una forma de modulación en la que la amplitud de la onda portadora varía de acuerdo con alguna característica de la señal modulante.

Modulación en frecuencia Modulación en la que la frecuencia de una señal sinusoidal alterna es el parámetro que se varía.

Modulación por codificación de pulsos Proceso en el que se muestrea una señal, se cuantiza y se convierte la magnitud de cada muestra según una referencia prefijada, codificándola en una señal digital.

Modulación por desplazamiento de amplitud Modulación en la que los dos valores binarios se representan con dos amplitudes diferentes de la frecuencia de la portadora.

Modulación por desplazamiento de fase Modulación en la que la fase de la señal portadora se desplaza para representar datos digitales.

Modulación por desplazamiento de frecuencia Modulación en la que los dos valores binarios se representan con dos frecuencias diferentes próximas a la frecuencia de la portadora.

Multiplexación En transmisión de datos, una función que permite a dos o más fuentes de datos compartir un medio de transmisión común tal que cada fuente de datos tiene su propio canal.

Multiplexación estadística por división del tiempo Método de TDM en el que los intervalos de tiempo, en una línea de transmisión compartida, se sitúan en canales de E/S bajo demanda.

Multiplexación por división de frecuencia División de un medio de transmisión en dos o más canales fraccionando la banda de frecuencia transmitida, en bandas más estrechas, y usando cada una de ellas como un canal diferente.

Multiplexación por división del tiempo División de un servicio de transmisión en dos o más canales transmitiendo la información de cada uno de ellos en intervalos de tiempo diferentes.

Multiplexación síncrona por división del tiempo Método TDM en el que los intervalos de tiempo de una línea de transmisión compartida son asignados a canales de E/S de forma fija y predeterminada.

Multipunto Configuración en la que más de dos estaciones comparten un camino de transmisión.

Notación de sintaxis abstracta 1 (ASN.1) Un lenguaje formal usado para definir una sintaxis. En el caso de SNMP, la notación ASN.1 se usa para definir el formato de las unidades de datos y objetos del protocolo SNMP.

Octeto Grupo de ocho bits, con el que usualmente se opera como una entidad.

Onda periódica Una onda $f(t)$ que satisface $f(t) = f(t + nk)$ para todo entero n, siendo k una constante.

Paquete Grupo de bits que incluyen datos e información adicional de control. Generalmente se refiere a una unidad de datos del protocolo de la capa de red (capa 3 de OSI).

Par trenzado Medio de transmisión que consta de dos cables aislados dispuestos según un patrón regular en forma de espiral.

Parada y espera Protocolo de control de flujo donde la estación que envía transmite un bloque de datos y después espera un reconocimiento antes de transmitir el siguiente bloque.

Paso de testigo en anillo Técnica de control de acceso al medio para anillos. Un testigo circula por el anillo. Una estación puede transmitir captando el testigo, insertando un paquete en el anillo y retransmitiendo después el testigo.

PBX (Private Branch Exchange) Centralita privada. Una centralita de teléfono bajo el punto de vista del usuario. Proporciona un servicio de conmutación para teléfonos en líneas de extensión dentro de un edificio y de acceso a la red telefónica pública.

Periodo Valor absoluto del mínimo intervalo tras el que se obtienen los mismos valores de una onda periódica.

Petición automática de repetición Una característica que inicia automáticamente una petición de una retransmisión en la que se detecta un error en la transmisión.

Portadora Frecuencia continua capaz de ser modulada o readapatada por una segunda señal (portadora de información).

Portadora común En los Estados Unidos, las compañías que ofrecen servicios de comunicación al público. La aplicación usual es proporcionar servicios de telecomunicación a larga distancia. Las portadoras comunes son reguladas por las comisiones de regulación federales y estatales.

Protocolo Conjunto de reglas que gobiernan la operación de unidades funcionales para llevar a cabo la comunicación.

Protocolo Internet Protocolo de interconexión entre redes que proporciona servicios sin conexión a través de varias redes de conmutación de paquetes.

Puente* Unidad funcional que interconecta dos redes de área local (LAN) que usan el mismo protocolo de control de enlace lógico pero que pueden usar distintos protocolos de control de acceso al medio.

Punto a punto Configuración en la que dos estaciones comparten una ruta de transmisión.

Punto de acceso al servicio (SAP, Service Access Point) Una manera de identificar a un usuario de servicios de una entidad de protocolo. Una entidad de protocolo proporciona uno o más SAP para uso de las entidades del nivel superior.

RDSI de banda ancha (RDSI-BA) Segunda generación de la RDSI. La característica clave de la RDSI de banda ancha es que proporciona canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria RDSI.

Red de área local Red de comunicación que proporciona interconexión entre varios dispositivos de comunicación de datos en un área pequeña.

Red de comunicación Colección de unidades funcionales interconectadas que proporcionan servicios de comunicación de datos entre estaciones conectadas a la red.

Red de comunicación conmutada Red de comunicación formada por una red de nodos conectados por enlaces punto a punto. Los datos se transmiten desde la fuente al destino a través de nodos intermedios.

Red de comunicación por difusión Red de comunicación en la que la transmisión emitida por una estación es recibida por todas las demás estaciones.

Red de datos pública Una red de paquetes conmutados de monopolio nacional o controlada por el gobierno. Este servicio está disponible públicamente para procesar datos de los usuarios.

