Redes de Datos

Resumen

Unidad 1 - Introducción

Internet

Internet conecta **hosts** o **sistemas terminales** mediante **enlaces de comunicación** y **conmutadores de paquetes**.

Los conmutadores de paquetes más comunes son los **routers** y los **switches** de la capa de enlace.

Los **ISP** (Internet Service Provider) son redes de conmutadores y enlaces. Los hay de nivel inferior, que se conectan a otros de nivel superior para la comunicación a mayor distancia. Los ISP de nivel superior consisten en routers conectados con fibra óptica.

Los protocolos en internet controlan el envío y la recepción de información.

TCP (Transmission Control Protocol) especifica cómo se realiza la conexión, e **IP** (Internet Protocol) indica el formato de los paquetes. **TCP/IP** son los principales protocolos de internet.

Los estándares de internet son desarrollados por el IETF (Internet Engineering Task Force). Los documentos asociados a estos estándares se conocen como RFC (Request For Comments).

Cuando una aplicación involucra a muchos sistemas terminales que intercambian datos, se dice que es **distribuida**. Esto se logra mediante una **API** (Application Programming Interface).

Redes

Un **protocolo** define el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican, así como las acciones tomadas en la transmisión y/o la recepción de un mensaje u otro suceso.

Un programa **cliente** es aquel que se ejecuta en un sistema terminal y recibe un servicio de un programa **servidor** en otro sistema terminal. Estos programas forman **aplicaciones distribuidas**.

Otra arquitectura de aplicación posible es **P2P** (Peer-to-Peer), donde los sistemas terminales cumplen funciones tanto de cliente como de servidor.

Hay equipos activos (que utilizan corriente) y pasivos.

Las redes de acceso son los enlaces físicos que conectan un sistema terminal con el primer router (router de acceso).

Formas comunes de acceso a Internet:

- Acceso telefónico: permite conectarse a internet reutilizando las redes telefónicas, pero tiene una velocidad máxima de 56kbps.

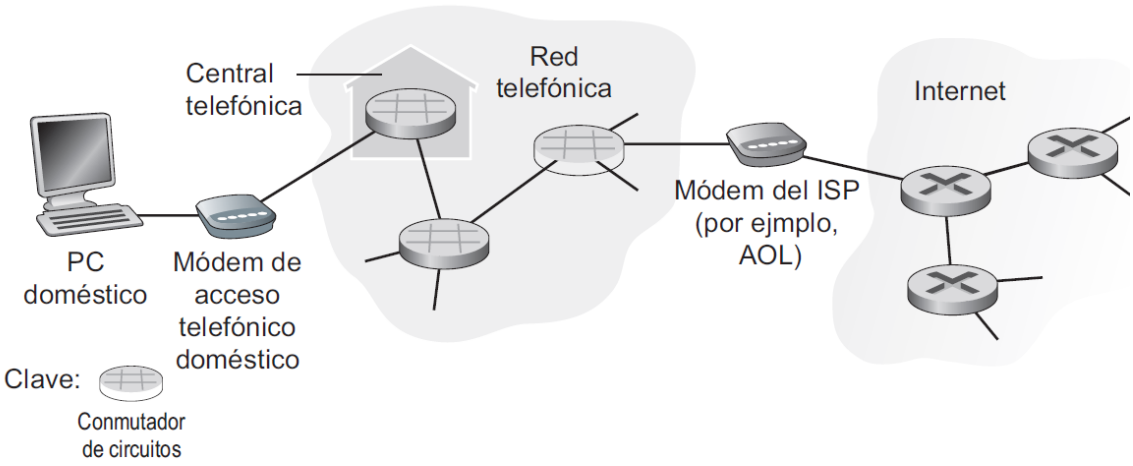


Figura 1.5 • Acceso telefónico a Internet.

- DSL (Digital Subscriber Line): se utiliza la línea telefónica existente para intercambiar datos con un DSLAM (DSL Access Multiplexer). Así, por el mismo cable hay tres canales: uno de descarga (alta velocidad), de carga (velocidad media) y uno telefónico bidireccional. Es efectivo cuando el domicilio se encuentra a un radio de entre 8km y 16km de la central.

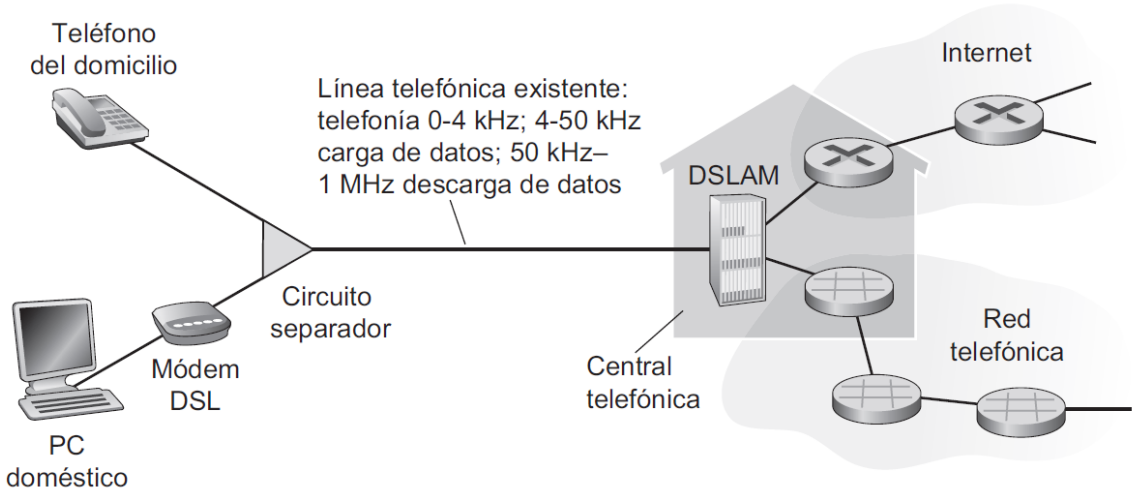


Figura 1.6 • Acceso mediante DSL a Internet.

- Cable (HFC, Hybrid Fiber Coax): consiste en utilizar la red existente de televisión por cable, mediante módems por cable. Tiene dos canales, uno de descarga más veloz y uno de carga más lento. Todos los sistemas terminales se comunican por el mismo cable, por lo que si hay mucha demanda se ralentiza.

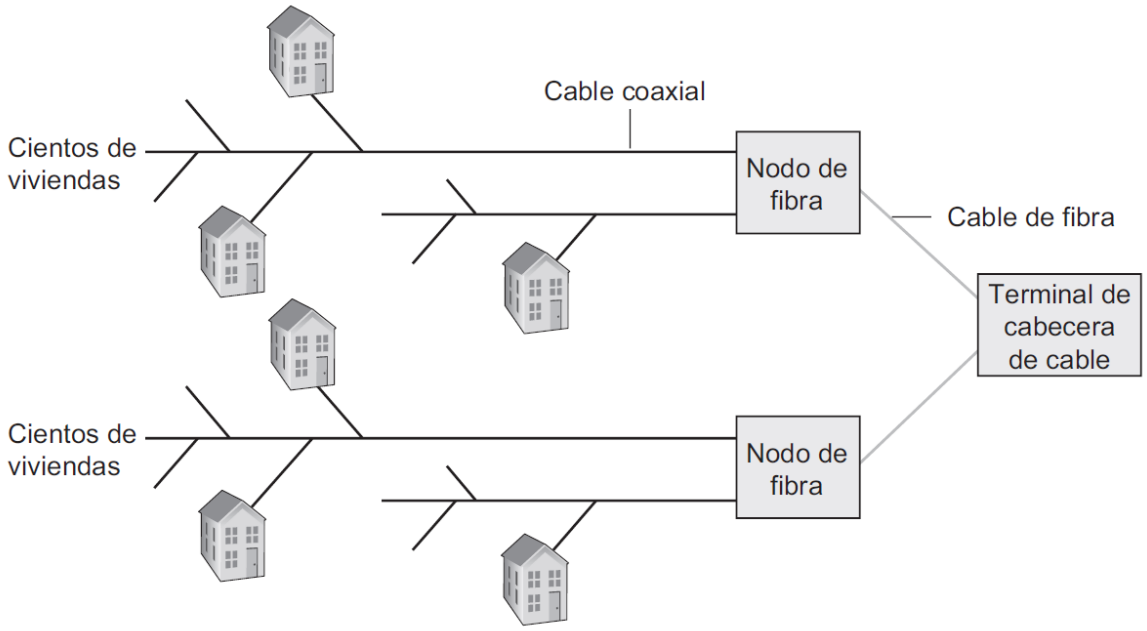


Figura 1.7 • Red de acceso híbrida de fibra óptica y cable coaxial.

- FTTH (Fiber To The Home): utilizando fibra óptica para conectar la central con los hogares. Puede ser por fibra directa o compartida (AON, Active Optical Network o PON, Passive Optical Network). Las redes AON son redes Ethernet conmutadas.
  En las redes PON, cada vivienda cuenta con un router conectado a un ONT (Optical Network Terminator), que se conecta a un distribuidor óptico. Este, combina hasta 100 viviendas en un único cable de fibra óptica compartido, que va hasta un OLT (Optical Line Terminator) de la central.

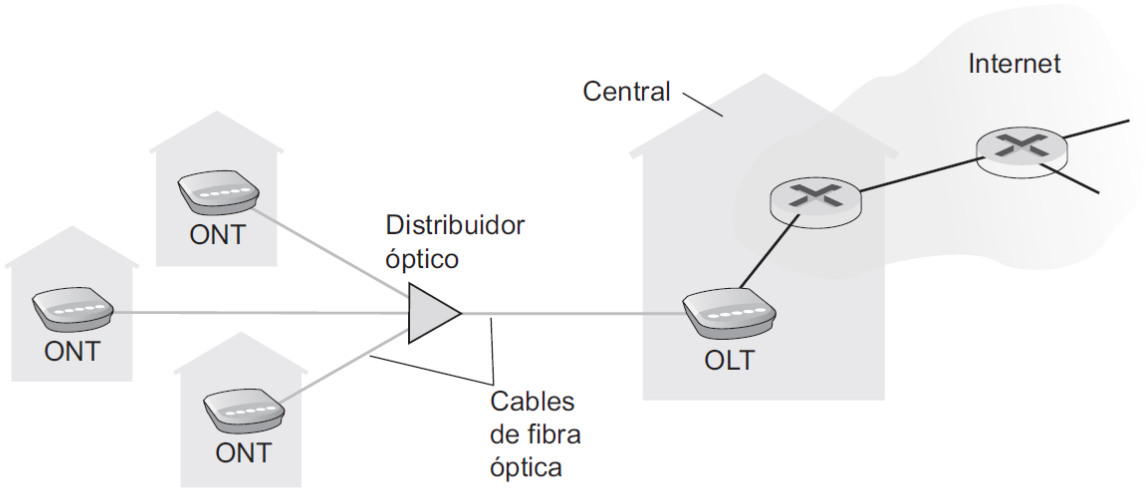


Figura 1.8 • Acceso a Internet mediante FTTH.

- Ethernet: para su uso en LAN (Local Area Network).

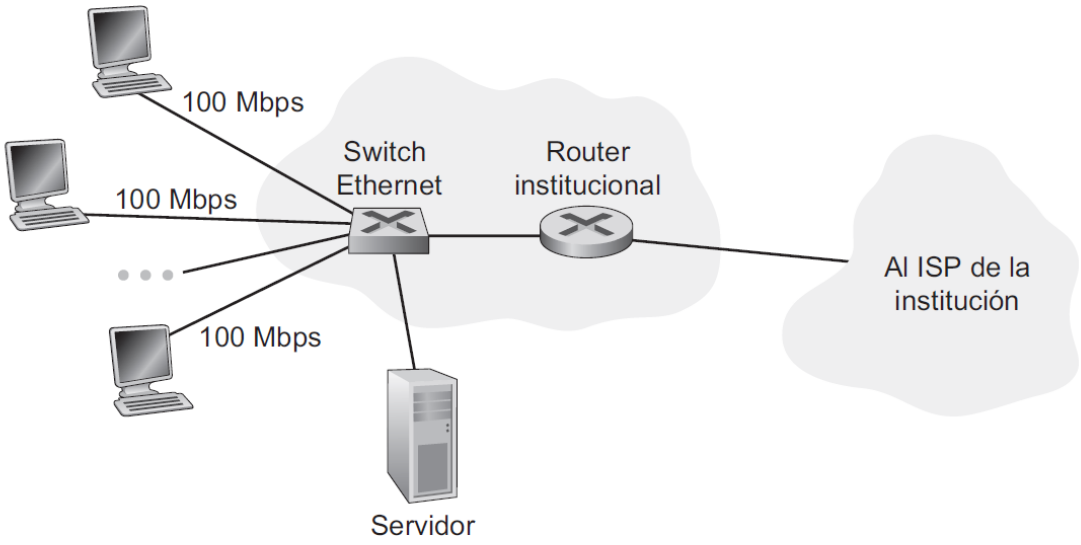


Figura 1.9 • Acceso a Internet utilizando tecnología Ethernet.

- WiFi: permite tener una LAN Inalámbrica, mediante un AP (Access Point) conectado a Internet mediante cable. Utiliza el protocolo IEEE 802.11.

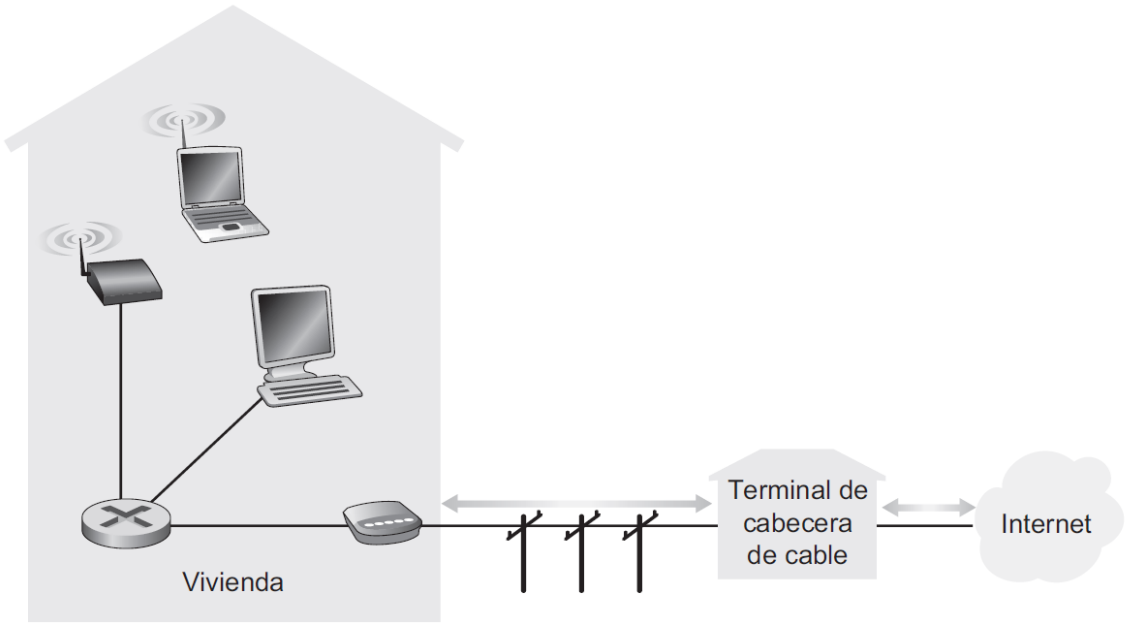


Figura 1.10 • Esquema de una red doméstica típica.

- Acceso inalámbrico de área extensa: los paquetes se transmiten a una estación base a través de la misma infraestructura utilizada por la telefonía móvil.
- WiMax: IEEE 802.16 establece una posible mejora a WiFi, incrementando significativamente el alcance sin recurrir a la red de telefonía móvil.

Medios Físicos

Los hay guiados (propagación por un medio sólido) y no guiados (propagación por la atmósfera).

- Cable de cobre de par trenzado: medio guiado más barato. Consta de dos cables de cobre de un milímetro de espesor aislados, que siguen un patrón en espiral (para reducir interferencias de otros cables similares cercanos).

  Normalmente, una serie de pares se meten dentro de un cable que los envuelve con una pantalla protectora.

  El UTP (Unshielded Twisted Pair) suele ser utilizado en redes LAN.
- Cable coaxial: consta de dos conductores de cobre dispuestos de forma concéntrica.
- Fibra óptica: tiene velocidades de transmisión muy altas y presenta muy poca atenuación, siendo también inmune a las interferencias electromagnéticas.
- Canales de radio terrestres: son clasificables según si cubren un área local o extensa.
- Canales de radio vía satélite: mediante satélites geoestacionarios (órbita GEO) y de órbita baja (LEO).

Núcleo de la red

Conmutación de circuitos

Para establecer la conexión, se debe reservar un ancho de banda dedicado a la misma. Esto se puede lograr de dos maneras: multiplexación por división de frecuencia (FDM) o de tiempo (TDM). Con FDM, el ancho de banda se divide para las distintas conexiones; y con TDM, hay una división del canal en marcos de tiempo que podrá usar cada conexión con todo el ancho de banca.

Ambos métodos implican un derroche en los periodos de inactividad, y además requieren software de señalización complejo para coordinar el funcionamiento de los switches.

Conmutación de paquetes

Las distintas conexiones comparten ancho de banda. Se envían paquetes, que son retransmitidos por conmutadores (routers o switches de la capa de enlace).

Hay retardos por el medio de enlace en sí, por el método de transmisión de almacenamiento y reenvío (el conmutador no reenvía el paquete hasta haberlo recibido por completo) y por acumulación de paquetes en el buffer de salida. Si se llenara el buffer de salida, podría también haber pérdida de paquetes.

Se le llama multiplexación estadística de recursos a esta compartición bajo petición que se logra mediante paquetes.

La mayor crítica son los retardos variables e impredecibles.

Los routers cuentan con una tabla de reenvío, que indican a dónde se debe reenviar un paquete tras analizar una parte de la dirección de destino del mismo.

Los ISP de nivel 1 son aquellos de alcance internacional que se encuentran todos conectados entre sí. Son llamados proveedores de ISP de nivel 2, más regionales. Así, se establece una jerarquía con ISP de niveles inferiores, finalizando con los ISP de acceso (que pueden ser clientes de ISP de distintos niveles superiores). Los puntos en que un ISP se conecta a otro se llaman **puntos de presencia** (POP).

Retardos, pérdidas y tasa de transferencia en las redes de conmutación de paquetes

Retardo

Retardo nodal: se calcula como la suma de:

- Procesamiento: tiempo utilizado, entro otros motivos, para examinar la cabecera de un paquete y determinar dónde enviarlo.
- Cola: tiempo a esperar para que el paquete sea transmitido por el número de paquetes que haya llegado antes.
  Intensidad de tráfico = velocidad de llegada de bit / velocidad de transmisión de bits. Al estar cerca de 0, el retardo es pequeño, y crece exponencialmente al acercarse a 1.
  Al llenarse la cola, se pierden los paquetes.
- Transmisión: tiempo necesario para introducir todos los bits del paquete por el enlace.
- Propagación: tiempo que tarda un bit en ir de un router al otro. Depende del medio físico del enlace.