Red de valor añadido Red de paquetes conmutados privada cuyos servicios se ofertan al público.

Red digital de servicios integrados (RDSI) Servicio de telecomunicación mundial que usa transmisión digital y tecnología de conmutación para realizar comunicaciones con datos digitales y voz.

Redes interconectadas (internetwork) Conjunto de redes de conmutación de paquetes y de difusión que están interconectados mediante enrutadores.

Retardo de propagación Retardo entre el momento en el que una señal entra al canal y el momento en que se recibe.

Retransmisión de celdas (cell relay) Mecanismo de conmutación de paquetes usado para los paquetes de tamaño fijo llamados celdas. ATM se basa en la tecnología de retransmisión de celdas.

Retransmisión de tramas (frame relay) Una forma de conmutación de paquetes basada en el uso de tramas de la capa de enlace de longitud variable. No hay capa de red y muchas de las funciones básicas se descartan o eliminan para proporcionar mayor rendimiento.

Ruido Señales no deseadas que se combinan con la señal de transmisión o de recepción y que por tanto la distorsionan.

Ruido de intermodulación Ruido debido a la combinación no lineal de señales de frecuencias diferentes.

Ruido impulsivo Pulso de ruido de gran amplitud y corta duración.

Ruido térmico Ruido estadísticamente uniforme que depende de la temperatura del medio de transmisión.

Secuencia de verificación de trama Código de detección de errores insertado como campo en un bloque de datos para transmitirlos. El código sirve para comprobar errores cuando se reciben los datos.

Señal analógica Onda electromagnética que varía continuamente y se puede propagar por medios diversos.

Señal de banda limitada Una señal en la que toda la energía está contenida en un rango de frecuencia finito.

Señal digital Una señal discreta o discontinua, como, por ejemplo, un conjunto de pulsos de tensión.

Señalización de canal común Técnica en la que las señales de control de la red (por ejemplo: llamadas de petición) no se transmiten a través del camino de voz o datos asociados, sino situándola en un canal separado dedicado solamente a señalización.

Sin regreso a cero Técnica de señalización digital en la que la señal permanece en un nivel constante (distinto de cero) durante la duración completa de un bit.

Sistema intermedio (IS, Intermediate System) Dispositivo conectado a dos o más subredes en una internet y que realiza enrutamiento y relanzamiento de datos entre sistemas extremos. Ejemplos de sistemas intermedios son puentes y enrutadores.

Sondeo y selección Proceso mediante el cual una estación primaria sondea a las estaciones secundarias, una a una, invitándolas a transmitir (recepción), o solicita a una secundaria recibir datos (selección).

Tasa de bits erróneos Probabilidad de que un bit transmitido se reciba con error.

Tasa de error Cociente entre el número de unidades de datos erróneas y el número total de unidades de datos.

Tasa de error residual Porcentaje de error que permanece después de haber hecho un intento de corrección.

Técnica de ventana deslizante Método de control de flujo en el que una estación que transmite puede enviar paquetes numerados dentro de un intervalo (ventana) de números. La ventana cambia dinámicamente para permitir que se envíen paquetes adicionales.

Telemática Servicios de transmisión de información orientados a usuario. Incluye teletexto, videotexto y fax.

Test de redundancia longitudinal Uso de un conjunto de bits de paridad para un bloque de caracteres tales que hay un bit de paridad para cada posición de bit de los caracteres.

Test o comprobación de redundancia cíclica Código de detección de errores en el que el código es el resto del resultado de dividir los bits que se van a comprobar entre un número binario predeterminado.

Testigo del bus Técnica de control de acceso a bus/árbol. Las estaciones forman un anillo lógico alrededor del que se pasa el testigo. La estación que recibe el testigo puede transmitir datos y después puede pasar el testigo a la siguiente estación del anillo.

Texto cifrado La salida de un algoritmo de cifrado; la forma cifrada de un mensaje o dato.

Texto puro La entrada de una función de cifrado o la salida de una función de descifrado.

Topología Estructura, que consta de caminos y conmutadores, que proporciona el medio de interconexión entre los nodos de la red.

Trama Grupo de bits que incluye datos, además de una o más direcciones y otra información de control de protocolo. Generalmente se refiere a la unidad de datos del protocolo de la capa de enlace (capa 2 de OSI).

Transferencia de datos orientada a conexión Protocolo para intercambio de datos en el que se establece una conexión lógica entre los puntos extremos (por ejemplo: circuito virtual).

Transferencia de datos sin conexión Protocolo para intercambio de datos de una manera no planeada y sin coordinación previa (por ejemplo: datagrama).

Transmisión analógica La transmisión de señales analógicas independientemente de su contenido. La señal se puede amplificar, pero no hay intentos intermedios de extraer los datos de la señal.

Transmisión asíncrona Transmisión en la que cada carácter de información se sincroniza individualmente (normalmente usando elementos de inicio y parada).

Transmisión balanceada Modo de transmisión en el que las señales se transmiten como una corriente que viaja a través de un conductor y vuelve por otro. Para señales digitales, esta técnica se conoce como señalización diferencial, y el valor binario viene determinado por una diferencia de tensión.

Transmisión digital Transmisión de datos digitales, usando tanto señales analógicas como digitales, en la que los datos digitales se recuperan y repiten en puntos intermedios para reducir los efectos del ruido.

Transmisión en modo corriente Modo de transmisión en el que el transmisor aplica alternativamente corriente a cada uno de los dos conductores de un par trenzado para representar el 1 o 0 lógicos. La corriente total es constante y siempre en la misma dirección.

Transmisión full-duplex Transmisión de datos en ambas direcciones y al mismo tiempo.

Transmisión no balanceada Modo de transmisión en el que las señales se transmiten por un único conductor. Transmisor y receptor comparten una tierra común.

Transmisión semi-duplex Transmisión de datos en cualquier dirección, en un instante dado sólo una dirección.

Transmisión simplex Transmisión de datos solamente en una dirección preasignada.

Transmisión síncrona Transmisión de datos en la que el tiempo de ocurrencia de cada señal que representa un bit se relaciona con un marco de tiempo fijo.

Unidad de datos de protocolo (PDU, Protocol Data Unit) Conjunto de datos especificado en un protocolo de una capa dada y que consta de información de control del protocolo de esa capa, y posiblemente de datos del usuario de esa capa.

Bibliografía

ABSX92 Apple Computer, Bellcore, Sun Microsystems and Xerox. *Network Compatible ATM for Local Network Applications, Version 1.01.* October 19, 1992 (disponible en parcftp.xerox.com/pub/latm).

ARMI93 Armitage, G., and Adams, K. «Packet Reassembly During Cell Loss.» *IEEE Network,* September 1993.

ARUL96 Arulambalam, A.; Chen, X.; and Ansari, N. «Allocating Fair Rates for Available Bit Rate Service in ATM Networks.» *IEEE Communications Magazine,* November 1996.

ASH90 Ash, G. «Design and Control of Networks with Dynamic Nonhierarchical Routing.» *IEEE Communications Magazine,* October 1990.

ATM96 ATM Forum. *Traffic Management Specification Version* 4.0. April 1996.

BANT94 Bantz, D., and Bauchot, F. «Wireless LAN Design Alternatives.» *IEEE Network*, March/April, 1994.

BELL90 Bellcore (Bell Communications Research). *Telecommunications Transmission Engineering*, 3*rd Edition*. Three volumes. 1990.

BELL91 Bellamy, J. *Digital Telephony.* New York: Wiley, 1991.

BERG91 Bergman, W. «Narrowband Frame Relay Congestion Control.» *Proceedings of the Tenth Annual Phoenix Conference of Computers and Communications,* March 1991.

BERG96 Bergmans, J. *Digital Baseband Transmission and Recording.* Boston: Kluwer, 1996.

BERT92 Bertsekas, D., and Gallager, R. *Data Networks.* Englewood Cliffs, NJ: Prentice Hall, 1992.

BHAT97 Bhatnagar, P. *Engineering Networks for Synchronization, CCS 7 and ISDN.* New York: IEEE Press, 1997.

BLAC93 Black, U. *Data Link Protocols.* Englewood Cliffs, NJ: Prentice Hall, 1993.

BLAC95 Black, U. *The V Series Recommendations: Standards for Data Communications Over the Telephone Network.* New York: McGraw-Hill, 1996.

BLAC96 Black, U. *Physical Level Interfaces and Protocols.* Los Alamitos, CA: IEEE Computer Society Press, 1996.

BLAC97 Black, U. *ISDN and SS7: Architectures for Digital Signaling Networks.* Upper Saddle River, NJ: Prentice Hall, 1997.

BLAC98 Black, U. *Frame Relay Networks: Specifications and Implementations.* New York: McGraw-Hill, 1998.

BONO95 Bonomi, F., and Fendick, K. «The Rate-Based Flow Control Framework for the Available Bit Rate ATM Service.» *IEEE Network,* March/April 1995.

BORE97 Borella, M., et al. «Optical Components for WDM Lightwave Networks.» *Proceedings of the IEEE,* August 1997.

BOSE81 Bosen, R. «A Low-Speed Local Net for Under $100 per Station.» *Data Communications,* December 1981.

BOSS98 Bosse, J. *Signaling in Telecommunication Networks.* New York: Wiley, 1998.

BRAD96 Bradner, S., and Mankin, A. *IPng: Internet Protocol Next Generation.* Reading, MA: Addison-Wesley, 1996.

BURG91 Burg, J., and Dorman, D. «Broadband ISDN Resource Management: The Role of Virtual Paths.» *IEEE Communications Magazine,* September 1991.

CARL98 Carlo, J., et al. *Understanding Token Ring Protocols and Standards.* Boston: Artech House, 1999.

CARN95 Carne, E. *Telecommunications Primer.* Upper Saddle River, NJ: Prentice Hall, 1995.

CERT99 CERT Coordination Center. CERT Coordination Center 1998 Annual Report. Carnegie-Mellon University, 1999. Available at http://www.cert.org/annual_rpts/cert_rpt_98.html

CHEN89 Chen, K.; Ho, K.; and Saksena, V. «Analysis and Design of a Highly Reliable Transport Architecture for ISDN Frame- Relay Networks.» *IEEE Journal on Selected Areas in Communications,* October 1989.

CHEN96 Chen, T.; Liu, S.; and Samalam, V. «The Available Bit Rate Service for Data in ATM Networks.» *IEEE Communications Magazine,* May 1996.

CIOF97 Cioffi, J. «Asymmetric Digital Subscriber Lines.» In Gibson, J., ed. *The Communications Handbook.* Boca Raton, FL: CRC Press, 1997.