Retardo terminal: se puede calcular sumando los retardos de los nodos de la ruta hacia el sistema terminal destino, y agregar posibles retardos de módem o empaquetamiento, por ejemplo.

Tasa de transferencia

Es la velocidad a la que llegan los bits descargados al sistema terminal destino. Se encuentra determinado por el enlace cuello de botella, es decir, aquel que menor velocidad tenga en el momento de la descarga (según su velocidad habitual y la demanda momentánea del enlace).

Capas

Pila de protocolos: conjunto de protocolos de las distintas capas.

Capas de Internet: Física, Enlace, Red, Transporte y Aplicación.

Capas OSI (Open Systems Interconnection): Física, Enlace, Red, Transporte, Sesión, Presentación y Aplicación.

- Capa de **Aplicación**: aquí residen las aplicaciones de red y sus protocolos (HTTP, SMTP, FTP). Incluye también el protocolo de los servidores DNS (Domain Name System). Utiliza **mensajes**.
- Capa de **Transporte**: transporta los mensajes entre los puntos terminales de la aplicación. Hay dos protocolos en Internet: TCP (orientado a la conexión, con un mecanismo de control de flujo y de congestión) y UDP (sin conexión, sin fiabilidad, control de flujo ni congestión). Los paquetes de esta capa se denominan **segmentos**.
- Capa de **Red**: traslada los paquetes de la capa de red (**datagramas**) de un host a otro. La capa de transporte le pasa un segmento y una dirección de destino. Consiste en el protocolo IP.
- Capa de **Enlace**: traslada los paquetes (**tramas**) de un nodo a otro, intercambiando los datagramas con la capa de red. Incluye los protocolos Ethernet, WiFi y PPP (Point-to-Point Protocol). El protocolo puede variar en cada enlace.
- Capa **Física**: mueve los bits individuales de una trama de un nodo a otro. El protocolo puede variar en cada enlace, dependiendo también del protocolo de la capa de enlace del nodo.

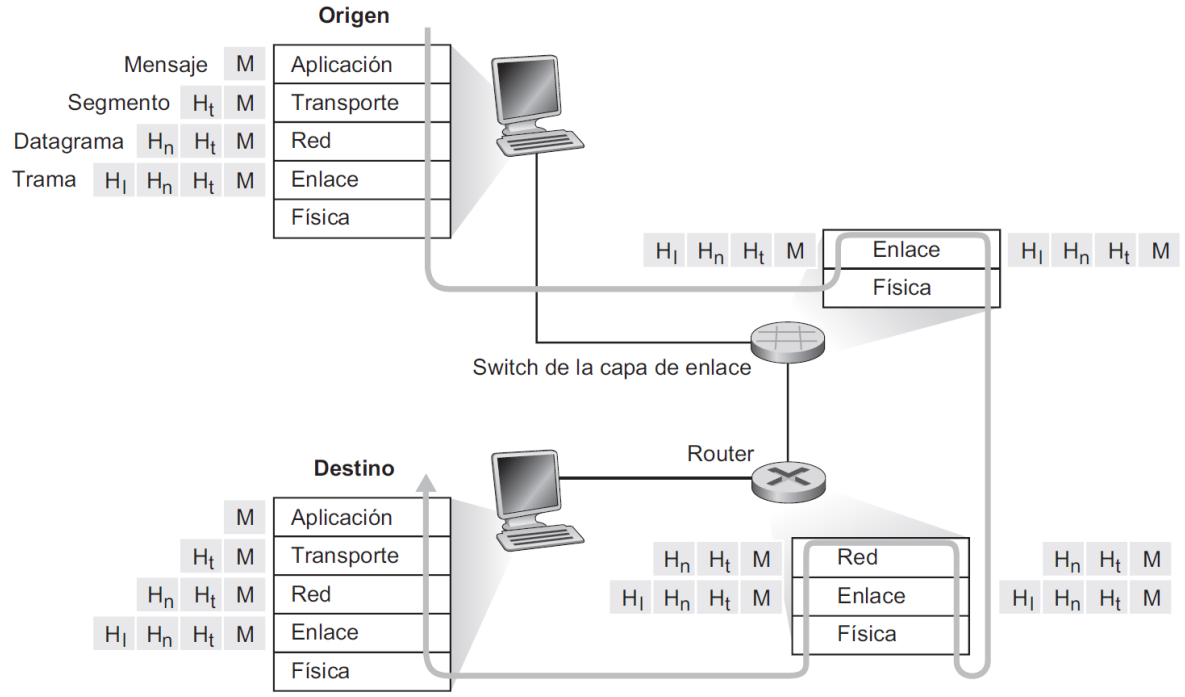


Figura 1.24 • Hosts, routers y switches de la capa de enlace. Cada uno de ellos contiene un conjunto distinto de capas, lo que refleja sus distintas funcionalidades.

Ataques a las redes

Inserción de software malicioso a través de internet

El software malicioso o malware infecta dispositivos con distintos propósitos, como eliminación de archivos, espionaje, o la formación de una botnet. Este software suele ser auto-replicante.

- Virus: requiere cierta interacción del usuario para infectar el dispositivo.
- Gusano: ingresan al dispositivo sin interacción explícita del usuario.
- Caballo de Troya: oculto dentro de otro software útil.

Ataques a servidores e infraestructura de red

Los ataques DoS (Denial-of-Service) vuelven inutilizable una red o host para los usuarios legítimos, ya sea a una vulnerabilidad (pocos mensajes bien construidos para provocar un fallo a una aplicación vulnerable), inundando el ancho de banda (saturando el enlace de acceso) o inundando de conexiones (estableciendo muchas conexiones TCP abiertas o semi-abiertas, impidiendo el establecimiento de conexiones legítimas). Se dice que un ataque DoS es distribuido (DDoS) cuando proviene de muchos orígenes; estos hacen más difícil la detección y la defensa.

Análisis de paquetes

Un packet sniffer es un receptor pasivo de paquetes que guarda una copia de los mismos, para que el atacante pueda buscar en ellos información confidencial. Las redes inalámbricas son especialmente vulnerables. Su detección es difícil (puesto que no envían paquetes), así que la mejor forma de combatirlos son las técnicas criptográficas.

Suplantación de identidades

La inyección de paquetes en Internet con dirección de origen falsa se llama **suplantación IP**. Para resolver esto, se utiliza un medio de autenticación en el punto terminal.

Ataques de interposición

Al tomar el control de un router o de un módulo software residente en una capa inferior de la pila de protocolos en un sistema terminal, un atacante puede modificar o eliminar paquetes, además de leerlos. Se dice que los ataques de interposición comprometen la integridad de los datos enviados.

Unidad 2 – Capa de Enlace – Subcapa de Control de Acceso al Medio

Los bits se entregan en el mismo orden en que fueron enviados.

Cuestiones de diseño

La capa de enlace tiene varias funciones específicas, entre ellas:

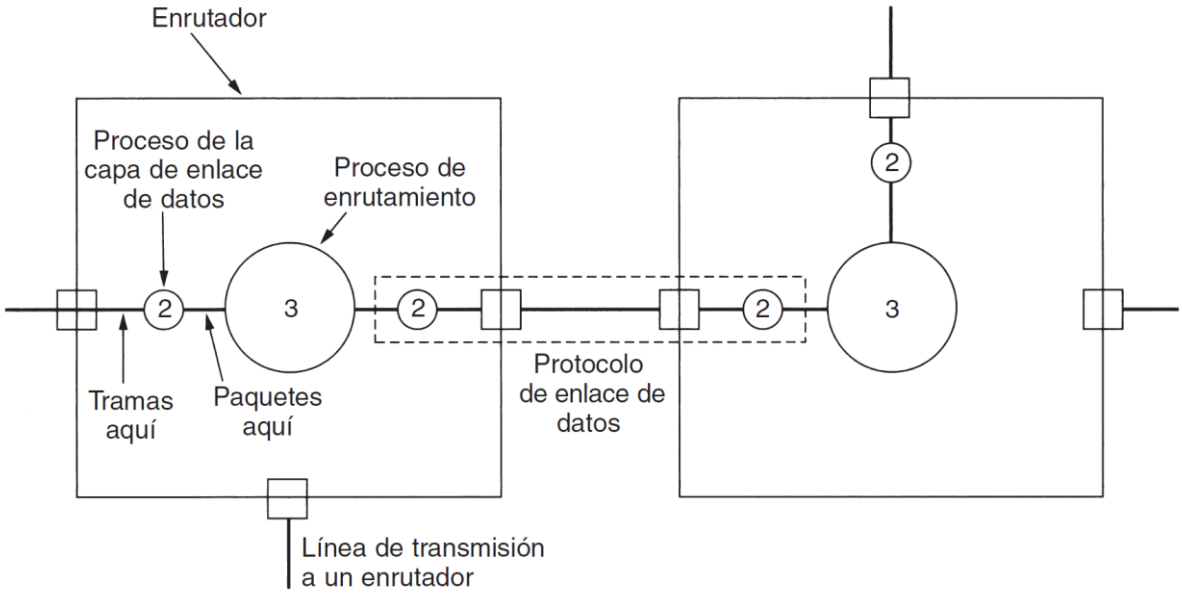
- Proporcionar una interfaz de servicio bien clara a la capa de red.
- Manejar los errores de transmisión.
- Regular el flujo de datos para evitar saturación de receptores lentos por emisores rápidos.

Se toma el datagrama de la capa de red y se lo encapsula en una trama. Las tramas tienen un encabezado, una carga útil (payload) (contiene al paquete) y un terminador.

El tamaño de las tramas se encuentra limitado por hardware, por lo que los datagramas pueden dividirse en múltiples tramas.

Servicios proporcionados a la capa de red

- No orientado a la conexión sin confirmación de recepción: apropiada cuando hay baja tasa de errores y para el tráfico en tiempo real (la llegada retrasada es peor que los errores).
- No orientado a la conexión con confirmación de recepción: si la confirmación no llega en un cierto tiempo, se reenvía la trama. Es más veloz aquí que en la capa de red, dado que en la capa de red, si se pierde una trama, se reenvía todo el datagrama.
- Orientado a la conexión con confirmación de recepción: consiste en tres fases: establecimiento de la conexión, transmisión de tramas y cierre de conexión.



Al llegar una trama a un enrutador, un proceso de la capa de enlace verifica que esté libre de errores y pasa el paquete al proceso de enrutamiento. Este proceso verifica que sea la trama esperada, elige la línea de salida adecuada y reenvía el paquete al software de la capa de enlace, para luego transmitirlo mediante un protocolo de enlace de datos.

Entramado

La capa de enlace debe detectar y corregir errores, lo cual logra mediante sumas de verificación aplicadas a cada trama. La mayor dificultad de esto es la división del flujo de bits en tramas. Los métodos para lograr el entramado son:

- Conteo de caracteres: introduciendo un carácter al inicio con el número de caracteres de la trama. De haber un error en el carácter inicial, el receptor no sabrá donde termina la trama.
- Banderas, con relleno de caracteres: colocando un carácter especial al inicio y al final de cada trama, y colocando otro carácter de escape antes de los caracteres que se asemejen a la bandera o al carácter de escape y se encuentren en el payload.
- Banderas, con relleno de bits: utilizando banderas al nivel de los bits, para evitar inconvenientes por caracteres de distinto tamaño.
- Violaciones de codificación de la capa física: en redes cuya codificación en el medio físico tiene cierta redundancia, se puede utilizar una combinación incorrecta como bandera.
- Conteo de caracteres junto a otro método.

Control de errores

Para garantizar que las tramas lleguen al destino en orden y sin repeticiones, se hace lo siguiente:

- Confirmaciones de recepción (positivas o negativas). Retransmisión si fuera negativa.
- Retransmisión tras expirar un temporizador sin confirmación de recepción.
- Números de secuencia de tramas para evitar duplicación en la capa de red.

Control de flujo

Para evitar la pérdida de datos porque el emisor envíe tramas más rápido que lo que el receptor puede procesar, se utiliza **control de flujo basado en retroalimentación**. Esto se basa en que el receptor autorice, explícita o implícitamente, al emisor a enviar n tramas.

Detección y Corrección de Errores

Los errores son inevitables, y su naturaleza depende del medio físico: pueden ser más comunes individualmente o en ráfagas.

Hay dos principales estrategias:

- Incluir suficiente redundancia para detectar errores, y solicitar la retransmisión. Para canales de alta confiabilidad.
- Incluir suficiente redundancia para corregir errores. Para canales de menor confiabilidad.

Distancia de Hamming: cantidad de bits en que difieren dos palabras. Se obtiene calculando XOR de dos palabras y contando la cantidad de bits 1. Indica cuántos errores de un bit se necesitan para convertir una palabra en la otra.

La distancia de Hamming de un código es la menor distancia de Hamming de las palabras válidas en el mismo.

Códigos de corrección

Se requiere un código de distancia de Hamming 2d + 1 para corregir d errores.

Un código de Hamming permite la corrección de hasta un error por palabra, utilizando múltiples bits de paridad. La palabra codificada se forma juntando estos bits de paridad con los bits de la palabra original, siendo los bits potencia de dos (1, 2, 4, etc.) los de paridad. Así, cada bit de paridad se genera considerando todos los bits de datos cuya posición requiere la suma de la posición del bit de paridad (con 4 bits de datos y 3 de paridad, el bit 1 se genera considerando los bits 3, 5 y 7; el 2 con 3, 6 y 7; y el 4 con 5, 6 y 7).

Al llegar al receptor, este analiza cada bit de paridad y, de haber un error, suma la posición del mismo a un contador. Al finalizar el análisis, el contador indica la posición del bit del error (pudiendo invertirlo para corregirlo).

Hay un truco para que pueda corregir errores en ráfaga: en lugar de transmitir k palabras codificadas secuencialmente, transmitir primero el primer bit de cada palabra, luego el segundo, y así sucesivamente. De este modo, si hubiera habido una ráfaga de hasta k errores, como mucho habrá afectado un bit de cada palabra, siendo corregible.

Códigos de detección

Se requiere un código de distancia de Hamming d + 1 para detectar d errores. Un método sencillo es agregar un bit de paridad por palabra, lo cual funciona para errores individuales pero hay posibilidad del 50% de falla con errores en ráfaga. Esto se puede mejorar al transmitir k palabras secuencialmente, detectando fallas de hasta k bits de largo.

El método más común es el **código polinomial** o **CRC** (código de redundancia cíclica). Para generarlo, tanto el emisor como el receptor deben estar de acuerdo en un polinomio G(x) (es decir, una secuencia de r+1 bits, siendo r el grado de G(x)).

Para generar un CRC, se siguen los siguientes pasos:

- Agregar r bits 0 al final de la trama (T(x))
- Dividir la trama con los r bits por G(x). Esto se hace tomando de a r+1 bits de la trama, y considerar:
    - Si el primer bit es 0, ignorarlo y tomar el siguiente bit de la trama
    - Si el primer bit es 1, aplicar la operación XOR a esta parte de la trama con G(x)
- Al finalizar con el análisis de todos los bits de la trama, se habrá obtenido un resto de r bits. El código CRC se obtiene haciendo un OR entre la trama y el resto (es decir, reemplazando los r bits 0 agregados al final por el resto).

La verificación del error simplemente consiste en dividir la trama recibida por G(x) y, si el resto fuera 0, no se detectaría ningún error.

El método CRC se basa en que la operación XOR funciona como una suma o resta bit a bit sin acarreo. La división se realiza con el método de restas sucesivas, y al sumar el resto (R(x)) de T(x)/G(x) a T(x), (T(x) + R(x))/G(x) = 0.

Los errores se expresan como la operación XOR entre G(x) y un polinomio E(x), donde cada bit 1 de E(x) corresponde a un error individual. Esto es así porque (T(x) + R(x) + E(x))/G(x) = (T(x) + R(x))/G(x) + E(x)/G(x) = 0 + E(x)/G(x) = E(x)/G(x).

La efectividad de este método consiste en disminuir la probabilidad de que E(x)/G(x) = 0, seleccionando un buen G(x) con ciertas propiedades. La IEEE 802 utiliza un G(x) particular, con propiedades como la detección de toda ráfaga de longitud de 32 bits o menor, o que afecte un número impar de bits.

El cálculo y comprobación de CRC puede realizarse con circuitos (hardware) muy sencillos.

Protocolos

Se hacen ciertas suposiciones: que en las capas física, de enlace y de red hay procesos independientes que se comunican mediante mensajes; que la máquina A desea mandar un flujo considerable de datos a la máquina B con un servicio confiable orientado a la conexión y que las máquinas no fallan (sus protocolos sí pueden fallar).

A la capa de enlace no le interesa el contenido del datagrama, simplemente forma la trama con:

- Información de control en el encabezado, con campos como:
    - kind: tipo de trama (datos, acknowledge, datos y acknowledge)
    - seq: número de secuencia de la trama
    - ack: número de secuencia de la trama recibida
- El datagrama en el payload
- Una suma de verificación en el terminador

Cuando solo hay comunicación en un sentido, se utiliza un protocolo simplex.

Considerando que el receptor no necesariamente será suficientemente rápido para recibir y procesar las tramas al mismo ritmo que el emisor las envía, se puede utilizar un protocolo simplex de parada y espera, con un canal semidúplex por el que el receptor siempre envíe una trama confirmando la recepción, no pudiendo el emisor enviar otra trama hasta recibir la confirmación de recepción.

Si hubiera ruido en el canal (y por ende, errores), se necesita modificar el protocolo anterior para que solo haya una confirmación si la trama se recibió correctamente, y agregar el campo seq (pudiendo ser un único bit).

Si hubiera transmisión en ambos sentidos, se puede tener dos canales separados simplex, uno en cada dirección. Sin embargo, esto implica un desperdicio del ancho de banda del canal de las confirmaciones de respuesta.

Es mejor opción utilizar un único canal dúplex, agregando más bits a seq y los campos kind y ack. El valor de kind dependerá de si se trata de una trama de datos o de confirmación de recepción; en el segundo caso, ack indicará el número seq de la trama recibida.

Una optimización al protocolo anterior es utilizar superposición (piggybacking), es decir, el receptor espera un cierto tiempo desde la recepción de una trama correcta, por si tuviera que enviar una trama de datos. Así, incorpora el kind de trama y confirmación, utilizando tanto el payload como ack.

Hay protocolos más avanzados, conocido como "de **ventana corrediza**". Estos se basan en el concepto de **ventana emisora** (grupo de números de secuencia de tramas que una máquina tiene permitido enviar) y **ventana receptora** (ídem, pero de las que puede aceptar). Según el protocolo, las ventanas pueden tener distintos límites superior e inferior, distintos tamaños y el mismo puede variar.

Si el tamaño máximo fuera de un bit, se utiliza un protocolo de parada y espera.