CLAR88 Clark, D. «The Design Philosophy of the DARPA Internet Protocols.» *Proceedings, SIGCOMM '88, Computer Communication Review,* August 1988; reprinted in Computer Communication Review, January 1995.

CLAR92 Clark, D.; Shenker, S.; and Zhang, L. «Supporting Real-Time Applications in an Integrated Services Packet Network: Architecture and Mechanism» *Proceedings, SIGCOMM '92,* August 1992.

CLAR95 Clark, D. *Adding Service Discrimination to the Internet.* MIT Laboratory for Computer Science Technical Report, September 1995. Available at http://ana-www.lcs.mit.edu/anaweb/papers.html

COME99 Comer, D., and Stevens, D. *Internetworking with TCP/IP, Volume II: Design Implementation, and Internals.* Upper Saddle River, NJ: Prentice Hall, 1999.

COME97 Comer, D., and Stevens, D. *Internetworking with TCP/IP, Volume III: Client-Server Programming and Applications.* Upper Saddle River, NJ: Prentice Hall, 1997.

COME95 Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture.* Upper Saddle River, NJ: Prentice Hall, 1995.

COUC97 Couch, L. *Digital and Analog Communication Systems.* Upper Saddle River, NJ: Prentice Hall, 1997.

CROW97 Crow, B., et al. «IEEE 802.11 Wireless Local Area Networks.» *IEEE Communications Magazine,* September 1997.

DAVI89 Davies, D. and Price, W., *Security for Computer Networks.* New York: Wiley, 1989.

DIFF76 Diffie, W. and Hellman, M., «New Directions in Cryptography.» *IEEE Transactions on Information Theory,* November 1976.

DIJK59 Dijkstra, E. «A Note on Two Problems in Connection with Graphs.» *Numerical Mathematics,* October 1959.

DIXO94 Dixon, R. *Spread Spectrum Systems with Commercial Applications.* New York: Wiley, 1994.

DORL96 Dorling, B.; Pieters, P.; and Valenzuela, E. *IBM Frame Relay Guide.* IBM Publication SG24-4463-01, 1996. Available at www.redbooks.ibm.com.

DOSH88 Doshi, B., and Nguyen, H. «Congestion Control in ISDN Frame-Relay Networks.» *AT&T Technical Journal,* November/December 1988.

EFF98 Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design.* Sebastopol, CA: O'Reilly, 1998

FIOR95 Fiorini, D.; Chiani, M.; Tralli, V.; and Salati, C. «Can We Trust HDLC?» *Computer Communications Review,* October 1995.

FORD62 Ford, L. and Fulkerson, D. *Flows in Networks.* Princeton, NJ: Princeton University Press, 1962.

FRAZ99 Frazier, H., and Johnson, H. «Gigabit Ethernet: From 100 to 1,000 Mbps.» *IEEE Internet Computing,* January/February 1999.

FREE94 Freeman, R. *Reference Manual for Telecommunications Engineering.* New York: Wiley, 1994.

FREE96 Freeman, R. *Telecommunication System Engineering.* New York: Wiley, 1996.

FREE98a Freeman, R. *Telecommunications Transmission Handbook.* New York: Wiley, 1998.

FREE98b Freeman, R. «Bits, Symbols, Bauds, and Bandwidth.» *IEEE Communications Magazine,* April 1998.

GARR96 Garrett, M. «A Service Architecture for ATM: From Applications to Scheduling.» *IEEE Network,* May/June 1996.

GAUD89 Gaudette, P. *A Tutorial on ASN.1.* Technical Report NCSL/SNA-89/12. Gaithersburg, MD: National Institute of Standards and Technology, 1989.

GEIE99 Geier, J. *Wireless LANs.* New York: Macmillan Technical Publishing, 1999.

GERS91 Gersht, A. and Lee, K., «A Congestion Control Framework for ATM Networks.» *IEEE Journal on Selected Areas in Communications,* September 1991.

GIBS93 Gibson, J. *Principles of Digital and Analog Communications.* New York: Macmillan, 1993.

GIRA90 Girard, A. *Routing and Dimensioning in Circuit-switching Networks.* Reading, MA: Addison-Wesley, 1990.

GLOV98 Glover, I., and Grant, P. *Digital Communications.* Upper Saddle River, NJ: Prentice Hall, 1998.

GORA95 Goralski, W. *Introduction to ATM Networking.* New York: McGraw-Hill, 1995.

HALS96 Halsall, F. *Data Communications, Computer Networks, and Open Systems.* Reading, MA: Addison-Wesley, 1996.

HAMM86 Hammond, J., and O'Reilly, P. *Performance Analysis of Local Computer Networks.* Reading, MA: Addison-Wesley, 1986.

HAND94 Handel, R.; Huber, N.; and Schroder, S. *ATM Networks: Concepts, Protocols, Applications.* Reading, MA: Addison- Wesley, 1994.

HARB92 Harbison, R. «Frame Relay: Technology for Our Time.» *LAN Technology,* December 1992.

HAWL97 Hawley, G. «Systems Considerations for the Use of xDSL Technology for Data Access.» *IEEE Communications Magazine,* March 1997.

HAYK94 Haykin, S. *Communication Systems.* New York: Wiley, 1995.

HIND83 Hinden, R.; Haverty, J.; and Sheltzer, A. «The DARPA Internet: Interconnecting Heterogeneous Computer Networks with Gateways.» *Computer,* September 1983.

HIND95 Hinden, R. «IP Next Generation Overview.» *Connexions,* March 1995.

HUIT95 Huitema, C. *Routing in the Internet.* Englewood Cliffs, NJ: Prentice Hall, 1995.

HUIT98 Huitema, C. IPv6: *The New Internet Protocol.* Upper Saddle River, NJ: Prentice Hall, 1998.

HUMP97 Humphrey, M., and Freeman, J. «How xDSL Supports Broadband Services to the Home.» *IEEE Network,* January/March 1997.

JACO88 Jacobson, V. «Congestion Avoidance and Control.» *Proceedings, SIGCOMM '88, Computer Communication Review,* August 1988; reprinted in *Computer Communication Review,* January 1995; a slightly revised version is available at ftp.ee.lbl.gov/papers/congavoid.ps.Z

JACO90 Jacobson, V. «Berkeley TCP Evolution from 4.3 Tahoe to 4.3-Reno.» *Proceedings of the Eighteenth Internet Engineering Task Force,* September 1990.

JAIN90 Jain, R. «Congestion Control in Computer Networks: Issues and Trends.» *IEEE Network Magazine,* May 1990.

JAIN91 Jain, R. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling.* New York: Wiley, 1991.

JAIN92 Jain, R. «Myths About Congestion Management in High-Speed Networks.» *Internetworking: Research and Experience,* Volume 3, 1992.

JAIN93 Jain, B., and Agrawala, A. *Open Systems Interconnection.* New York: McGraw-Hill, 1993.

JAIN96 Jain, R., et al. «Source Behavior for ATM ABR Traffic Management: An Explanation. *IEEE Communications Magazine,* November 1996.

JAME95 James, J. *A Student's Guide to Fourier Transforms.* Cambridge, England: Cambridge University Press, 1995.

KADA98 Kadambi, J.; Crayford, I.; and Kalkunte, M. *Gigabit Ethernet.* Upper Saddle River, NJ: Prentice Hall, 1998.

KAHN97 Kahn, J., and Barry, J. «Wireless Infrared Communications.» *Proceedings of the IEEE,* February 1997.

KALI91 Kaliski, B. *A Layman's Guide to a Subset of ASN.1, BER, and DER.* Report SEC-SIG-91-17, Redwood City, CA: RSA Data Security Inc. 1991.

KARN91 Karn, P., and Partridge, C. «Improving Round-Trip Estimates in Reliable Transport Protocols.» *ACM Transactions on Computer Systems,* November 1991.

KAVA95 Kavak, N. «Data Communication in ATM Networks.» *IEEE Network,* May/June 1995.

KESH98 Keshav, S., and Sharma, R. «Issues and Trends in Router Design.» *IEEE Communications Magazine,* May 1998.

KESS99 Kessler, G., and Southwick, P *ISDN: Concepts, Facilities, and Services.* New York: McGraw-Hill, 1999.

KHAN89 Khanna, A. and Zinky, J. «The Revised ARPANET Routing Metric.» *Proceedings, SIGCOMM '89 Sypmosium,* 1989.

KLEI76 Kleinrock, L. *Queuing Systems, Volume II: Computer Applications.* New York: Wiley, 1976.

KUMA98 Kumar, V.; Lakshman, T.; and Stiliadis, D. «Beyond Best Effort: Router Architectures for the Differentiated Services of Tomorrow's Internet.» *IEEE Communications Magazine,* May 1998.

LATH98 Lathi, B. *Modern Digital and Analog Communication Systems.* New York: Oxford University Press, 1998.

LEUT94 Leutwyler, K. «Superhack.» *Scientific American,* July 1994.

LUIN97 Luinen, S., Budrikis, Z.; and Cantoni, A. «The Controlled Cell Transfer Capability.» *Computer Communications Review,* January 1997.

MAXW96 Maxwell, K. «Asymmetric Digital Subscriber Line: Interim Technology for the Next Forty Years.» *IEEE Communications Magazine,* October 1996.

MCDO91 McDonald, C. «A Network Specification Language and Execution Environment for Undergraduate Teaching.» *Proceedings of the ACM Computer Science Educational Technical Symposium,* March 1991.

MCDY99 McDysan, D., and Spohn, D. *ATM: Theory and Applications.* New York: McGraw-Hill, 1999.

MCQU80 McQuillan, J.; Richer, I.; and Rosen, E. «The New Routing Algorithm for the ARPANET.» *IEEE Transactions on Communications,* May 1980.

MEEK90 Meeks, F. «The Sound of Lamarr.» *Forbes,* May 14, 1990.

MILL95 Mills, A. *Understanding FDDI.* Englewood Cliffs, NJ: Prentice Hall, 1995.

MILL98 Miller, S. *IPv6: The Next Generation Internet Protocol.* Bedford, MA: Digital Press, 1008.

MOSH89 Moshos, G. *Data Communications: Principles and Problems.* New York: West Publishing Co., 1989.

MURH98 Murhammer, M., et al. *TCP/IP: Tutorial and Technical Overview.* Upper Saddle River, NJ: Prentice Hall, 1998.

NAUG96 Naugle, M. *Local Area Networking.* New York: McGraw-Hill, 1996.

NEWM94 Newman, P. «ATM Local Area Networks.» *IEEE Communications Magazine,* March 1994.