Para aprovechar el ancho de banda, se puede utilizar una ventana emisora grande, capaz de llenar el canal (es decir, del producto entre el ancho de banda y el retardo de ida y vuelta). A este proceso se le llama **canalización**. Para manejar errores, hay dos técnicas:

- Retroceso n: el receptor no envía confirmación de recepción cuando la trama recibida no es la próxima que espera (ventana receptora de tamaño 1). El emisor continúa enviando tramas hasta que expira el temporizador de la trama incorrecta, allí retrocede hasta la trama correspondiente y reenvía esa y las posteriores. Prioriza el espacio de buffers en la capa de enlace.
- Repetición selectiva: con una ventana receptora de mayor tamaño, el receptor confirma y almacena las tramas correctas posteriores a una incorrecta, haciendo que el emisor solo reenvíe la incorrecta. Esto se puede optimizar con el uso de confirmaciones negativas, para no tener que esperar a la expiración del temporizador en el emisor. Prioriza el ahorro en ancho de banda.

Verificación de los protocolos

Los protocolos son especificados y verificados mediante técnicas matemáticas formales:

- Máquina de estados finitos: analizando los estados posibles de las máquinas, las posibles transiciones y el estado inicial de las máquinas. Para determinar si un protocolo es correcto o no, se puede hacer un análisis de asequibilidad. También permite encontrar en los protocolos los bloqueos irreversibles.
- Modelo de red de Petri: mediante lugares, transiciones, arcos y tokens, permitiendo una representación tanto gráfica como algebraica de la red. Permite encontrar bloqueos irreversibles.

Ejemplos de Protocolos

HDLC: Control de Enlace de Datos de Alto Nivel

Se trata de una familia de protocolos orientados a bits (con relleno de bits).

Bits	8	8	8	≥0	16	8
	0 1 1 1 1 1 1 0	Dirección	Control	Datos	Suma de verificación	0 1 1 1 1 1 1 0

Figura 3-24. Formato de trama para protocolos orientados a bits.

Campos de la trama:

- Dirección: identifica la terminal destino.
- Control: seq, ack y otros propósitos.
- Datos
- Suma de verificación: CRC
- Banderas: 01111110. En las líneas punto a punto inactivas se transmiten banderas continuamente.

Hay tres tipos de tramas: de información, de supervisión y no numeradas.

Bits	1	3	1	3
(a)	0	Secuencia	P/F	Siguiente
(b)	1	0	Tipo	P/F	Siguiente
(c)	1	1	Tipo	P/F	Modificado

Figura 3-25. Campo de Control de (a) una trama de información, (b) una trama de supervisión y (c) una trama no numerada.

PPP: Protocolo Punto a Punto

Es utilizado por Internet para, principalmente, manejar el tráfico entre routers y entre usuarios domésticos e ISPs. Está definido en el RFC 1661 y se ha desarrollado más en otros.

Características:

- Método de entramado que delinea sin ambigüedades el final de una trama y el inicio de la siguiente, manejando la detección de errores.
- Protocolo de Control de Enlace (**LCP**) para activar líneas, probarlas, negociar opciones y desactivarlas. Admite circuitos síncronos y asíncronos, y codificaciones orientadas a bits y caracteres.
- Protocolo de Control de Red (**NCP**) (uno para cada protocolo de capa de red soportado) que permite negociar opciones de capa de red independientemente de su protocolo.

Bytes	1	1	1	1 o 2	Variable	2 o 4	1
	Bandera 01111110	Dirección 11111111	Control 00000011	Protocolo	Carga útil	Suma de verificación	Bandera 01111110

Figura 3-27. Formato de trama completa PPP para el modo de operación no numerado.

Fases simplificadas para activar y desactivar una línea con PPP:

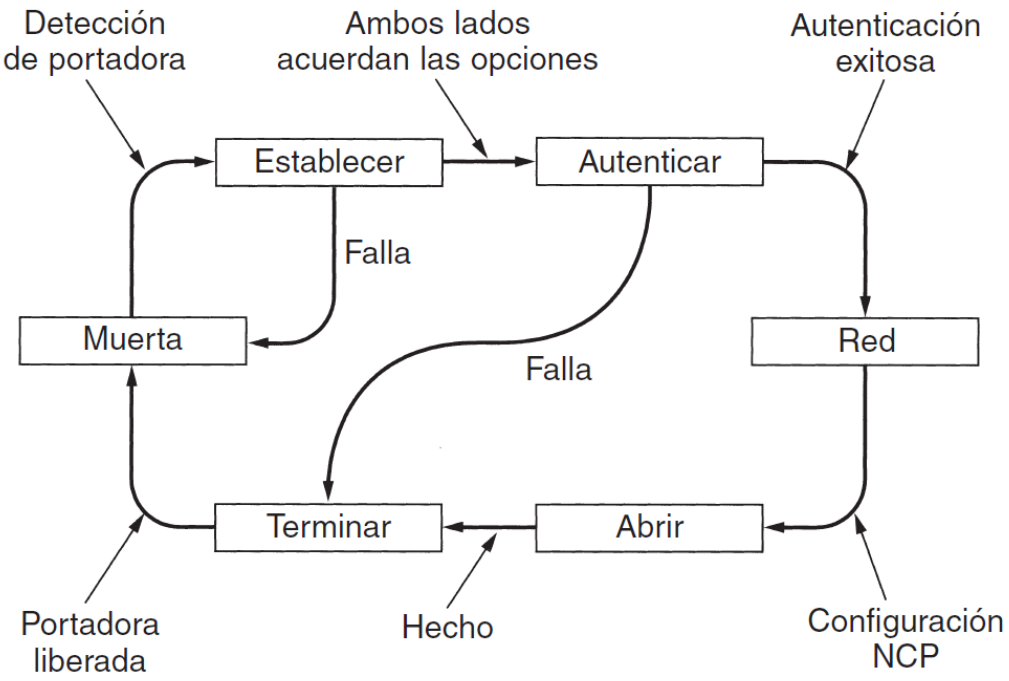


Figura 3-28. Diagrama de fases simplificado para activar y desactivar una línea.

LCP se utiliza entre “Establecer” y “Autenticar” para establecer las opciones del protocolo de enlace de datos. NCP se utiliza entre “Red” y “Abrir” para configurar la capa de red.

Problema de Asignación del Canal

Se le dice canal **multiacceso** o **de acceso aleatorio** a los canales de difusión, es decir, aquellos por donde muchos hosts se intentan comunicar en simultáneo.

Los protocolos usados para determinar quién sigue en un canal multiacceso pertenecen a la subcapa **MAC** (Control de Acceso al Medio), que se encuentra en la parte inferior de la capa de enlace.

Los métodos estáticos para asignar canales en LANs y MANs (FDM y TDM) tienen un gran desperdicio de ancho de banda, por lo que no son usados.

Los métodos dinámicos se basan en cierto supuestos:

- Modelo de estación: hay N estaciones independientes, cada una con un programa que genera tramas para su transmisión
- Canal único

- Colisión: cuando dos tramas se transmiten en forma simultánea, y se alteran. Todas las estaciones pueden detectarlas. Las tramas en colisión deben ser retransmitidas.
- Tiempo continuo / ranurado: la transmisión de una trama puede comenzar en cualquier momento / al inicio de una ranura (pudiendo haber ranuras inactivas de 0 tramas, transmisiones con éxito de 1 trama o colisiones de más de 1 trama.
- Detección de portadora / No detección de portadora: las estaciones pueden saber o no si el canal está en uso antes de transmitir.

Protocolos de acceso múltiple

ALOHA puro

Cada host transmite cuando lo requiere, y escucha el medio físico por si hubiera colisiones. Si las hubiera, retransmite la trama. Se optimiza el funcionamiento al usar tramas de tamaño fijo.

Como resultado de un análisis estadístico de Poisson, se concluye que el mayor rendimiento esperable (velocidad real de transporte por tiempo de trama, es decir, éxitos) es del 18%, con 0,5 intentos de retransmisión media por tiempo de trama.

ALOHA ranurado

Duplica la eficiencia de ALOHA puro (37% de velocidad real de transporte). Requiere que los hosts acuerden límites de ranura, sincronizándose. Los hosts, así, solo pueden transmitir al inicio de las ranuras.

CSMA persistente y no persistente

CSMA (Acceso Múltiple con Detección de Portadora) **persistente-1** consiste en que, cuando tiene datos a transmitir, la estación primero escucha el canal. Si estuviera ocupado, espera a que el mismo se desocupe antes de transmitir. Si detectara una colisión, espera un tiempo aleatorio antes de retransmitir. Se llama persistente-1 porque la estación transmite con probabilidad 1 cuando encuentra que el canal está inactivo.

El retardo de propagación afecta al rendimiento del protocolo, pues mientras más grande sea, aumentan las probabilidades de colisiones.

CSMA no persistente no continúa escuchando continuamente el canal, cuando el mismo está ocupado, en espera de que se desocupe; en cambio, espera un tiempo aleatorio y vuelve a escucharlo, hasta que se desocupe. En consecuencia, este algoritmo lleva a un mejor uso del canal pero mayores retardos que con CSMA persistente-1

CSMA persistente-p es una generalización de persistente-1, utilizando ranuras. En estos protocolos, se establece que p es la probabilidad de que, al detectar una ranura vacía, se transmita. Si se decidiera no transmitir, se espera a la siguiente ranura y se repite el proceso, hasta que se transmita o se ocupe el canal (en este último caso, se lo sigue escuchando hasta que se encuentre vacío).

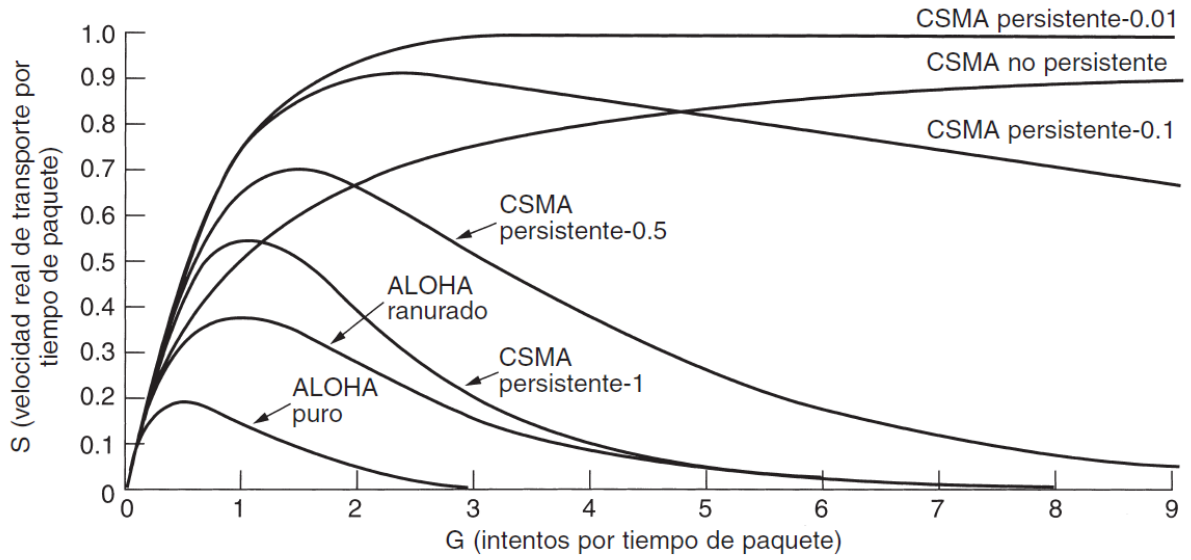


Figura 4-4. Comparación de la utilización del canal contra la carga para varios protocolos de acceso aleatorio.

CSMA/CD

CSMA con detección de colisiones difiere en que, al detectar una colisión, los hosts dejan de transmitir, ahorrando tiempo y ancho de banda.

La detección de colisiones es un proceso analógico que consiste en comparar lo que se debería estar transmitiendo con lo que realmente se está transmitiendo. Implica una demora: si una señal tarda un tiempo τ en propagarse de una estación a otra, en el caso más extremo, una estación tardará 2τ en detectar la colisión desde que comenzó a transmitir.

Las colisiones no ocurren una vez que una estación tomó el canal, pero sí ocurren en los periodos de contención (donde más de una estación quiere transmitir). Los problemas de colisiones empeoran con τ grandes y tramas cortas.

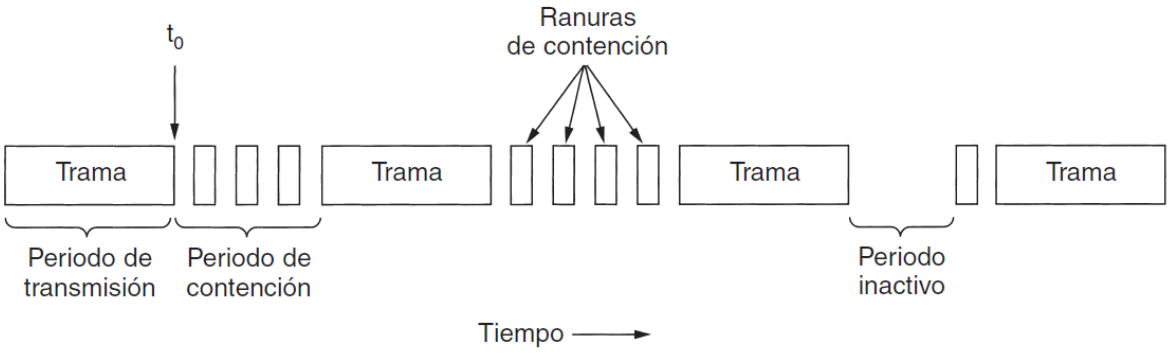


Figura 4-5. El CSMA/CD puede estar en uno de tres estados: contención, transmisión o inactivo.

Protocolo de mapa de bits

Si hay N estaciones, cada una con un identificador número en su hardware, se dividen los periodos de contención en N ranuras de 1 bit, pudiendo cada estación transmitir un 1 solo en su ranura, para indicar que tiene una trama a transmitir. Así, al terminar el periodo de contención, todas las estaciones sabrán quiénes van a transmitir y en qué orden, así como cuándo comienza el próximo periodo de contención. Con este protocolo se evitan las colisiones.

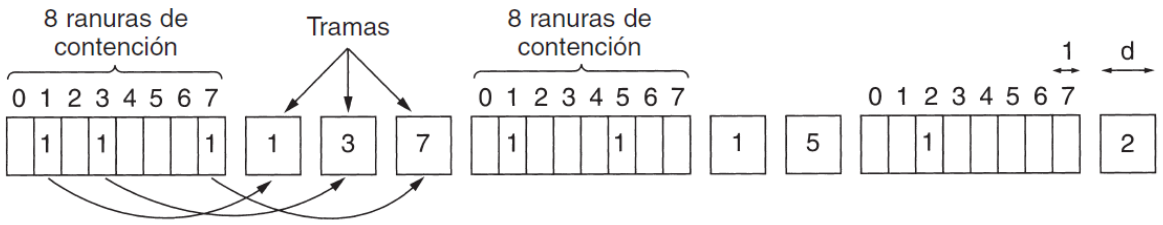


Figura 4-6. Protocolo básico de mapa de bits.

Se dice que este es un **protocolo de reservación**.

Conteo descendente binario

Cada estación tiene una dirección binaria, y mediante operaciones OR se determina cuál es el mayor entre todas las estaciones que desean transmitir, permitiéndole a esta ocupar el canal.

Una variación consiste en el uso de direcciones virtuales, cambiándolas para dar mayor prioridad a las estaciones que llevan mucho tiempo sin poder transmitir.

Protocolos de contención limitada

Se divide el canal en ranuras, asignando grupos de estaciones de tamaño variable a ciertas ranuras de forma dinámica, según la carga de la red. Al haber carga baja, se desea muchas estaciones por ranura (similar a ALOHA); y al haber carga alta, pocas estaciones por ranura (similar a conteo descendente binario).

Protocolo de recorrido de árbol adaptable

Habiendo N estaciones, se arma un árbol binario de $\log_2 N$ niveles, siendo hojas las estaciones. Así, al finalizar una trama, se toma la raíz y transmite a todas las estaciones. De haber una colisión, se toma el primer nodo bajo la raíz y transmiten todas las estaciones bajo ese nodo. Mientras siga habiendo colisiones, se seguirá recorriendo el árbol hacia abajo, hasta que no haya más colisiones. La próxima trama se reserva para el segundo nodo al que pudo transmitir.

Hay mejoras posibles, como evitar verificar los primeros niveles cuando hay carga alta (por la alta probabilidad de colisión), o evitar probar el segundo nodo cuando en el primero no estaba inactivo (está garantizado que habrá colisión en el segundo).

Protocolos de acceso múltiple por división de longitud de onda (WDMA)

Utilizando fibra óptica, se puede dividir el canal en múltiples canales con diferentes longitudes de onda, asignándolos a las estaciones (1 angosto de control y otro ancho de envío datos para cada estación).

Las estaciones tienen un receptor de onda fija para su canal de control, utilizado por las otras estaciones para señalizar que configure su receptor sintonizable a su canal de envío de datos. También tienen un emisor sintonizable para canales de control, para indicar a otras estaciones que va a enviar datos con su emisor de onda fija (así los reciben).

En otras palabras, el canal de control se utiliza para que una estación indique a otra que va a transmitirle, para que la receptora se prepare. Sin embargo, las estaciones no pueden transmitir en cualquier ranura: tienen que esperar a ver la información transmitida periódicamente en una ranura de estado en el canal de datos del receptor, para así saber qué ranuras están disponibles en sus dos canales.

El protocolo indica en detalle cómo proceder con tres tipos de comunicación: orientada a la conexión con tasa constante, orientada a la conexión con tasa variable y no orientada a la conexión (con datagramas).

Protocolos de LANs inalámbricas

Problemas con CSMA

- Estación oculta: dos estaciones que no se pueden detectar entre sí transmiten a una misma receptora. Hay colisión.
- Estación expuesta: una estación intenta transmitir a una estación receptora, pero detecta que otra estación está realizando una transmisión a otra. Se evita una colisión que no ocurriría.

MACA (Acceso Múltiple con Detección de Colisiones) y MACAW (MACA Inalámbrico)

Una estación emisora, antes de transmitir, envía una trama RTS (Request to Send) a la receptora, avisándole que le transmitirá y el tamaño de la trama. La receptora, en respuesta, envía una trama CTS (Clear to Send), y la emisora comienza a transmitir apenas la recibe.

Ninguna de las estaciones cercanas a la emisora o receptora transmitirán, puesto que sabrán que el canal está ocupado por haber recibido RTS y/o CTS.

MACAW incorpora una trama ACK detrás de cada trama de datos exitosa, así como detección de portadora para el RTS. También se introdujeron mecanismos para mejorar la equidad y evitar congestionamientos.

Ethernet

Es casi idéntico al protocolo IEEE 802.3.

Los tipos más comunes de cableado Ethernet son 10Base2, 10Base-T y 10Base-F. Todas operan a 10 Mbps en banda base.

Nombre	Cable	Seg. máx.	Nodos/seg	Ventajas
10Base5	Coaxial grueso	500 m	100	Cable original; ahora obsoleto
10Base2	Coaxial delgado	185 m	30	No se necesita concentrador
10Base-T	Par trenzado	100 m	1024	Sistema más económico
10Base-F	Fibra óptica	2000 m	1024	Mejor entre edificios

Figura 4-13. Los tipos más comunes de cableado Ethernet.