OSHA95 Oshaki, H., et al. «Rate-Based Congestion Control for ATM Networks.» *Computer Communication Review,* April 1995.

PAHL95 Pahlavan, K.; Probert, T.; and Chase, M. «Trends in Local Wireless Networks.» *IEEE Communications Magazine,* March 1995.

PARE88 Parekh, S., and Sohraby, K. «Some Performance Trade-Offs Associated with ATM Fixed-Length Vs. Variable-Length Cell Formats.» *Proceedings, GlobeCom,* November 1988.

PEAR92 Pearson, J. *Basic Communication Theory.* Englewood Cliffs, NJ: Prentice Hall, 1992.

PEEB87 Peebles, P. *Digital Communication Systems.* Englewood Cliffs, NJ: Prentice Hall, 1987.

PERL92 Perlman, R. *Interconnections: Bridges and Routers.* Reading, MA: Addison-Wesley, 1992.

PETE95 Peterson, R.; Ziemer, R.; and Borth, D. *Introduction to Spread Spectrum Communications.* Englewood Cliffs, NJ: Prentice Hall, 1995.

PETE96 Peterson, L., and Davie, B. *Computer Networks: A Systems Approach.* San Francisco: Morgan Kaufmann, 1996.

PITT96 Pitts, J., and Schormans, J. *Introduction to ATM Design and Performance.* New York: Wiley, 1996.

PROA94 Proakis, J., and Salehi, M. *Communication Systems Engineering.* Englewood Cliffs, NJ: Prentice Hall, 1995.

PRYC96 Prycker, M. *Asynchronous Transfer Mode: Solutions for Broadband ISDN.* New York: Ellis Horwood, 1996.

RAMA88 Ramabadran, T., and Gaitonde, S. «A Tutorial on CRC Computations.» *IEEE Micro,* August 1988.

RIVE78 Rivest, R.; Shamir, A.; and Adleman, L. «A Method for Obtaining Digital Signatures and Public Key Cryptosystems.» *Communications of the ACM,* February 1978.

REEV95 Reeve, W. *Subscriber Loop Signaling and Transmission Handbook.* Piscataway, NJ: IEEE Press, 1995.

ROSE93 Rose, M. *The Internet Message: Closing the Book with Electronic Mail.* Englewood Cliffs, NJ: Prentice Hall, 1993.

RUSS95 Russell, R. *Signaling System #7.* New York: McGraw-Hill, 1995.

SACH96 Sachs. M., and Varma, A. «Fibre Channel and Related Standards.» *IEEE Communications Magazine,* August 1996.

SAIT96 Saito, J., et al. «Performance Issues in Public ABR Service.» *IEEE Communications Magazine,* November 1996.

SATO90 Sato, K.; Ohta, S.; and Tokizawa, I. «Broad-band ATM Network Architecture Based on Virtual Paths.» *IEEE Transactions on Communications,* August 1990.

SCHN96 Schneier, B. *Applied Cryptography.* New York: Wiley, 1996.

SCHW77 Schwartz, M. *Computer-Communication Network Design and Analysis.* Englewood Cliffs, NJ: Prentice Hall, 1977.

SCHW96 Schwartz, M. *Broadband Integrated Networks.* Upper Saddle River, NJ: Prentice Hall PTR, 1996.

SEIF98 Seifert, R. *Gigabit Ethernet.* Reading, MA: Addison Wesley, 1998.

SHAH94 Shah, A., and Ramakrishnan, G. *FDDI: A High-Speed Network.* Englewood Cliffs, NJ: Prentice Hall, 1994.

SHEN95 Shenker, S. «Fundamental Design Issues for the Future Internet.» *IEEE Journal on Selected Areas in Communications,* September 1995.

SKLA88 Sklar, B. *Digital Communications: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice Hall, 1988.

SKLA93 Sklar, B. «Defining, Designing, and Evaluating Digital Communication Systems.» *IEEE Communications Magazine,* November 1993.

SPOH97 Spohn, D. *Data Network Design.* New York: McGraw-Hill, 1994.

SPRA91 Spragins, J.; Hammond, J.; and Pawlikowski, K. *Telecommunications Protocols and Design.* Reading, MA: Addison-Wesley, 1991.

SPUR96 Spurgeon, C. *Ethernet Configuration Guidelines.* San Jose, CA: Peer-to-Peer Communications, 1996.

STAL98 Stallings, W. *High-Speed Networks: TCP/IP and ATM Design Principles.* Upper Saddle River, NJ: Prentice Hall, 1998.

STAL99a Stallings, W. *Cryptography and Network Security: Principles and Practice, 2nd Edition.* Upper Saddle River, NJ: Prentice Hall, 1999.

STAL99b Stallings, W. *ISDN and Broadband ISDN, with Frame Relay and ATM.* Upper Saddle River, NJ: Prentice Hall, 1999.

STAL99c Stallings, W. *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.* Reading, MA: Addison-Wesley, 1999.

STAL00 Stallings, W. *Local and Metropolitan Area Networks, 6th Edition.* Upper Saddle River, NJ: Prentice Hall, 2000.

STEE90 Steedman, D. *ASN.1: The Tutorial and Reference.* London: Technology Appraisals, 1990.

STEE95 Steenstrup, M. *Routing in Communications Networks.* Englewood Cliffs, NJ: Prentice Hall, 1995.

STEI95 Steinke, S. «IP Addresses and Subnet Masks.» *LAN Magazine,* October 1995.

STEV94 Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols. Reading,* MA: Addison-Wesley, 1994.

STEV96 Stevens, W. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX(R) Domain Protocol.* Reading, MA: Addison-Wesley, 1996.

STUC85 Stuck, B., and Arthurs, E. *A Computer Communications Network Performance Analysis Primer.* Englewood Cliffs, NJ: Prentice Hall, 1985.

SUZU94 Suzuki, T. «ATM Adaptation Layer Protocol.» *IEEE Communications Magazine,* April 1994.

TANE96 Tanenbaum, A. *Computer Networks.* Upper Saddle River, NJ: Prentice Hall, 1996.

TRUL97 Trulove, J. *LAN Wiring.* New York: McGraw-Hill, 1997.

TSUD92 Tsudik, G. «Message Authentication with One-Way Hash Functions.» *Computer Communications Review,* October 1992.

TUCH79 Tuchman, W. «Hellman Presents No Shortcut Solutions to DES.» *IEEE Spectrum,* July 1979.

VALE92 Valenzano, A., DeMartini, C. and Ciminiera, L. *MAP and TOP Communications: Standards and Applications.* Reading, MA: Addison-Wesley, 1992.

WANG92 Wang, Z., and Crowcroft, J. «SEAL Detects Cell Misordering.» *IEEE Network,* July 1992.

WEIS98 Weiss, W. «QoS with Differentiated Services.» *Bell Labs Technical Journal,* October-December 1998.

WHIT97 White, P., and Crowcroft, J. «The Integrated Services in the Internet: State of the Art.» *Proceedings of the IEEE,* December 1997.

WIDM83 Widmer, A., and Franaszek, P. «A DC-Balanced, Partitioned, 8B/10B Transmission Code.» *IBM Journal of Research and Development,* September 1983.

WILL97 Willner, A. «Mining the Optical Bandwidth for a Terabit per Second.» *IEEE Spectrum,* April 1997.

WRIG95 Wright, G., and Stevens, W. *TCP/IP Illustrated, Volume 2: The Implementation.* Reading, MA: Addison-Wesley, 1995.

XIAO99 Xiao, X., and Ni, L. «Internet QoS: A Big Picture.» *IEEE Network,* March/April 1999.

YANG95 Yang, C., and Reddy, A. «A Taxonomy for Congestion Control Algorithms in Packet Switching Networks.» *IEEE Network,* July/August 1995.

YEN83 Yen, C., and Crawford, R. «Distribution and Equalization of Signal on Coaxial Cables Used in 10-Mbits Baseband Local Area Networks.» *IEEE Transactions on Communications,* October 1983.

ZHAN86 Zhang, L. «Why TCP Timers Don't Work Well.» *Proceedings, SIGCOMM '86 Symposium,* August 1986.

ZHAN93 Zhang, L.; Deering, S.; Estrin, D.; Shenker, S.; and Zappala, D. «RSVP: A New Resource ReSerVation Protocol.» *IEEE Network,* September 1993.

ZHAN95 Zhang, H. «Service Disciplines for Guaranteed Performance Service in Packet-Switching Networks.» *Proceedings of the IEEE,* October 1995.

Índice alfabético

E

F

G

H

I

J

K

L

M

N

O

T

U

V

W

X

ACRÓNIMOS

Acrónimo	Término en inglés	Término en castellano
AAL	ATM Adaptation Layer	Capa de adaptación ATM
ADSL	Asymmetric Digital Subscriber Line	Línea de abonado digital asimétrica
AES	Advanced Encryuption Standard	Normalización avanzada de cifrado
AM	Amplitude Modulation	Modulación en amplitud
AMI	Alternate Mark Inversion	Inversión de marca alternada
ANS	American National Standard	Normalización nacional americana
ANSI	American National Standard Institute	Instituto de normalizaciones nacional americano
ARQ	Automatic Repeat Request	Petición de repetición automática
ASCII	American Standard Code for Information Interchange	Código normalizado americano para intercambio de información
ASK	Amplitude-Shift Keying	Modulación por desplazamiento de amplitud
ATM	Aynchronous Transfer Mode	Modo de transferencia asíncrono
BER	Bit Error Rate	Tasa de bits erróneos
RDSI-BA	Broadband ISDN	RDSI de banda ancha
BGP	Border Gateway Protocol	Protocolo de pasarela externa
BOC	Bell Operating Company	
CBR	Constant Bit Rate	Velocidad de transmisión de bits constante
CCITT	International Consultative Committee on Telegraphy and Telephony	Comité de consulta internacional en telegrafía y telefonía
CIR	Committed Information Rate	Razón de información comprometida
CMI	Coded Mark Inversion	Inversión de marca codificada
CRC	Cyclic Redundancy Check	Test de redundancia cíclica
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	Acceso múltiple sensible a portadora con detección de colisión
DCE	Data Circuit-Terminating Equipment	Equipo de terminación del circuito de datos
DEA	Data Encryption Algorithm	Algoritmo de cifrado de datos
DES	Data Encryption Standard	Normalización de cifrado de datos
DS	Differentiated Services	Servicios diferenciados
DTE	Data Terminal Equipment	Equipo terminal de datos
FCC	Federal Communications Commission	Comisión federal de comunicaciones
FCS	Frame Check Sequence	Secuencia de test de trama
FDDI	Fiber Distributed Data Interface	Interfaz para distribución de datos en fibra
FDM	Frecuency-Division Multiplexing	Multiplexación por división de frecuencia
FSK	Frecuency-Shift Keying	Modulación por desplazamiento de frecuencia
FTP	File Transfer Protocol	Protocolo de transferencia de ficheros
FM	Frecuency Motulation	Modulación en frecuencia
HDLC	High-Level Data Link Control	Control de enlace de datos de alto nivel
HTTP	Hypertext Transfer Protocol	Protocolo de transferencia de hipertextos
IAB	Internet Architecture Board	Tarjeta de arquitectura Internet
ICMP	Internet Control Message Protocol	Protocolo de mensajes de control Internet
RDI	Integrated Digital Network (IDN)	Red digital integrada
IEEE	Institute of Electrical and Electronics Engineers	Instituto de ingenieros eléctricos y electrónicos
IETF	Internet Engineering Task Force	Agrupación de esfuerzos para ingeniería internet
IGMP	Internet Group Management Protocol	
IP	Internet Protocol	Protocolo internet
IPng	Internet Protocol—Next Generation	Protocolo internet de próxima generación
IRA	International Reference Alphabet	Alfabeto de referencia internacional
ISA	Integrated Services Architecture	Arquitectura de servicios integrados
ISO	International Organization for Standardization	Organización internacional para normalizaciones
ITU	International Telecommunication Union	Unión internacional para telecomunicaciones