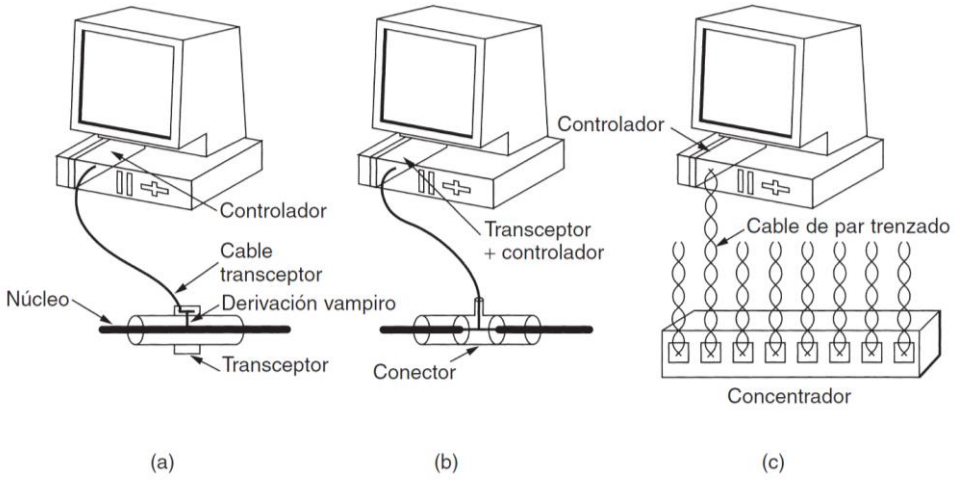


Figura 4-14. Tres tipos de cableado Ethernet. (a) 10Base5. (b) 10Base2. (c) 10Base-T.

Las siguientes son las topologías más comunes para cablear un edificio:

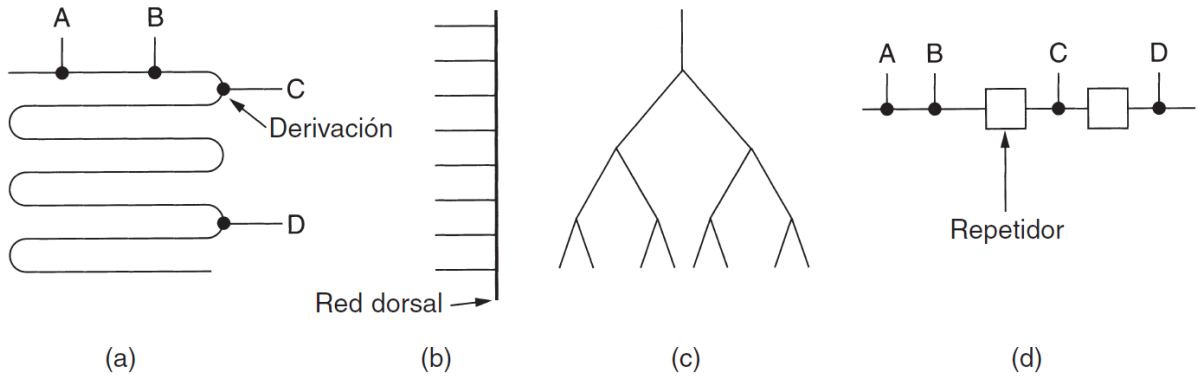


Figura 4-15. Topologías de cableado. (a) Lineal. (b) Columna vertebral. (c) Árbol. (d) Segmentada.

Ethernet utiliza codificación Manchester con voltaje superior de 0,85V e inferior de -0,85V, donde un voltaje disminuyente indica un 1 y uno que aumenta indica un 0. Requiere el doble de ancho de banca que la codificación binaria, pero elimina la inconsistencia por desincronización. Es menos inmune al ruido que Manchester Diferencial, pero el equipamiento para implementarlo es más sencillo.

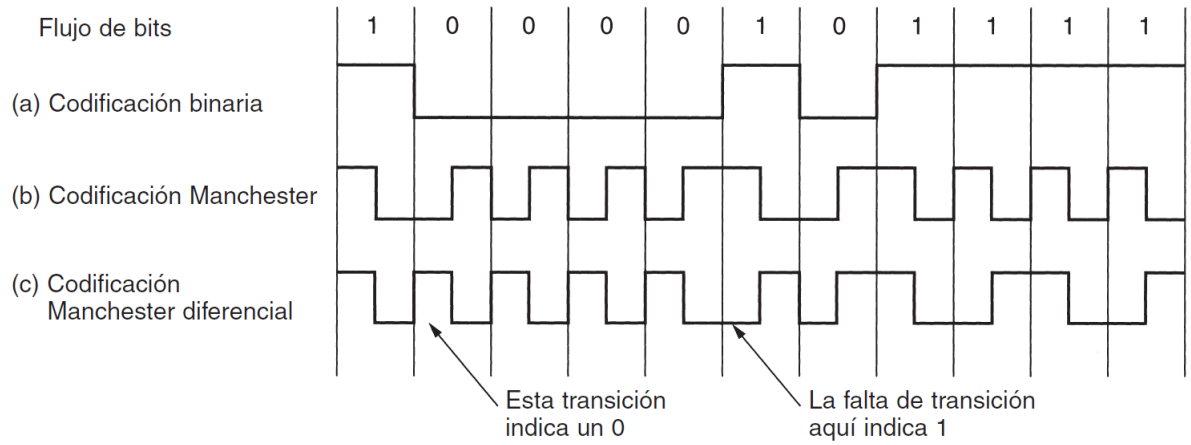


Figura 4-16. (a) Codificación binaria. (b) Codificación Manchester. (c) Codificación Manchester diferencial.

Protocolo de subcapa MAC de Ethernet

Originalmente, se planteó Ethernet DIX con una trama específica, luego modificada por la IEEE 802.3.

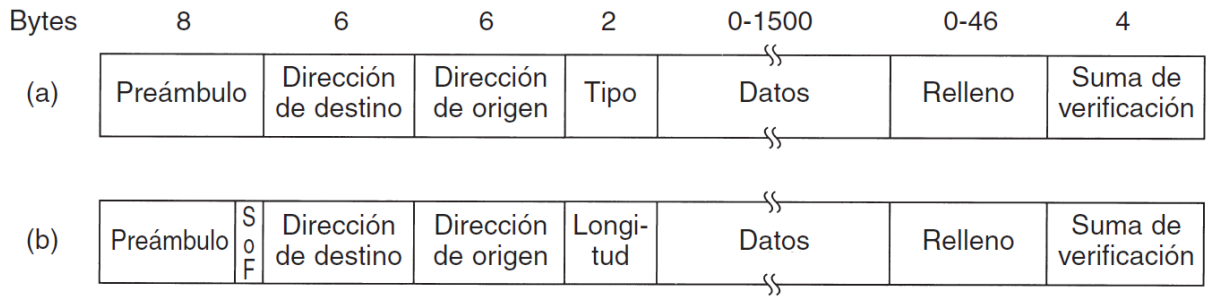


Figura 4-17. Formatos de trama. (a) Ethernet DIX. (b) IEEE 802.3.

El preámbulo sirve para que emisor y receptor se sincronicen, con sus 8 bytes consistiendo en la secuencia 10101010. IEEE modificó el último byte de para que sirva como delimitador de trama, por compatibilidad con 802.4 y 802.5.

Las direcciones de destino y origen pueden ser de 2 u 6 bytes, pero para el estándar de banda base de 10 Mbps solo se usan direcciones de 6 bytes. El bit de orden mayor de la dirección de destino indica 0 para direcciones ordinarias y 1 para direcciones de grupo (multidifusión / multicast). La dirección que consiste en solamente 1s está reservada para difusión (broadcast) a todas las estaciones. El bit 46 (adyacente al de orden mayor) se utiliza para distinguir direccionamiento local de global.

En DIX, se usa el campo de tipo para indicarle a la capa de enlace del receptor a qué protocolo de la capa de red debe entregarle la trama. En cambio, en IEEE 802.3 esta información se coloca dentro de un encabezado en el campo de datos, colocándose un campo con la longitud de la trama en lugar del campo de tipo de DIX.

El campo de datos puede ser de entre 0 y 1500 bytes. El límite superior se eligió para ahorrar RAM (la cuál era más cara cuándo surgió Ethernet).

Se requiere que las tramas tengan un límite inferior para distinguir las tramas válidas de las truncadas por colisiones, y para que el emisor se entere de que hubo una colisión antes de haber terminado de transmitir. El límite inferior se estableció en 64 bytes, utilizándose el campo de relleno cuando el de datos no tiene el tamaño suficiente.

Se utiliza CRC de 32 bits como suma de verificación.

Retroceso exponencial binario

Se define como tiempo de ranura al tiempo de propagación de ida y vuelta en el peor caso en un cable.

Al detectar una colisión, cada emisora espera aleatoriamente entre 0 y $2^1 - 1$ tiempos de ranura. Si colisionara de nuevo, esperan entre 0 y $2^2 - 1$. En general, esperan entre 0 y $2^i - 1$ tiempos de ranura, siendo $i$el número de colisiones. El máximo es $i = 10$, es decir, entre 0 y 1023.

Esto permite evitar los casos extremos: muchas emisoras esperando entre 0 y 1 tiempos de ranura provocarían muchas colisiones, pero pocas emisoras esperando entre 0 y 1023 tiempos de ranura harían perder tiempo innecesariamente.

Tras 16 colisiones, el controlador deja de intentar el envío e informa del fracaso al emisor.

Ethernet conmutada

Mediante el uso de conmutadores (switches), se puede mejorar el desempeño de una red Ethernet:

- Con un tipo de tarjeta de conexión que funcione como red LAN dentro de sí, esta misma detecta las colisiones y permite formar su propio dominio de colisión. De haber una tarjeta por estación, las colisiones son imposibles y mejora el desempeño.
- Con el otro tipo de tarjeta de conexión, cada puerto tiene un búfer dentro de la tarjeta en donde almacena las tramas de entrada, y permite dar a cada puerto su propio dominio de colisión.

Fast Ethernet

Establecido en el protocolo 802.3u, Fast Ethernet se basa en 10Base-T, brindando las siguientes posibilidades para el cableado y buscando brindar compatibilidad hacia atrás:

Nombre	Cable	Segmento máximo	Ventajas
100Base-T4	Par trenzado	100 m	Utiliza UTP categoría 3
100Base-TX	Par trenzado	100 m	Dúplex total a 100 Mbps (UTP cat 5)
100Base-FX	Fibra óptica	2000 m	Dúplex total a 100 Mbps; distancias largas

Figura 4-21. El cableado original de Fast Ethernet.

100Base-T4 implica no usar codificación Manchester, para mejorar el ancho de banda; y el uso de señales ternarias en lugar de binarias (8B/6T).

Con 100Base-TX, se utiliza un esquema llamado 4B/5B en lugar de codificación binaria directa. Junto a 100Base-T4, forman los 100Base-T.

100Base-FX utiliza fibra multimodo.

Posteriormente se agregó el esquema de cableado 100Base-T2, que funciona con dos pares de cables UTP categoría 3.

Los 100Base-T posibilitan el uso de dos dispositivos de interconexión:

- Concentrador (hub): todas las líneas se conectan lógicamente, formando un único dominio de colisión. Usan comunicación semidúplex.
- Conmutador (switch): cada trama entrante se almacena en un búfer de una tarjeta de conexión y se pasa a través de una matriz de conmutación hacia un búfer de la tarjeta de destino. Solo se pueden usar conmutadores con 100Base-FX.

Gigabit Ethernet

Establecido en el protocolo 802.3z, Gigabit Ethernet ofrece dos posibles configuraciones: dúplex, con conmutadores; y semidúplex, con concentradores y usando CSMA/CD.

El radio del modo semidúplex sería de solo 25 m, por lo que se agregó dos métodos para aumentar el alcance:

- Extensión de portadora: agregar relleno al final de cada trama mediante hardware para llegar a 512 bytes.
- Ráfagas de trama: emitir una secuencia concatenada de tramas, rellenando por hardware solo cuando estas ráfagas no lleguen a 512 bytes.

El cableado puede hacerse de las siguientes formas:

Nombre	Cable	Segmento máximo	Ventajas
1000Base-SX	Fibra óptica	550 m	Fibra multimodo (50, 62.5 micras)
1000Base-LX	Fibra óptica	5000 m	Sencilla (10 μ) o multimodo (50, 62.5 μ)
1000Base-CX	2 pares de STP	25 m	Cable de par trenzado blindado
1000Base-T	4 Pares de UTP	100 m	UTP categoría 5 estándar

Figura 4-23. Cableado de Gigabit Ethernet.

En fibra óptica, en lugar de código Manchester, se utiliza un esquema llamado 8B/10B.

Control Lógico del Enlace (LLC) (IEEE 802.2)

Por sobre la subcapa MAC (dentro de la misma capa de enlace) se ubica la capa LLC, que agrega a los datagramas un encabezado con el número de secuencia y confirmación de recepción, colocando esto en el payload de una trama 802.

El encabezado LLC contiene tres campos: punto de acceso de destino, de origen y el campo de control. Los puntos de acceso indican de qué proceso viene la trama y a cuál va (reemplaza al campo tipo DIX). El campo de control contiene SEQ y ACK.

LANs Inalámbricas (IEEE 802.11)

Capa física

El protocolo 802.11 admite 6 técnicas de transmisión en la capa física:

- Infrarrojos: transmisión difusa a 0,85 o 0,95 micras, con velocidades de 1 Mbps o 2 Mbps. Utiliza código de Gray, codificando palabras de 4 bits en 16, o de 2 en 4 bits, respectivamente. No atraviesa paredes y es afectado por la luz solar.
- FHSS (Espectro Disperso con Salto de Frecuencia): utiliza 79 canales, cada uno con 1MHz de ancho de banda, empezando en el extremo inferior de la banda ISM de 2,4 GHz. Aleatoriamente, las estaciones van sintonizando de forma sincrónica los canales (pues utilizan la misma semilla). Utilizan un tiempo de permanencia ajustable, pero menor a 400 ms.
- DSSS (Espectro Disperso de Secuencia Directa): utiliza modulación por desplazamiento de fase a 1 Mbaudio y transmite 1 o 2 bits por baudio, según si usa velocidad 1 Mbps o 2Mbps.
- OFDM (Multiplexión por División de Frecuencias Ortogonales): establecido en 802.11a, permite enviar hasta 54Mbps en la banda ISM ancha de 5 GHz. Se utilizan 48 frecuencias para datos y 4 para sincronización. Utiliza modulación por desplazamiento de fase para velocidades de hasta 18 Mbps, y QAM para velocidades mayores.
- HR-DSSS (DSSS de Alta Velocidad): establecido en 802.11b, alcanza 11 Mbps en la banda de 2,4 GHz. Soporta 1, 2, 5,5 y 6 Mbps. Es más lento que 802.11a, pero su rango es 7 veces mayor.
- OFDM (802.11g): opera en la banda 2,4 GHz, y puede operar a hasta 54 Mbps en teoría.

Protocolo de la subcapa MAC

Para solucionar los problemas de la estación oculta y la estación expuesta, IEEE 802.11 ofrece dos modos de funcionamiento: DCF y PCF.

DCF (Función de Coordinación Distribuida) utiliza CSMA/CA (CSMA con Evitación de Colisiones) tanto para detección del canal físico como del virtual. CSMA/CA tiene dos modos de operación: uno detectando el canal con retroceso exponencial binario, y otro basado en MACAW con un temporizador de ACK en el emisor y señales internas NAV (Vector de Asignación de Red) en estaciones cercanas para evitar transmisiones hasta el ACK.

Debido al gran ruido, se suele dividir las tramas en fragmentos, cada uno con su propia suma de verificación, transmitiéndolos en ráfaga con un protocolo de parada y espera.

PCF (Función de Coordinación Puntual) establece que la estación base sondea las demás estaciones, difundiendo una trama de beacon de manera periódica con parámetros de

sistema, sincronización de reloj, etc. Una estación puede inscribirse al servicio de sondeo a cierta tasa, obteniendo una garantía de cierto ancho de banda y calidad del servicio.

DCF y PCF pueden coexistir en una celda, lo cual se logra definiendo cuatro intervalos de tiempo específicos:

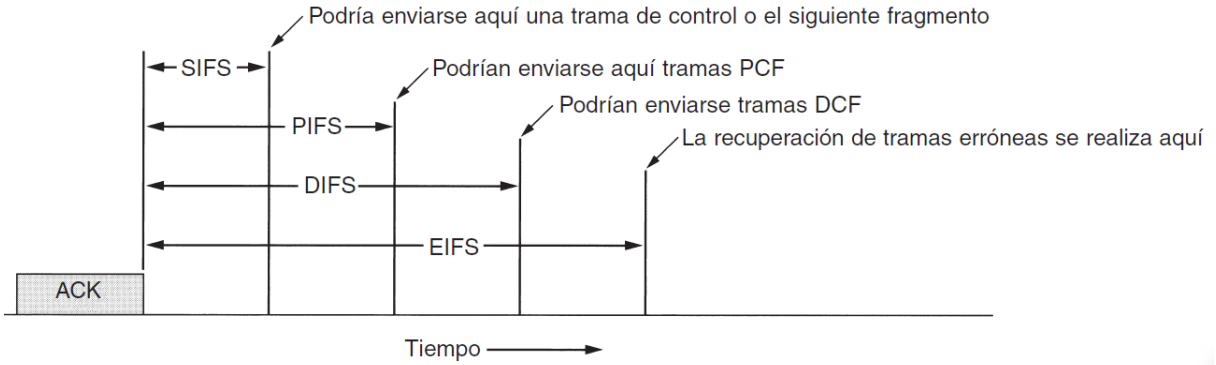


Figura 4-29. Espaciado entre tramas 802.11.

- SIFS (Espaciado Corto Entre Tramas): para que las distintas partes de un diálogo transmitan primero (RTS, CTS, ACK, fragmento de trama).
- PIFS (Espaciado Entre Tramas PCF): para envío de tramas de datos PCF o, en su defecto, tramas de beacon.
- DIFS (Espaciado Entre Tramas DCF): para envío de tramas de datos DCF.
- EIFS (Espaciado Entre Tramas Extendido): usado para reporte de tramas erróneas

Trama 802.11

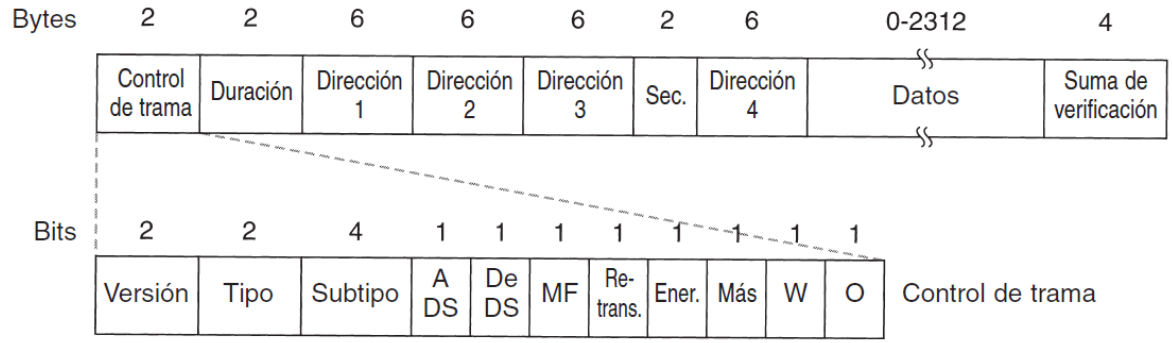


Figura 4-30. La trama de datos 802.11.

- Control de trama
  - Versión: permite que dos versiones del protocolo funcionen al mismo tiempo en la celda.
  - Tipo (datos, control o administración) y subtipo (RTC, CTS, ACK...).
  - A DS, De DS: la trama va hacia o viene desde el sistema de distribución de celdas.
  - MF: siguen más fragmentos.
  - Retransmisión: la trama es una retransmisión de otra enviada anteriormente.
  - Energía: pone al receptor en estado de hibernación o lo saca de ese estado.
  - Más: siguen más tramas.
  - W: se codificó el cuerpo con algoritmo WEP (Privacidad Inalámbrica Equivalente).
  - O: procesar tramas en orden estricto.
- Duración: tiempo a ocupar la trama y su ACK el canal. Usado para NAV.
- Dirección 1-4: para el origen, destino, estación base origen y estación base destino.

- Secuencia: 12 bits para la trama y 4 para el fragmento.
- Datos
- Suma de Verificación

Servicios

De distribución

Están relacionados a la administración de membresías dentro de la celda, y con la interacción con estaciones fuera de la celda. Son proporcionados por las estaciones base.

- Asociación: utilizado por las estaciones móviles para conectarse a las estaciones base. La estación móvil anuncia su identidad y sus capacidades.
- Disociación: romper la relación.
- Reasociación: cambiar de estación base.
- Distribución: determina cómo enrutar las tramas enviadas a la estación base: por aire si el destino es local, y por red cableada en caso contraria.
- Integración: traducción del formato de trama 802.11 al requerido por una red no 802.11.

De estación

Están relacionados con la actividad dentro de una sola celda.

- Autenticación: tras asociar una estación, la estación base le manda una trama de desafío, la cual es codificada usando una clave secreta por la estación, y devuelta. Recién ahí y si la clave es correcta, la estación se vuelve miembro de la celda.
- Desautenticación: para posiblemente abandonar la red.
- Privacidad: para mayor seguridad, se codifica y decodifica con el algoritmo RC4.
- Entrega de datos: transmitir y recibir datos. No hay confiabilidad.

Banda Ancha Inalámbrica (IEEE 802.16)

A diferencia de 802.11, busca conectar edificios, los cuales no son móviles y tienen muchas computadoras. Se utiliza dúplex total. Funciona a distancias de varios kilómetros. Funciona en el rango de 10 a 66 GHz, por lo que requiere un buen control de errores (al ser más susceptible al ruido por el agua). Soporta el tráfico en tiempo real.

Capas

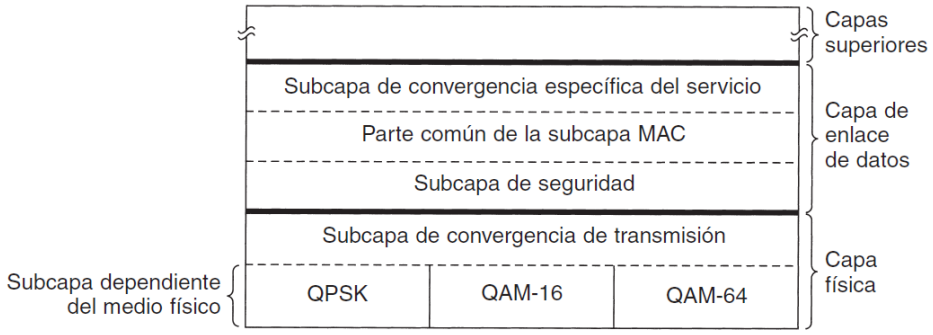


Figura 4-31. La pila de protocolos del 802.16.

Al usarse ondas milimétricas, las mismas pueden viajar en línea recta, por lo que la estación base puede tener múltiples antenas, una por sector y manteniendo una independencia entre los mismos.

En la capa física, ya que la fuerza de la señal y la relación señal a ruido descienden con la distancia a la estación base, se emplean tres esquemas de modulación diferentes: QAM-64 (6 bits/baudio) para suscriptores cercanos, QAM-16 (4 bits/baudio) para suscriptores a distancias medias, y QPSK (2 bits/baudio) para suscriptores distantes. Mientras más lejos esté el suscriptor, menor será la tasa de datos.

Se utiliza FDD y/o TDD para dividir las tramas ascendentes y descendentes, considerando que las primeras son menos comunes en el uso de internet.

802.16 tiene capacidad para empaquetar múltiples tramas MAC consecutivas en una sola transmisión física, para reducir los preámbulos y encabezados.

También se utilizan códigos de Hamming para la corrección de errores en la capa física.

Se usa una subcapa de seguridad para codificar los datos y asegurarse de que se mantengan en secreto.

La subcapa MAC establece que el canal descendente es administrado de forma directa por la estación base, pero el ascendente es usado por múltiples suscriptores compitiendo por él. Estos suscriptores pueden optar por distintos servicios:

- De tasa de bits constante: se dedican ciertas ranuras de tiempo a cada conexión de este tipo.
- De tasa de bits variable en tiempo real: es ajustada por la estación base sondeando al suscriptor a un intervalo fijo para saber el ancho de banda requerido.
- De tasa de bits variable en tiempo no real: es ajustada por la estación base sondeando frecuentemente al suscriptor a un intervalo fijo para saber el ancho de banda requerido. Un suscriptor de tasa de bits constante solicita enviar tráfico adicional (tasa de bits variable).
- De mejor esfuerzo: sin sondeo, los suscriptores de este tipo deben competir entre sí. Se usa retroceso exponencial binario.

Se puede asignar ancho de banda por estación o por conexión.

Trama 802.16

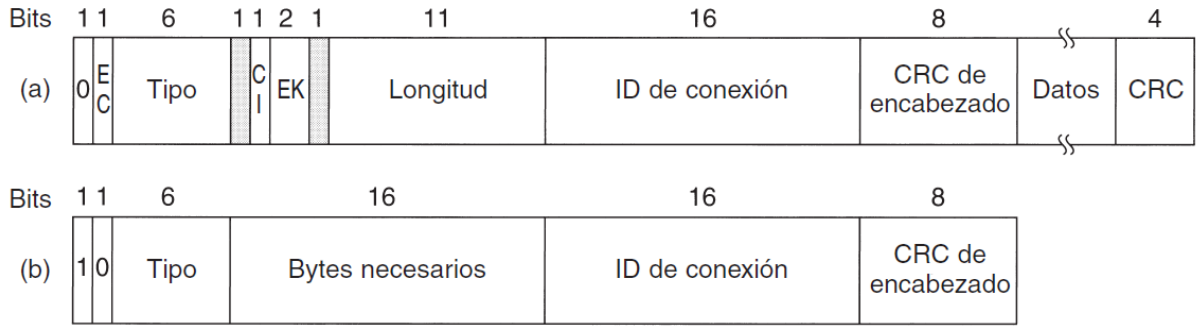


Figura 4-34. (a) Una trama genérica. (b) Una trama de solicitud de ancho de banda.

- EC: indica si la carga útil está encriptada.
- Tipo: indica el tipo de la trama, si hay empaquetamiento y fragmentación.
- CI: indica si hay una suma de verificación final.
- EK: indica cuál de las claves de encriptación se está usando (si se está usando alguna).
- Longitud: de la trama.
- ID de conexión: indica a cuál conexión pertenece la trama.

- CRC de encabezado: con polinomio 10111.
- Bytes necesarios: cantidad de ancho de banda necesaria para transmitir el número de bytes especificados.

Bluetooth

Fue creado un estándar que cubre todas las capas de la red por un SIG (Special Interest Group) formado por algunas empresas. El IEEE estandarizó una estructura muy similar de las capas física y de enlace.

La unidad básica de Bluetooth es una piconet, formada por un nodo y hasta 7 esclavos a hasta 10 m. Se pueden conectar entre sí varias piconets, mediante esclavos puente, formando así una scatternet. Además, puede haber hasta 255 nodos estacionados (en modo de bajo consumo de energía), que solo pueden responder a una señal de activación del nodo maestro.

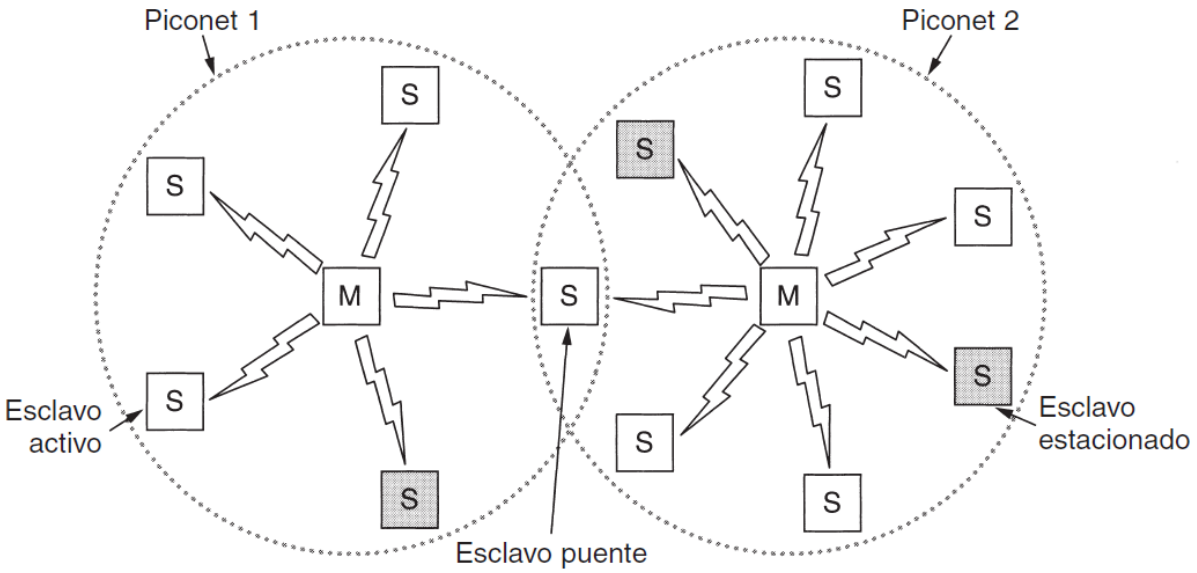


Figura 4-35. Dos piconets se pueden conectar para conformar una scatternet.

Perfiles

Bluetooth V1.1 especifica el soporte para 13 aplicaciones o perfiles:

Nombre	Descripción
Acceso genérico	Procedimientos para el manejo de enlaces
Descubrimiento de servicios	Protocolo para descubrir los servicios que se ofrecen
Puerto serie	Reemplazo para un cable de puerto serie
Intercambio genérico de objetos	Define la relación cliente-servidor para el traslado de objetos
Acceso a LAN	Protocolo entre una computadora móvil y una LAN fija
Acceso telefónico a redes	Permite que una computadora portátil realice una llamada por medio de un teléfono móvil
Fax	Permite que un fax móvil se comunique con un teléfono móvil
Telefonía inalámbrica	Conecta un handset (teléfono) con su estación base local
Intercom (Intercomunicador)	Walkie-talkie digital
Headset (Diadema telefónica)	Posibilita la comunicación de voz sin utilizar las manos
Envío de objetos	Ofrece una manera de intercambiar objetos simples
Transferencia de archivos	Proporciona una característica para transferencia de archivos más general
Sincronización	Permite a un PDA sincronizarse con otra computadora

Figura 4-36. Los perfiles de Bluetooth.

Capas

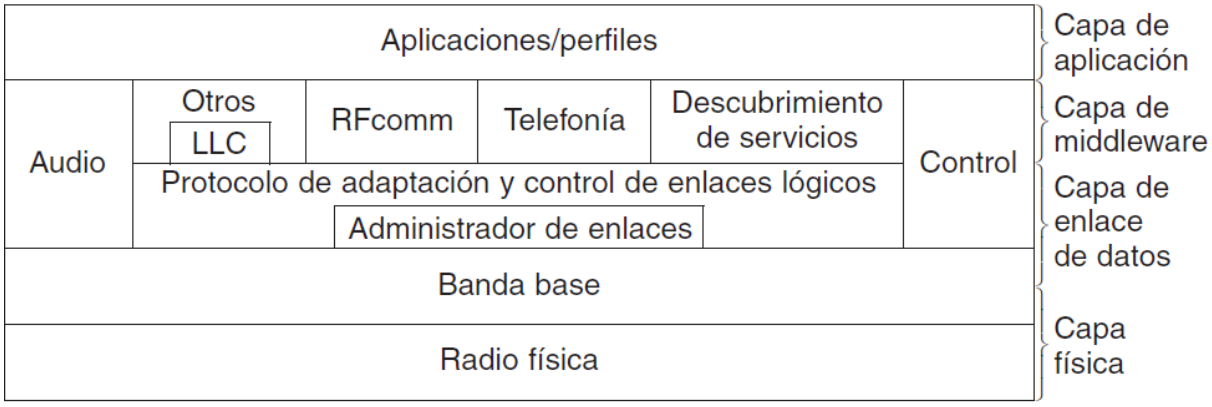


Figura 4-37. Versión 802.15 de la arquitectura de protocolos de Bluetooth.

La capa de radio física traslada los bits del maestro al esclavo o viceversa. Tiene un rango de 10 m y opera en la banda ISM de 2,4 GHz, dividiéndola en 79 canales de 1 MHz cada uno. Usa FDM, permitiendo una tasa de 1 Mbps. Interfiere con el IEEE 802.11.

La capa de banda base se asemeja a una subcapa MAC. El maestro de cada piconet define ranuras de tiempo de 625 μs, siendo las ranuras pares usadas por el maestro y las impares por los esclavos. Las tramas pueden tener 1, 3 o 5 ranuras de longitud.

Cada trama se transmite en un canal lógico, llamado enlace. Hay dos tipos:

- ACL (Asíncrono no Orientado a la Conexión): para datos conmutados en paquetes disponibles a intervalos regulares. Los datos viajan de la capa L2CAP del emisor a la del receptor. Se utiliza el mejor esfuerzo, no hay garantías. Un esclavo puede establecer hasta uno con su maestro.
- SCO (Síncrono Orientado a la Conexión): para datos en tiempo real, con una ranura fija. No hay retransmisión. Un esclavo puede establecer hasta tres con su maestro.

La capa L2CAP tiene tres funciones:

- Convertir paquetes de hasta 64 KB en tramas y viceversa.

- Manejar la multiplexión y demultiplexión de paquetes, para saber cuál protocolo de las capas superiores debe manejarlo.
- Gestiona la calidad de los requerimientos de servicio durante el establecimiento de enlaces y la operación normal. Negocia, por ejemplo, el tamaño máximo de carga útil permitido.

Trama Bluetooth

Hay diversos formatos de trama, siendo este el más importante:

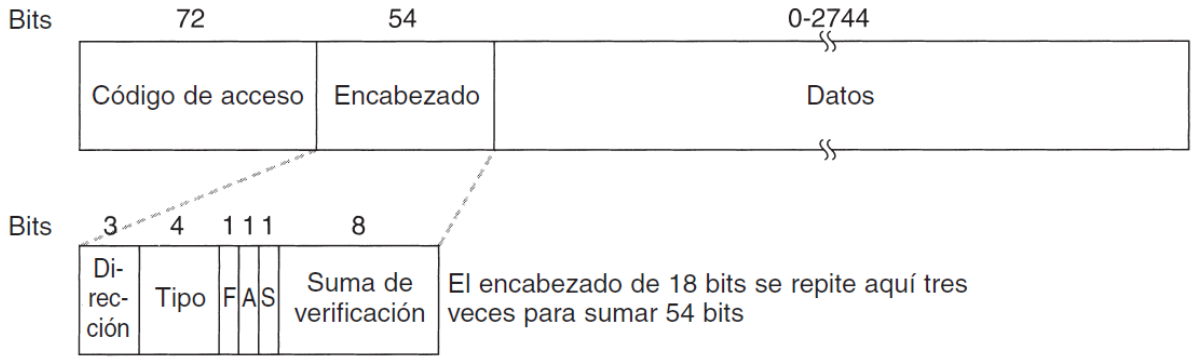


Figura 4-38. Trama de datos típica de Bluetooth.

El código de acceso identifica al maestro, y el tamaño del campo de datos depende de cuántas ranuras de tiempo ocupa la trama.

El campo dirección indica a cuál de los 8 dispositivos activos está dirigida la trama; tipo indica el tipo de la trama (ACL, SCO, de sondeo o nula), el tipo de corrección de errores utilizado en el campo de datos y la cantidad de ranuras de longitud de la trama. El bit F (flujo) indica que el búfer del esclavo está lleno y no puede recibir más datos. El bit A (ACK) permite incorporar una confirmación de recepción en una trama. El bit S (secuencia) permite numerar las tramas para detectar retransmisiones (el protocolo es de parada y espera).

El encabezado se repite tres veces, para poder corregir errores en el mismo.

Conmutación en la capa de enlace de datos

Los puentes, que funcionan en la capa de enlace, examinan las direcciones físicas para enrutar los datos, a diferencia de los routers (de capa de red).

Los puentes permiten la separación de una red grande en LANs.

Algunos motivos para usar puentes son la separación de departamentos de una organización con distintas metas, separación geográfica, manejo de grandes cargas, distancias demasiado largas para un funcionamiento veloz, evitar problemas de confiabilidad por un nodo defectuoso y evitar problemas de seguridad al no enviar todas las tramas a todas las estaciones.

Un puente conecta LANs, utilizando sus múltiples capas físicas y MAC para quitar y colocar los encabezados correspondientes al protocolo al que se dirigen los paquetes, y siendo la capa LLC la encargada de decidir a qué subcapa MAC enviar un paquete recibido.