Acrónimo	Término en inglés	Término en castellano
ITU-T	ITU Telecommunication Standardization Sector	Sector de normalización de telecomunicaciones de la ITU
LAN	Local Area Network	Red de área local
LAPB	Link Access Procedure—Balanced	Procedimiento balanceado de acceso a enlace
LAPD	Link Access Procedure on the D Channel	Procedimiento de acceso a enlace en el canal D
LAPF	Link Access Procedure for Frame Mode Bearer Services	Procedimiento de acceso a enlace para servicios que admiten modo de trama
LLC	Logical Link Control	Control de enlace lógico
MAC	Medium Access Control	Control de acceso al medio
MAN	Metropolitan Area Network	Red de área metropolitana
MIME	Multi-Purpose Internet Mail Extension	Ampliación para correo internet multiuso
NRZI	Nonretun to Zero, Inverted	Sin retorno a cero, invertido
NRZL	Nonretun to Zero, Level	Sin retorno a cero, de nivel
NT	Network Termination	Terminación de red
OSI	Open Systems Interconnection	Interconexión de sistemas abiertos
OSPF	Open Shortest Path First	Primer camino abierto más corto
PBX	Private Branch Exchange	Centralita telefónica privada
PCM	Pulse Code Modulation	Modulación por código de pulsos
PDU	Protocol Data Unit	Unidad de datos de protocolo
PSK	Phase-Shift Keying	Modulación por desplazamiento de fase
PTT	Postal, Telegrah, and Telephone	Correo, telégrafo y teléfono
PM	Phase Modulation	Modulación en fase
QAM	Quadrature Amplitude Modulation	Modulación en amplitud de cuadratura
QoS	Quality of Service	Calidad del servicio
QPSK	Quadrature Phase-Shift Keying	Modulación por desplazamiento de fase en cuadratura
RBOC	Regional Bell Operating Company	
RDSI	Integrated Services Digital Network (ISDN)	Red digital de servicios integrados
RF	Radio Frecuency	Radio frecuencia
RSA	Rivest, Shamir, Adleman Algorithm	Algoritmo de Rivest, Shamir y Adleman
RSVP	Resource ReSerVation Protocol	Protocolo de reserva de recurso
SAP	Service Access Point	Punto de acceso al servicio
SDH	Syncrhonous Digital Hierarchy	Jerarquía digital síncrona
SDU	Service Data Unit	Unidad de datos del servicio
SMTP	Simple Mail Transfer Protocol	Protocolo sencillo de transferencia de correo
SNMP	Simple Network Management Protocol	Protocolo sencillo de gestión de red
SONET	Syncrhonous Optical Network	Red óptica síncrona
SS7	Signaling System Number 7	Sistema de señalización numero 7
STP	Shielded Twisted Pair	Par trenzado apantallado
TCP	Transmission Control Protocol	Protocolo de control de transmisión
TDEA	Triple Data Encryption Algorithm	Algoritmo triple de cifrado de datos
TDM	Time-Division Multiplexing	Multiplexación por división en el tiempo
TE	Terminal Equipment	Equipo terminal
UDP	User Datagram Protocol	Protocolo de datagrama de usuario
UNI	User-Network Interface	Interfaz usuario-red
URI	Universal Resource Identifier	Identificador universal de recursos
URL	Uniform Resource Locator	Localizador uniforme de recursos
UTP	Unshielded Twister Pair	Par trenzado sin apantallar
VAN	Value-Added Network	Red de valor añadido
VBR	Variable Bit Rate	Velocidad de transmisión de bits variable
VCC	Virtual Channel Connection	Conexión a canal virtual
VPC	Virtual Path Connection	Conexión a camino virtual
WDM	Wavelength Division Multiplexing	Multiplexación por división de longitud de onda
WWW	World Wide Web	Red extendida por todo el mundo