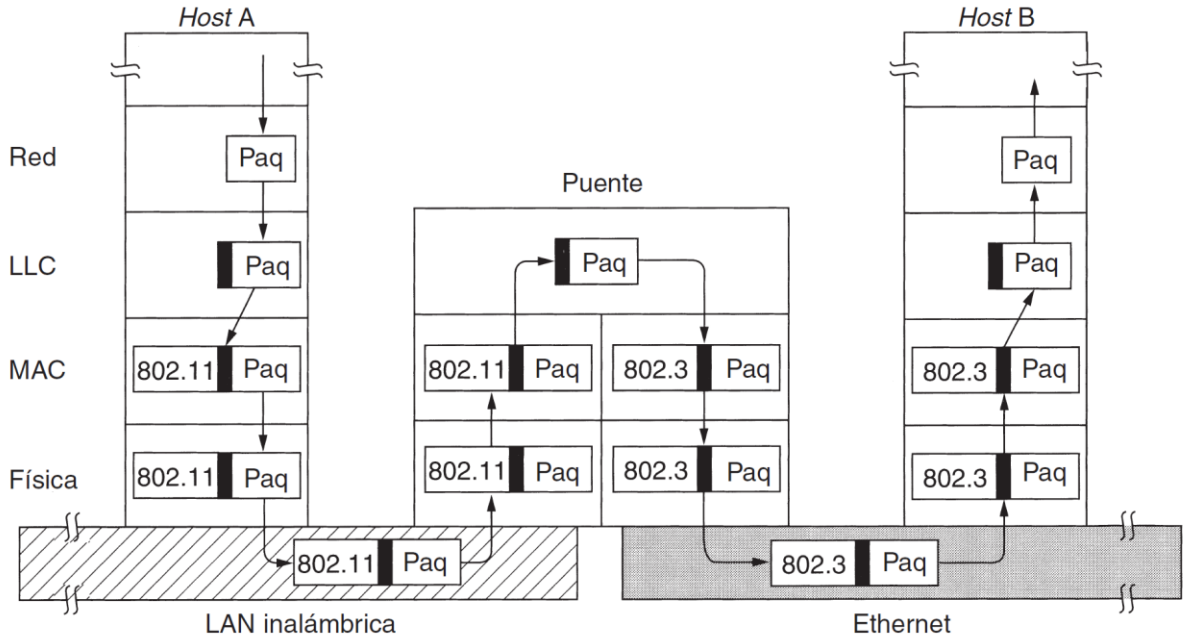


Figura 4-40. Operación de un puente entre una red 802.11 y una 802.3.

Los puentes tienen ciertos problemas a solucionar:

- Dados los formatos de tramas distintos de las LANs, el puente debe adaptarlas y recalcular el CRC.
- Diferencias en tasa de datos de las LANs: si una (o varias) LANs envían tramas a otra LAN más lenta, el puente tendrá que tener un buffer suficientemente grande para que estas tramas no se pierdan.
- Diferencias en la longitud máxima de trama: dado que la capa de enlace no puede dividir la carga útil, cuando una LAN trata de enviar una trama a otra LAN que no soporta tramas de esa longitud, el puente no tiene más remedio que desecharla.
- Seguridad diferente en LANs: si una LAN soporta encriptación y el puente pasa sus paquetes a otra LAN que no la soporta, la estación destino no tendrá forma de saber qué dice el paquete. Se puede solucionar encriptando en una capa superior al enviar paquetes a esta otra LAN, pero se pierde la transparencia.
- Calidad del servicio: se pierden las garantías de calidad ofrecidas por una LAN al conectarla con un puente a otra LAN que no soporta estas garantías.

Interconectividad local

Al recibir una trama, los puentes tienen dos decisiones que tomar: si la descartan o la reenvían y, de decidir reenviarla, hacia dónde.

Cada puente tiene una tabla de hash donde relaciona las LANs que conecta con las máquinas a las cuales se accede por dichas LANs. Esta tabla se va llenando cada vez que recibe una trama, al analizar el origen (algoritmo de **aprendizaje hacia atrás**).

Cuando el destino de una trama es el mismo que su origen, descarta la misma. Si no fuera así, se dan dos situaciones:

- Si conociera el destino, lo reenvía a esta LAN
- Si no, lo reenvía a todas las LANS (inundación) (con excepción del origen).

Para manejar topologías dinámicas, siempre que se recibe una trama no solo se guarda su LAN de origen, sino también la hora actual, para así poder purgar las entradas que tengan más de algunos minutos y, si una estación cambiara de lugar, la red se adaptará sola.

Los ciclos creados al conectar LANs con múltiples puentes presentan un problema: al desconocer un destino, un puente recurre a la inundación, haciendo llegar una trama a otros puentes que también recurrirán a la inundación. Al repetirse este proceso, la trama podrá llegar de nuevo al primer puente, inundando nuevamente de forma recursiva.

Para solucionar el problema de los ciclos, se arma un árbol de expansión, de forma que los puentes de ponen de acuerdo para no armar ciclos. Al conectarse, se envían tramas con su dirección MAC, y se elige como raíz al puente cuya dirección sea la menor. Luego, todos los puentes se van organizando para armar la ruta más corta al puente raíz. Este algoritmo se repite periódicamente para detectar cambios en la topología.

También se usan puentes para conectar LANs remotas, pudiendo considerar al enlace como una LAN sin hosts. Se puede utilizar un protocolo como PPP.

Dispositivos de redes

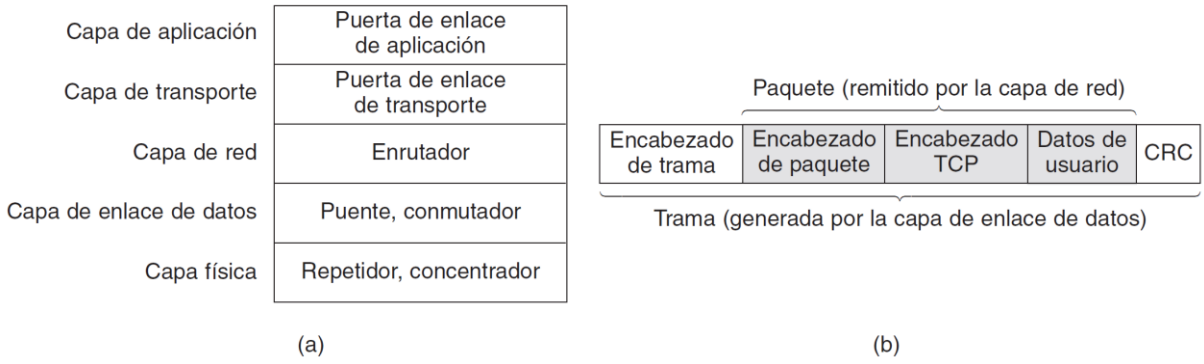


Figura 4-46. (a) Los dispositivos y sus capas correspondientes. (b) Tramas, paquetes y encabezados.

Un repetidor conecta dos cables: cuando aparece una señal en uno, la amplifica y la envía al otro.

Un concentrador une sus múltiples puertos de entrada de manera eléctrica, enviando las tramas que llegan a uno de estos a todos los demás. Forman un solo dominio de colisión.

Un conmutador es utilizado para comunicar múltiples computadoras individuales, de manera similar a como un puente conecta LANs. Cada puerto forma su propio dominio de colisión.

Los conmutadores, como los puentes, tienen un problema cuando llegan tramas más rápido de lo que son retransmitidas. Los conmutadores cut-through alivian este problema al no usar el método de almacenamiento y reenvío, sino al comenzar el reenvío apenas llega el encabezado del destino.

Un enrutador usa el encabezado del paquete (en capa de red) para elegir el puerto de salida, ignorando la dirección física y los protocolos usados en las capas inferiores.

Las puertas de enlace de transporte conectan dos computadoras con diferentes protocolos de transporte orientados a la conexión.

Las puertas de enlace de aplicación traducen los mensajes de un formato a otro.

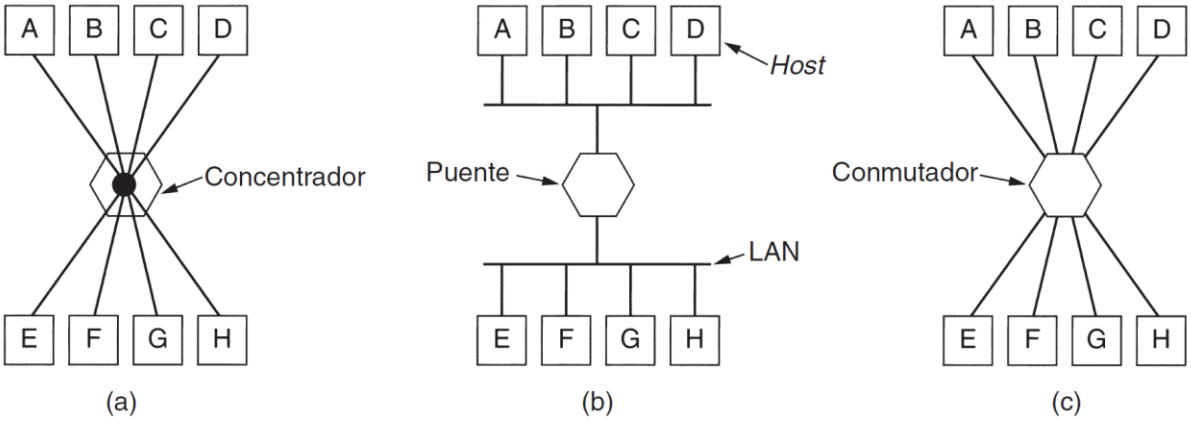


Figura 4-47. (a) Concentrador. (b) Puente. (c) Conmutador.

VLANs

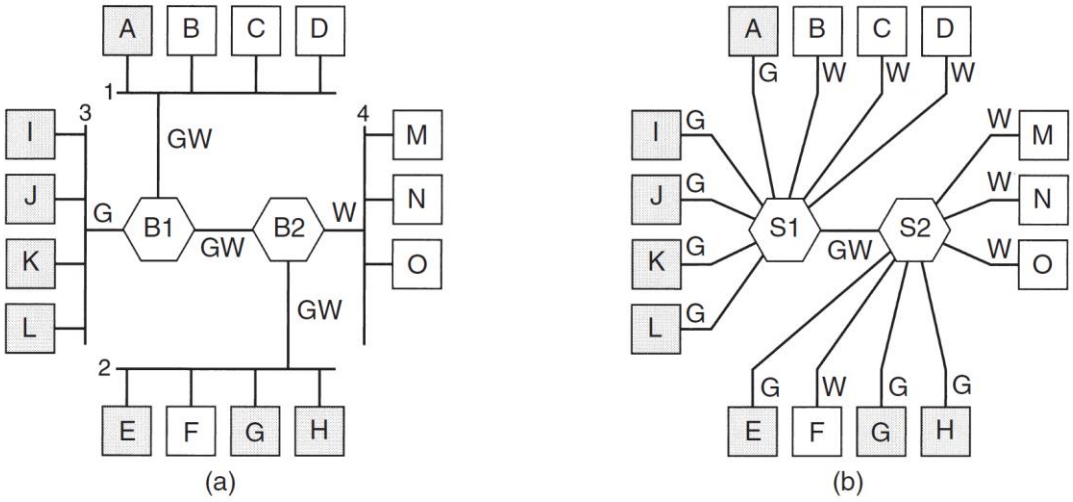


Figura 4-49. (a) Cuatro LANs físicas organizadas en dos VLANs, en gris y blanco, mediante dos puentes. (b) Las mismas 15 máquinas organizadas en dos VLANs mediante conmutadores.

Para poder agrupar lógicamente las estaciones sin considerar la geografía, se utilizan LANs Virtuales o **VLANs**. Sin importar en qué LAN se encuentren realmente, se pueden configurar puentes o conmutadores para que se reenvíen las tramas procedentes de un dispositivo de una VLAN hacia los otros, funcionando como concentradores.

Los métodos para lograr las VLANs son:

- Vincular un puerto con una VLAN (no permite asignar máquinas de múltiples VLANs a un mismo puerto).
- Vincular una dirección MAC a una VLAN.
- Vincular un protocolo de capa de red o una dirección IP con una VLAN (con conmutadores de capa de red).

El estándar 802.1Q agregó un campo VLAN al encabezado de Ethernet para facilitar el enrutamiento. Dado lo caro que sería cambiar todas las tarjetas de red, este campo es agregado por la primera tarjeta en la red que soporte el estándar, ya sea la estación de origen o un puente o conmutador. Los puentes y conmutadores posteriores que soporten el estándar podrán simplemente leer el campo para enrutar; no se le debería enviar estas tramas a los que no lo soporten.

Unidad 3 – Capa de Red

La capa de red tiene una función de **reenvío** (forwarding, transmisión de un paquete de un enlace de entrada a uno de salida en un router) y **enrutamiento** (routing, interacciones colectivas de todos los routers de la red que determinan las rutas que siguen los paquetes).

Otra función de la capa de red que a veces tienen las redes es la **configuración de la conexión**, una negociación entre los routers a lo largo de la ruta para configurar el estado antes de transmitir los paquetes.

La capa de red tiene distintos modelos de servicio de red, como:

- Entrega garantizada (el paquete llegará a su destino)
- Entrega garantizada con retardo limitado (el paquete llegará a su destino en menos de un cierto límite de tiempo)
- Entrega de los paquetes en orden
- Ancho de banda mínimo garantizado (mientras se transmitan los bits a menor velocidad que cierto límite, todos los paquetes llegarán en un intervalo de retardo pre-especificado
- Fluctuación máxima garantizada (la diferencia entre la separación al emitir dos paquetes consecutivos y al recibirlos no variará más que un cierto valor especificado)
- Servicios de seguridad (encriptación con una clave secreta de sesión, integridad de datos, autenticación origen)
- Mejor esfuerzo (sin garantías, usado por Internet)
- CBR (tasa de bit constante, usado por ATM)
- ABR (tasa de bit disponible, usado por ATM)

Arquitectura de red	Modelo de servicio	Garantía de ancho de banda	Garantía sin pérdidas	Orden	Temporización	Indicación de congestión
Internet	Mejor esfuerzo	Ninguna	Ninguna	Posible cualquier orden	No se mantiene	Ninguna
ATM	CBR	Velocidad constante garantizada	Sí	En orden	Se mantiene	No se produce congestión
ATM	ABR	Mínimo garantizado	Ninguna	En orden	No se mantiene	Sí

Tabla 4.1 • Modelos de servicio de Internet, y CBR y ABR de redes ATM.

Redes de circuitos virtuales (VC) y de datagramas

Las redes de circuitos virtuales son aquellas orientadas a la conexión (con este protocolo implementado en la capa de red).

Allí, cada enlace tiene asociado un número de VC, y los routers mantienen una tabla relacionando el puerto y el número de VC con el otro puerto y número de VC para un circuito virtual. Los routers cambian el número de VC, pues esto permite disminuir el tamaño del mismo y no requiere coordinación entre todos los routers del circuito para elegir un VC que nadie esté usando.

Hay tres fases:

- Configuración del VC: la capa de transporte del emisor informa a la de red que desea establecer la conexión; la capa de red determina la ruta, los números de VC y, posiblemente, reserva recursos.
- Transferencia de datos
- Terminación del VC: la capa de red informa al receptor y elimina las entradas de las tablas de reenvío de los routers.

Los mensajes utilizados para configurar el VC se llaman **mensajes de señalización**, siendo intercambiados mediante **protocolos de señalización**.

Por otro lado, las redes de datagramas son no orientadas a la conexión; los routers utilizan la dirección de destino para reenviar los paquetes. Esto se logra buscando coincidencias en el prefijo de la dirección de destino con ciertos prefijos almacenados en la tabla de reenvío. Si hubiera varias coincidencias, el router prefiere aquella entrada de la tabla con el prefijo más largo.

Las tablas de reenvío pueden ser modificadas en cualquier instante, lo que hace factible que una serie de paquetes siga caminos distintos y los paquetes lleguen desordenados.

Reenvío en red de datagramas

Para cumplir con esta función, los routers tienen 4 componentes:

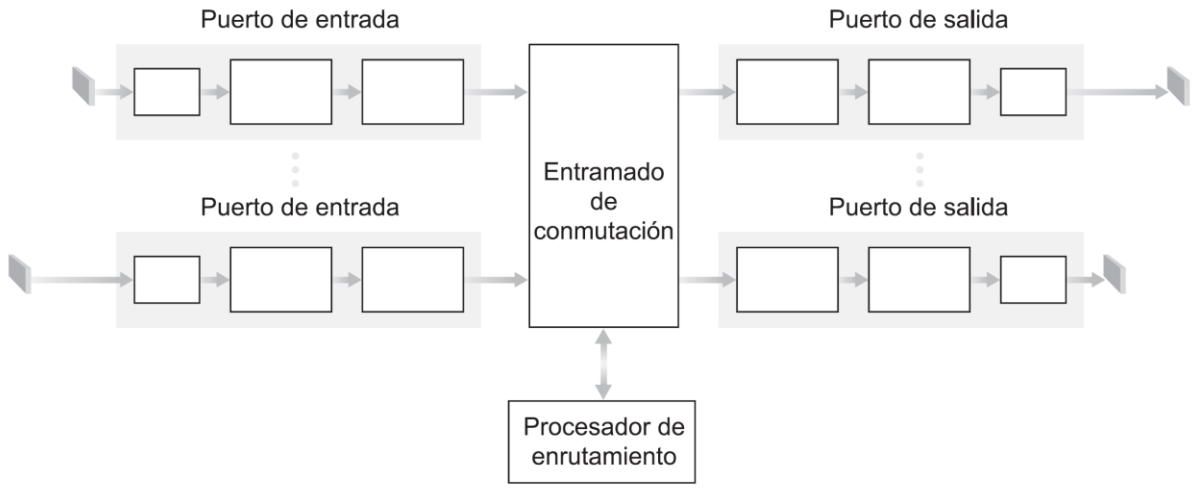


Figura 4.6 • Arquitectura de un router.

Puertos de entrada

Llevan a cabo las funciones de la capa física, de la capa de enlace y una función de búsqueda y reenvío. Suelen agrupase varios puertos en una única tarjeta de línea.

Los puertos de entrada suelen mantener una copia de la tabla de reenvío para poder determinar a qué puerto de salida mandar un paquete. Esta copia es actualizada por el procesador de enrutamiento. Así se evitan cuellos de botella.

Para buscar el prefijo coincidente más grande velozmente, hay distintas técnicas:

- Búsqueda binaria: tomando bit a bit la dirección de destino.
- CAM (memorias direccionables por contenido): acceder a la memoria mediante la dirección IP de 32 bits, almacenando allí la tabla de reenvío directamente.

- Uso de caché de la tabla de reenvío.
- Estructuras de datos rápidas o comprimidas

Antes de pasar al entramado de conmutación, de haber otro paquete ocupándolo, los que intenten entrar se ponen en cola.

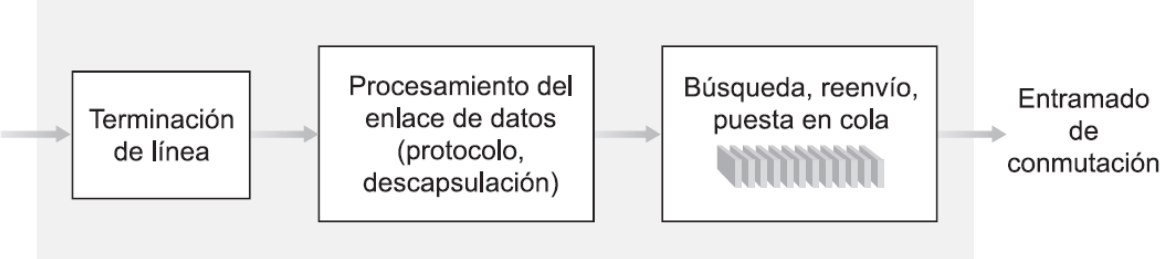


Figura 4.7 • Procesamiento en el puerto de entrada.

Entramado de conmutación

Conecta los puertos de entrada con los de salida. Hay distintos métodos:

- Conmutación vía memoria: de forma similar a una computadora, donde el procesador de enrutamiento es la CPU y los puertos de entrada y salida son dispositivos de E/S.
- Conmutación vía bus: no es necesaria la intervención del procesador, pero solo puede transmitirse un paquete a la vez.
- Conmutación vía una red de interconexión / malla : utilizando una malla para transmitir más de un paquete a la vez.

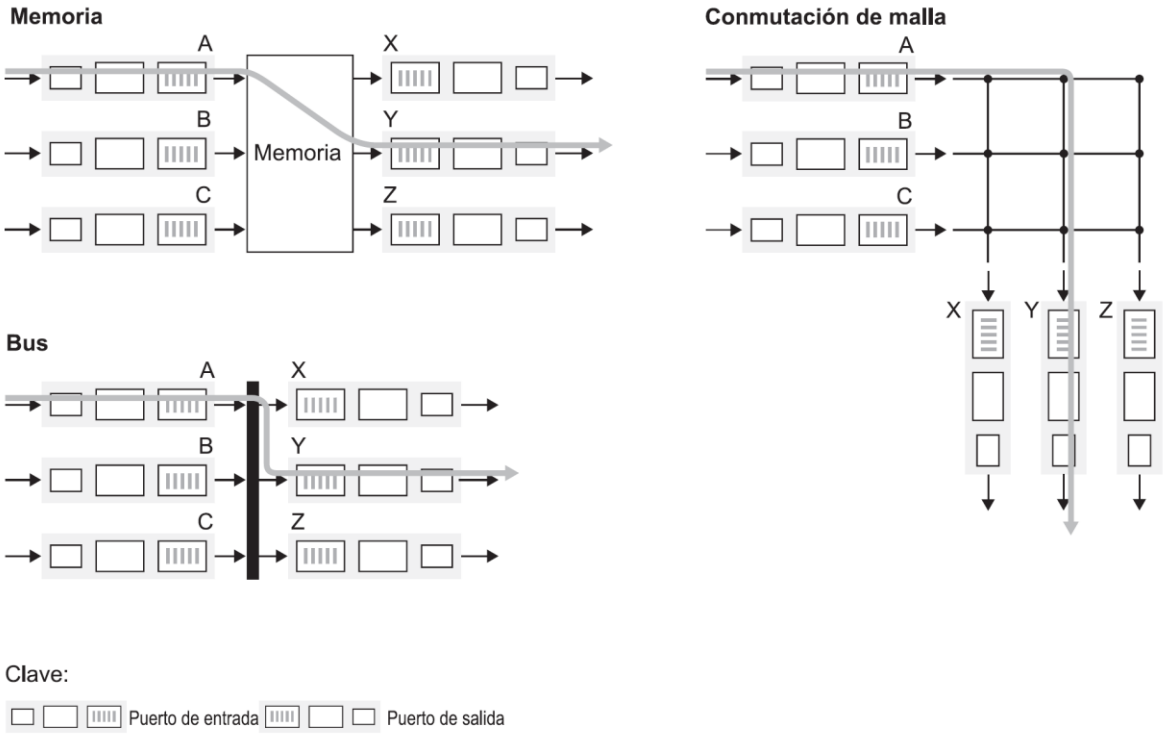


Figura 4.8 • Tres técnicas de conmutación.

Puertos de salida

Almacena y transmite los paquetes, de forma inversa a los puertos de entrada. Cuando un enlace es bidireccional, el puerto de salida suele estar emparejado con un puerto de entrada del mismo enlace en la misma tarjeta de línea.

Es necesario un buffer de cola cuando el entramado suministra paquetes más rápido que la velocidad del enlace de salida. Un planificador de paquetes se encarga de elegir cuál de la cola será transmitido (FIFO / First In First Out, WFQ / Weighted Fair Queuing, etc.), y permite proporcionar ciertas garantías de la calidad del servicio).

Procesador de enrutamiento

Ejecuta los protocolos de enrutamiento, mantiene la información de enrutamiento y las tablas de reenvío, y realiza funciones de gestión de red.

Colas

Si hay n puertos de entrada y n de salida, y las velocidades de línea de entrada y salida son las mismas, una velocidad del entramado de conmutación de al menos n veces mayor que la velocidad de línea de entrada garantiza que nunca habrá cola en los puertos de entrada. Sin embargo, si muchos paquetes fueran a un mismo puerto de salida, podría agotarse su memoria y así perderse paquetes. El tamaño (B) de los buffers se calcula considerando el valor medio del tiempo de ida y vuelta (RTT), la capacidad del enlace (C) y el número de flujos TCP (N): $B = RTT \cdot C/\overline{N}$.

Si no hay suficiente memoria en un buffer de entrada, se puede descartar los paquetes entrantes (drop-tail) o eliminar algún otro para hacer lugar a uno entrante. También se pueden marcar paquetes a descartar previamente, en caso de ser necesario.

Los algoritmos AQM (Active Queue Management) proponen ciertas políticas para descartar y marcar paquetes. Uno muy conocido es RED (Random Early Detection), que mantiene una media ponderada de la longitud de la cola de salida y, según qué tan bajo o alto se encuentre, acepta los paquetes, marca o descarta los paquetes, o se los marca o descarta con cierta probabilidad.

Con conmutación de malla, si múltiples puertos de entrada quieren enviar un paquete a un mismo puerto de salida, uno tendrá que esperar, haciendo esperar también a los demás paquetes detrás en la cola. Esto es un bloqueo HOL (Head-of-the-line).

IP

La capa de red de Internet cuenta con tres componentes: el protocolo IP, los protocolos de enrutamiento y el protocolo ICMP (Internet Control Message Protocol).

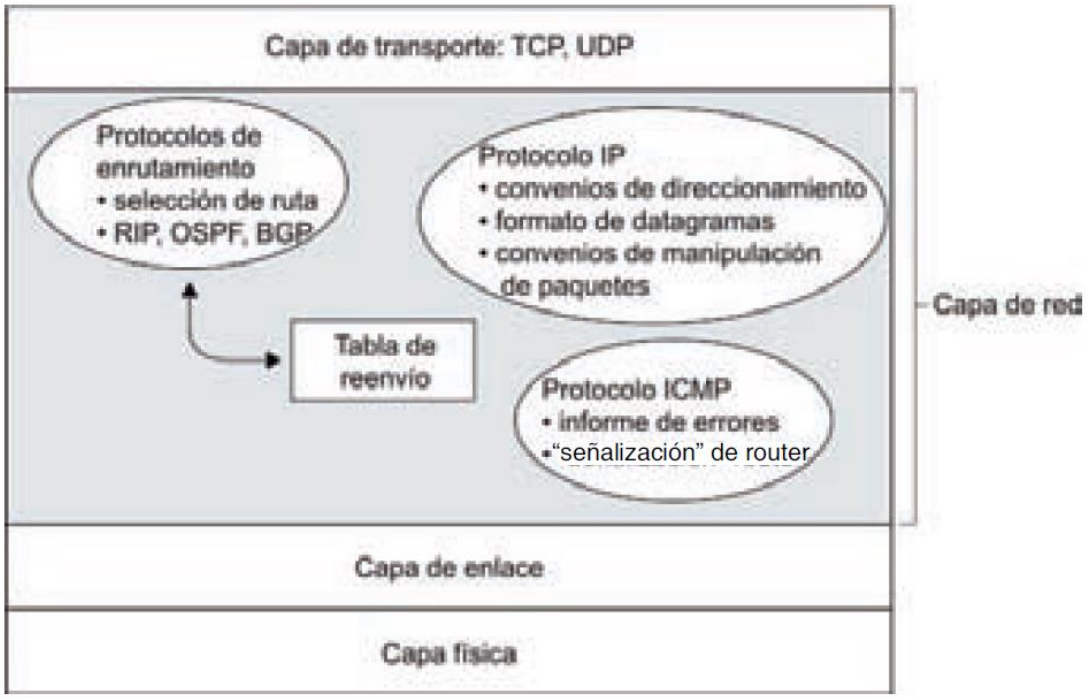


Figura 4.12 • Capa de red de Internet.

Los datagramas de IPv4 tienen el siguiente formato:

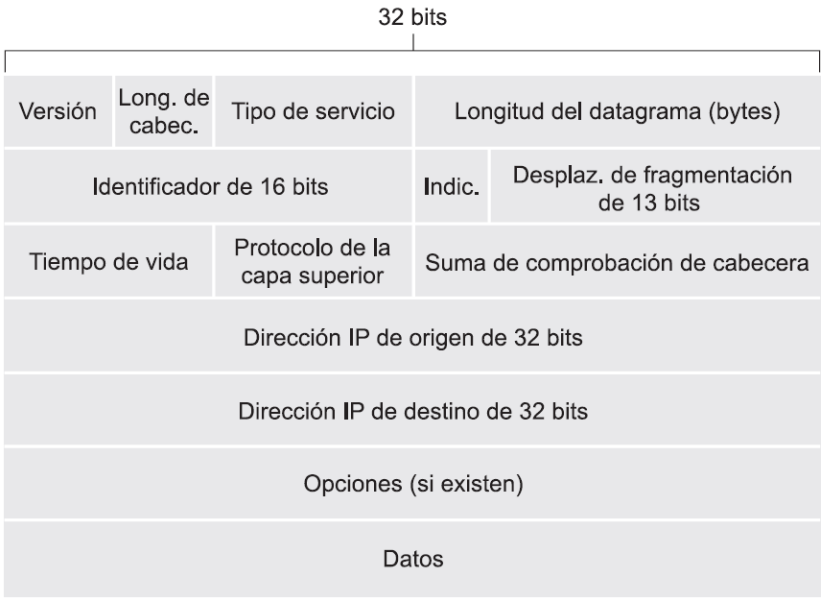


Figura 4.13 • Formato de los datagramas de IPv4.

- Versión: indica al router como interpretar el resto del datagrama.
- Longitud de cabecera: como los datagramas IPv4 pueden tener un número variable de opciones en su encabezado, este campo es necesario para saber dónde empiezan los datos.
- Tipo de servicio (TOS) (en tiempo real o no, orientado a la conexión, etc.)
- Longitud del datagrama: longitud de la cabecera y los datos, permitiendo un tamaño máximo de 65535 bytes.

- Identificador, indicador, desplazamiento de fragmentación: para la fragmentación IP. Al emitir un datagrama, el host le coloca un número en el identificador (suele irlo incrementando de a 1 por cada datagrama). Al llegar a un router que debe reenviarlo por medio de una capa de enlace con menor MTU (Maximum Transmission Unit, tamaño máximo de la trama), este divide los datos y arma múltiples tramas, conservando el identificador. Sin embargo, va incrementando el desplazamiento de fragmentación, y marca con 1 todos los indicadores salvo el último. Así, la capa de red del host destino puede recibir y reensamblar el datagrama original (si llegan todas las tramas).
- Tiempo de vida (TTL, Time-To-Live): campo con un contador que decrece cada vez que un router procesa el datagrama y, si llega a 0, es descartado. Evita que queden datagramas en circulación en un bucle.
- Protocolo: indica qué protocolo de la capa de transporte debe manejar el datagrama.
- Suma de comprobación de cabecera: calculada para detectar errores de un bit en cada router (y descartar el datagrama si hubiera un error).
- Direcciones IP de origen y destino
- Opciones
- Datos (carga útil): segmento de la capa de transporte.

Direccionamiento IPv4

IP requiere que cada interfaz (de host o de router) tenga su propia dirección IP. Estas consisten en 32 bits, usualmente separados en octetos y escritos como cuatro números decimales entre 0 y 255 separados por puntos.

Los routers permiten definir subredes, si todos los hosts conectados a una de sus interfaces comparten cierto número de bits a la izquierda (prefijo de red). La cantidad de bits (N) es indicada con la notación XXX.XXX.XXX.XXX/N, siendo N la máscara de subred. Los enlaces punto a punto entre routers también son subredes.

La estrategia de asignación de direcciones IP en Internet es CIDR (Classless Interdomain Routing, Enrutamiento entre Dominios sin Clase). Esto permite que las tablas de reenvío de los routers sean más pequeñas, al no necesitar una entrada por host (sino por red).

Antes de que se adoptara CIDR se usaba direccionamiento con clases, que definía las clases A, B y C, con prefijo de red de 8, 16 y 24 bits respectivamente.

La dirección IP 255.255.255.255 es de difusión, y los routers reenvían el datagrama a todos los hosts en la subred.

DHCP

Las direcciones IP de los routers suelen ser configuradas manualmente por el Administrador de Sistemas, pero las de host es común que sean asignadas mediante DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host). Este protocolo permite a los hosts solicitar, entre otras cosas, que se le asigne una dirección IP, su máscara de subred, la dirección del router del primer salto (o router de Gateway predeterminado) y la dirección de su servidor DNS local.

DHCP puede ser configurado de modo que un host dado reciba la misma dirección IP cada vez que se conecta a la red, o una dirección temporal. Funciona de modo plug-and-play.

Cuando un host se conecta a la red, genera un segmento UDP con un mensaje de descubrimiento DHCP, difundido a toda la red y con dirección de origen 0.0.0.0. El o los servidores DHCP que lo reciben le responden (difundiendo) con un mensaje de oferta DHCP,

incluyendo una dirección IP, su máscara de red y el tiempo de arrendamiento de la dirección IP. Luego, el host podrá elegir la dirección deseada y responder al servidor con un mensaje de solicitud DHCP, siendo este contestado con un mensaje ACK DHCP.

NAT

Un router NAT (Network Address Translation, Traducción de Direcciones de Red) es, para la red exterior, un único dispositivo con su dirección IP (la cual obtiene del servidor DHCP del ISP).

Cada vez que sale un datagrama de la red LAN por un router NAT, el host debe haber indicado su dirección IP y un puerto arbitrario. El router cambia esta dirección IP por su propia dirección, y el puerto por otro. Almacena tanto la dirección IP como el puerto original y el modificado en la tabla de traducciones NAT.

Por otro lado, al llegar un datagrama desde la WAN y si coincide la dirección IP de destino con la del router, busca en la tabla la entrada con ese puerto de la WAN y cambia la dirección de destino por la del host, y el puerto leído por el original que indicó el host.

ICMP

ICMP (Internet Control Messages Protocol, Protocolo de Mensajes de Control de Internet) queda justo por encima de IP, siendo colocado en la carga útil del datagrama su paquete. Este consiste en dos campos: tipo y código. Es utilizado, entonces, para transmitir cierta información sencilla.

Provee soporte para, por ejemplo, la solicitud y respuesta de eco (ping), red o host de destino inalcanzable o desconocido o TTL caducado.

IPv6

IPv6 surgió por la falta de direcciones IPv4. La estructura de su datagrama es la siguiente:

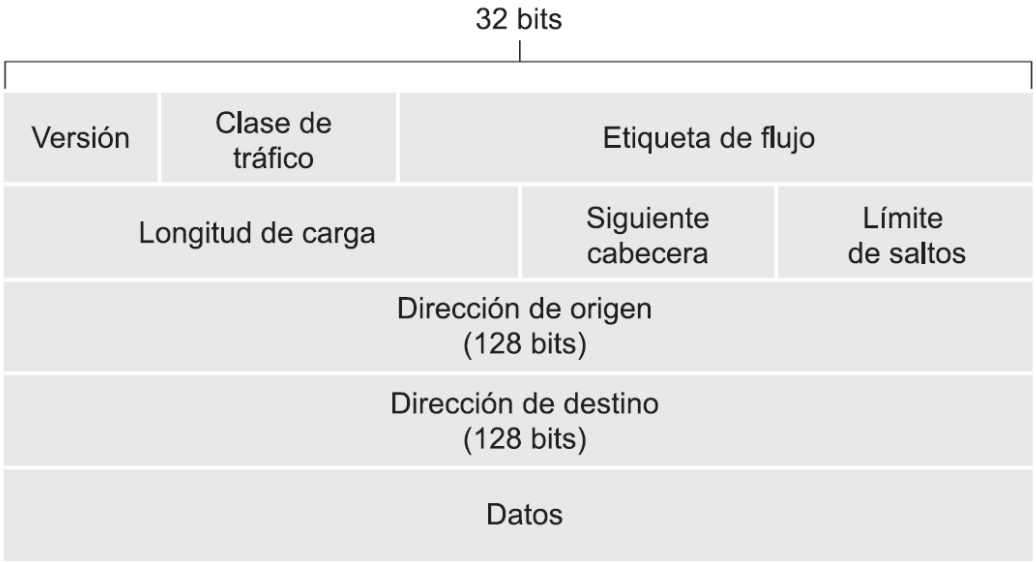


Figura 4.24 • Formato del datagrama de IPv6.

Al compararlo con el datagrama de IPv4, observamos que coincide el campo “versión”, que el campo “clase de tráfico” es equivalente a “tipo de servicio”, “longitud de carga” a “longitud del datagrama”, “siguiente cabecera” a “protocolo de la capa superior”, “límite de

saltos" a "tiempo de vida (TTL)". Ambas también tienen campos para las direcciones de origen y destino, pero estas ocupan 128 bits en lugar de 32. El encabezado ocupa 40 bytes.

La etiqueta de flujo permite "etiquetar" los paquetes para los que el emisor solicita un tratamiento especial.

Con IPv6, además, los routers no soportan fragmentación, por lo que los campos relacionados de IPv4 no son necesarios. Cuando una capa de enlace no soporta el tamaño del datagrama, el router devuelve un mensaje ICMP "Paquete demasiado grande" para que el emisor lo fragmente. ICMP recibió una nueva versión con otros mensajes adicionales; se lo llama ICMPv6.

La implantación de IPv6 se planteó de dos modos: pila dual (mediante nodos IPv6/IPv4, capaces de manejar los dos, pero solo usando IPv6 cuando ambos extremos lo soporten) y tunelización (cuando entre dos routers IPv6 haya routers IPv4, envolver el datagrama IPv6 en uno IPv4 con el otro router IPv6 como destino.

ARP

ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones) gestiona la traducción entre direcciones físicas (MAC) y lógicas (IP). Un módulo ARP, a partir de una dirección IP de la misma subred, puede obtener la dirección MAC.

Cada host y router contiene una tabla ARP, vinculando una dirección IP con una MAC y con un tiempo de vida (TTL) de normalmente 20 minutos.

Cuando un host quiere emitir un mensaje a otro host conociendo su dirección IP pero sin conocer su dirección MAC (es decir, no tiene una entrada para la dirección IP en su tabla ARP), utiliza ARP para enviar un paquete de consulta ARP envuelto en una trama a difundir (dirección MAC de destino: FF-FF-FF-FF-FF-FF). Este paquete contiene campos para las direcciones IP y MAC del emisor y del receptor.

Cada nodo (host o router), al recibir el paquete ARP, verifica si su dirección IP coincide con la de destino. Si esto fuera así, genera un paquete de respuesta ARP (con el mismo formato) y lo envía al emisor (en una trama estándar, no de difusión). Así, el emisor podrá agregar la entrada correspondiente a su tabla ARP (y, para mayor eficiencia, también lo hace el receptor).

Es común que, al conectar un host a la subred, este automáticamente difunda un paquete ARP con su propia dirección IP, permitiendo que todos los demás hosts lo agreguen a su tabla ARP y verificar que nadie más tenga su misma dirección lógica.

ARP se encuentra entre las capas de enlace y de red.

Para transmisión entre subredes, el emisor utiliza ARP para obtener la dirección MAC del router y envía el datagrama con destino al host receptor pero la trama con destino al router. Luego, el router la recibe y la reenvía al host receptor (u otro router, según indique su tabla de reenvío), obteniendo su dirección MAC mediante ARP a partir de la dirección IP en el datagrama.

Enrutamiento

Un algoritmo de enrutamiento global (o de estado de enlaces) busca la ruta de coste mínimo entre un origen y un destino basándose en el conocimiento global de los nodos, enlaces y costos de la red.

Un algoritmo de enrutamiento descentralizado (como vector de distancias) calcula la ruta de coste mínimo entre un origen y un destino mediante un proceso iterativo y distribuido, pues los enrutadores solo conocen los costos de sus propios enlaces.

También se puede clasificar los algoritmos de enrutamiento en estáticos y dinámicos, según la frecuencia con que cambian las rutas. Los algoritmos dinámicos pueden además ser sensibles a la carga, según si el coste de enlace varía dinámicamente para reflejar la congestión del enlace.

Estado de enlaces (LS)

Todos los nodos generan paquetes de estado de los enlaces y los difunden a la red. Con esta información, los nodos pueden ejecutar el algoritmo de Dijkstra, el cual calcula las rutas más cortas desde el nodo en que se encuentra hasta todos los otros. Este algoritmo analiza un nodo, luego sus vecinos y continúa hasta llegar al nodo final, guardando por cada nodo el costo mínimo para llegar a él y el camino que se sigue para ello. En el peor de los casos, tiene una complejidad de $O(n^2)$ (siendo n el número de nodos).

Un problema que surge cuando el algoritmo es sensible a la carga es que los routers actualicen las rutas de forma oscilante, provocando siempre la congestión de algunos enlaces mientras otros quedan libres. Una solución es asegurarse de que los routers se mantengan desincronizados para ejecutar el algoritmo de enrutamiento, posiblemente eligiendo el momento aleatoriamente.

Vector de distancias (VD)

Es un algoritmo distribuido (cada nodo se comunica con sus vecinos), iterativo y asíncrono.

Cada nodo almacena el coste hacia sus vecinos, un vector de distancias con sus costes estimados para ir a cada nodo y los vectores de distancias de sus vecinos.

Cada tanto, un nodo envía su vector de distancias a sus vecinos, los cuales lo usan para actualizar su propio vector de distancias. Tras actualizar su vector, lo envía a sus vecinos. Este proceso tiende a encontrar las rutas óptimas hacia todos los destinos.

La actualización del vector de distancias se consigue aplicando la fórmula de Bellman-Ford: la distancia estimada hacia cualquier otro nodo es la mínima suma entre la distancia que estiman los nodos vecinos y el coste de usar el enlace hacia dicho nodo vecino:

$$D_x(y) \quad \text{mín}_v\{c(x,v) + D_v(y)\}$$

El nodo vecino que haya generado el mínimo es el elegido, y se lo coloca en la tabla de reenvío para el nodo destino.

Eventualmente, el algoritmo entra en estado de reposo por haber encontrado la ruta de menor costo. Se puede salir de este estado cuando un nodo detecta un cambio en el costo a alguno de sus vecinos, si es que este cambio modifica su vector de distancias.

Existe la posibilidad de que, al modificarse el vector de distancias por un cambio en el costo, se forme un bucle de enrutamiento. Este se desarma solo, pero tarda mucho tiempo (pues se requieren muchos mensajes entre los nodos en bucle. A esto se le llama “problema de la cuenta hasta el infinito”.

La técnica de la inversa envenenada puede ayudar a solucionar este problema, siempre y cuando el bucle solo involucre dos nodos. Cuando un nodo A recibe el vector de distancias

actualizado de un nodo vecino B, y el nuevo mínimo para ciertos nodos destino C implica enviarlo por B, A envía un vector de distancias falso a B, indicando que la distancia hacia C es infinita. Así, B no enrutará hacia C mediante A, pero actualizará nuevamente su vector de distancias y, al enviarlo a B, este podrá encontrar la ruta de menor distancia. Finalmente, B envía su vector a A y A también obtendrá esta ruta.

Enrutamiento jerárquico

Considerando la escala de Internet y el deseo de las organizaciones de operar sus routers (autonomía administrativa), se puede organizar los routers en **sistemas autónomos** (AS). Todos los routers de un AS ejecutan el mismo protocolo de enrutamiento interno. Algunos de los routers tienen, además, la función de reenviar los paquetes a destinos externos (routers gateway).

Todos los AS ejecutan el mismo protocolo de enrutamiento entre AS, que les permite determinar si cierto destino es alcanzable por medio de cada AS (ya sea que se encuentre en el AS vecino o en otro, y se deba pasar por el vecino para llegar). Cuando hay más de una ruta por distintos AS, se usa el método de la patata caliente: se pasa el paquete a aquel AS cuyo router gateway se encuentre a menor distancia del router origen.

Enrutamiento en Internet

Se utilizan, dentro de los AS, protocolos de enrutamiento interno o de pasarela interior.

RIP

Routing Information Protocol (RIP) es un algoritmo de vector de distancias que cuenta saltos (tomando 1 como coste de cada enlace entre routers). Se limita el coste máximo a 15.

Cada router mantiene una tabla RIP que vincula la subred de destino con el coste hasta la misma y el siguiente router. Los anuncios RIP son mensajes que se envían cada 30 segundos o al actualizarse la tabla RIP de un router, y contienen esta misma tabla. Cuando un router recibe un anuncio RIP, modifica las entradas de su tabla correspondientes a las subredes de destino cuyo coste sea menor por otra ruta.

Los routers esperan que los demás routers les envíen anuncios al menos una vez cada 180 segundos; si esto no ocurre, los considera inalcanzables y actualiza su tabla, anunciándolo a los otros routers.

Los routers también pueden enviar solicitudes a otros routers acerca del costo de un cierto destino.

Las solicitudes y los mensajes de respuesta o anuncios RIP se envían utilizando UDP.

OSPF

Open Shortest Path First (OSPF) es un protocolo de estado de enlaces utilizado en ISP de nivel superior. No establece una política para los costes; la define el administrador de la red.

Los routers difunden los mensajes a todos los demás routers de la red. Por ejemplo, la información del estado de los enlaces se difunde cuando uno cambia, y periódicamente cada 30 segundos. Estos anuncios son transmitidos directamente por IP.

OSPF incluye funcionalidades de seguridad (autenticación simple y MD5), varias rutas de igual coste (usándose no solo una), soporte integrado para direccionamiento por unidifusión y multidifusión y soporte para definir una jerarquía dentro de un mismo dominio de enrutamiento (estructurando los AS jerárquicamente).

Un AS OSPF puede configurarse en áreas, cada una ejecutando su propio algoritmo de enrutamiento OSPF con difusión hacia los routers de la misma área. A su vez, las áreas cuentan con routers de frontera de área para enrutar los paquetes fuera de esta.

Una única área del AS se configura como área troncal o backbone, encargada de enrutar el tráfico de las demás áreas.

BGP4

Border Gateway Protocol (BGP) enruta entre diferentes AS. Ofrece a los AS mecanismos para obtener información sobre la alcanzabilidad de subredes de AS vecinos, propagar la misma a todos los routers internos del AS y determinar buenas rutas a las subredes.

Hay una conexión TCP BGP para cada enlace que conecta dos routers en distintos AS (sesión externa eBGP), así como conexiones TCP BGP entre los routers de un mismo AS (sesión interna iBGP).

BGP permite que cada AS aprenda qué destinos (prefijos CIDR, es decir, subredes) son alcanzables a través de AS vecinos.

Cada AS se identifica con un ASN (Número de AS) globalmente único.

Cuando un router anuncia un prefijo en una sesión, lo acompaña de ciertos atributos BGP. Un prefijo junto a sus atributos se denomina ruta.

El atributo AS-PATH almacena la secuencia de AS por los que ha pasado un anuncio, para evitar bucles. El atributo NEXT-HOP es la interfaz de router (una dirección IP) que inicia AS-PATH, utilizados para poder configurar las tablas de reenvío. A su vez, NEXT-HOP permite identificar distintos enlaces entre AS con el mismo AS-PATH.

Los routers de pasarela tienen una política de importación, que puede decidir si aceptar o filtrar la ruta (por no querer tráfico que pasó por cierto AS o por ya tener una ruta preferida, por ejemplo).

Cuando hay más de una ruta posible hacia un mismo prefijo, se siguen ciertas reglas de eliminación hasta quedarse con una:

- Por un valor de preferencia local establecido por el administrador de la red.
- Aquellas rutas con AS-PATH más corto.
- Aquellas rutas con el router de NEXT-HOP de menor costo.
- Según un identificador BGP.

Las redes (o AS) terminales nunca anuncian a sus AS (o ISP) proveedores que tienen rutas hacia otros AS, para que no se reenvíe tráfico mediante estos AS terminales.

El tráfico entre ISP proveedores no está estandarizado, pero por lo general solo se acepta aquel que tiene su origen o destino en un AS terminal del ISP.

Difusión y multidifusión

La difusión permite enviar un paquete a todos los nodos de la red, mientras que la multidifusión solo a algunos.

La unidifusión por N canales consiste en que el emisor simplemente envía N paquetes iguales, cada uno con la dirección IP de uno de los N destinatarios.

La inundación no controlada es el envío de un paquete de difusión a todos los nodos vecinos, replicando estos el paquete a todos sus vecinos, y así sucesivamente. Puede ocasionar bucles y una tormenta de difusión.

La inundación controlada busca evitar una tormenta de difusión. Una forma en que lo hace es manteniendo una lista con las direcciones de origen y el número de secuencia de todos los paquetes que ha difundido, evitando así difundir uno más de una vez. El algoritmo Gnutella hace esto, junto a un TTL, que hace que el paquete solo alcance a los nodos a cierta cantidad de saltos del origen.

Otro método de inundación controlada es RPF (Reverse Path Forwarding): los nodos solo reenvían si el paquete llegó por el mismo enlace de la ruta del menor costo al host de origen.

Los modos anteriores de lograr la difusión tienen el inconveniente de enviar paquetes que deben ser descartados, esto se puede solucionar mediante un árbol de recubrimiento. Este método elimina los bucles. Se construye seleccionando un nodo central (punto de cita), al que le llegan paquetes de unidifusión desde otros nodos, formando así el árbol.

Si se desea hacer multidifusión, se utilizan grupos de multidifusión, los cuales tiene su propia dirección IP de clase 10.

Mediante IGMP (Internet Group Management Protocol) se comunican los hosts con sus routers del primer salto, permitiendo averiguar de qué grupos es miembro el host.

Hay dos protocolos para lograr el enrutamiento por multidifusión, y ambos apuntan a armar un árbol:

- Árbol compartido por el grupo: seleccionando un nodo central, y enviando mensajes solicitando unirse solo los routers del primer salto conectados a hosts que usan multidifusión.
- Árbol basado en el origen: se usa RPF para armar el árbol por cada host, y mensajes de poda para eliminar las rutas que no llevan a miembros del grupo.

En Internet, se usan protocolos con árboles basados en el origen: DVMRP (Protocolo de Enrutamiento por Multidifusión por Vector de Distancias), con reenvío de camino inverso y poda; y PIM (Multidifusión Independiente del Protocolo). PIM cuenta con un modo denso (reenvío de camino inverso con inundación y poda) y un modo disperso (árbol compartido por el grupo).

Unidad 4- Capa de Transporte

La capa de transporte proporciona una comunicación lógica entre procesos de aplicación que se ejecutan en hosts diferentes. Los protocolos de esta capa se implementan solo en los hosts, no en los routers. Su trabajo consiste en armar y desarmar los segmentos a partir de los mensajes de la capa de aplicación, posiblemente dividiéndolos.

La capa de transporte puede ofrecer ciertas garantías, aunque la de red no lo haga.

Las redes TCP/IP (como Internet) ofrecen dos posibles protocolos de la capa de transporte: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). El servicio que prestan difiere en que el primero ofrece un servicio orientado a la conexión fiable y el segundo no.

TCP y UDP ofrecen un servicio de multiplexación y demultiplexación para extender la entrega host a host a una entrega proceso a proceso, y un servicio de comprobación de la integridad de los datos.

TCP además ofrece un servicio de transferencia de datos fiable (garantiza entrega de los segmentos, en orden y sin errores), y tiene mecanismos de control de congestión (un servicio para el bien común)

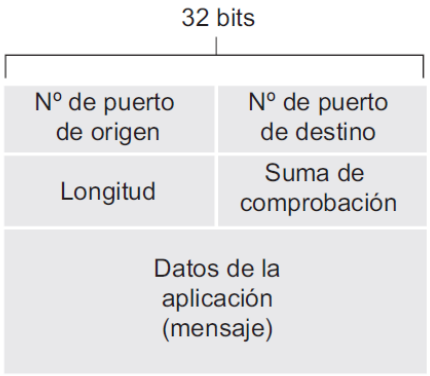
Multiplexación y Demultiplexación

Cada proceso de aplicación puede tener múltiples sockets, contando estos con un identificador. A su vez, cada segmento indica un número de puerto de origen y otro de destino (16 bits cada uno). Al vincular un socket con un número de puerto, la capa de transporte puede armar segmentos y enviarlos (multiplexación) o recibirlos y desarmarlos (demultiplexación).

Los puertos entre 0 y 1023 son considerados muy conocidos, por lo que están reservados.

Un socket UDP que totalmente identificado por una dirección IP de destino y un número de puerto de destino, mientras que uno TCP también requiere dirección IP y número de puerto del origen.

Segmento UDP



El encabezado de UDP contiene los números de puerto de origen y destino, la longitud del segmento (incluyendo el encabezado) y una suma de comprobación. Estos campos tienen 16 bits cada uno.

La suma de comprobación se calcula con complemento a 1 con acarreo al bit siguiente (o al de menor peso, en caso de ser el último bit), considerando palabras de 16 bits, tomando de a dos por vez. Es usada para la comprobación de errores terminal a terminal.

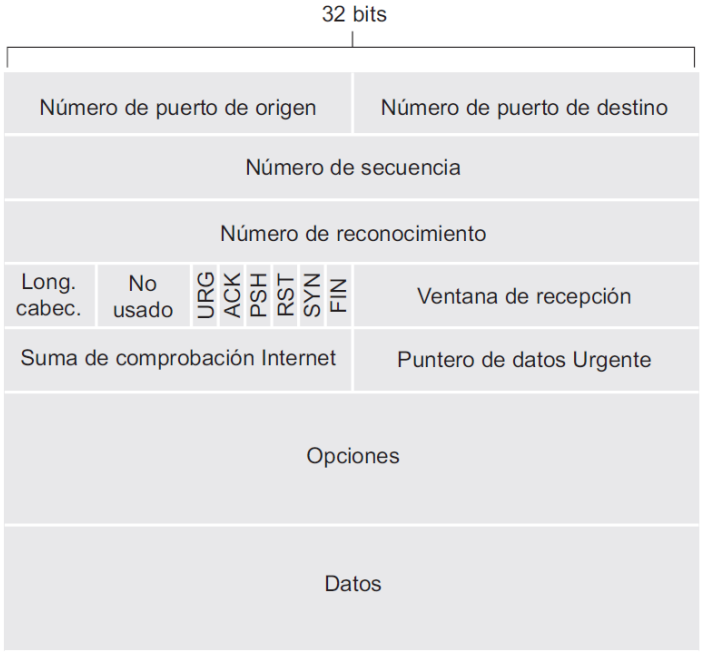
TCP

TCP proporciona un servicio full-duplex punto a punto.

Para establecerlo, se realiza el acuerdo en tres fases, en donde los hosts se ponen de acuerdo en ciertos parámetros.

Ambos hosts cuentan con buffers de emisión y recepción. Sus tamaños y el tamaño máximo de los segmentos (MSS) se determinan en el acuerdo en tres fases.

Segmento TCP



El encabezado (de al menos 20 bytes) contiene múltiples campos:

- Número de puerto de origen y destino
- Número de secuencia (incrementando por el MSS, tamaño máximo de segmento) y de reconocimiento (número del siguiente byte esperado). Usa una mezcla entre retroceso N y repetición selectiva. El temporizador para reenviar se obtiene a partir del promedio móvil exponencialmente ponderado del tiempo de ida y vuelta (RTT) de ciertos paquetes muestreados, y de la desviación estándar de los RTT.
- Ventana de recepción: para control de flujo. Se requiere que el emisor envíe segmentos de un byte de datos cada cierto tiempo para que el receptor pueda responder a los mismos con un AKC, y mantener actualizado el valor de la ventana de recepción.
- Suma de comprobación
- Longitud de la cabecera (cantidad de palabras de 32 bits)
- Opciones: de longitud variable, sirve para negociar el MSS o para definir una opción de marca temporal, por ejemplo
- Puntero de datos urgentes: puntero a parte del campo de datos con bits a pasar urgentemente
- Indicadores:
    - ACK: el valor del campo de número de reconocimiento es válido o no
    - RST, SYN y FIN: para establecer y cerrar conexiones
    - PSH: el receptor debe pasar los datos a la capa superior inmediatamente
    - URG: se usa o no el puntero de datos urgentes

Gestión de la conexión TCP

Para establecer la conexión (acuerdo en tres fases), se envían tres segmentos: SYN del cliente al servidor (estableciendo el número de secuencia del cliente y creando los buffers en el servidor), SYNACK del servidor al cliente (estableciendo el número de secuencia del servidor y creando los buffers en el cliente) y un ACK normal del cliente al servidor, que puede transportar datos. Los números de secuencia iniciales deben ser aleatorios.

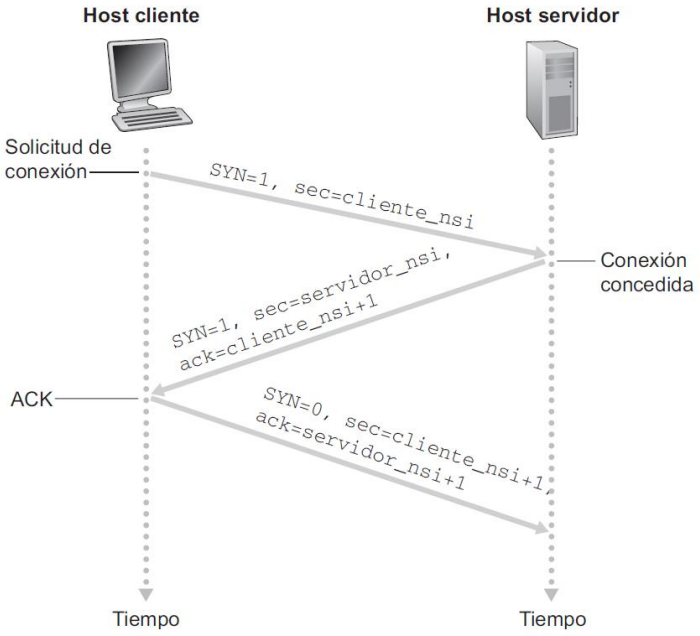


Figura 3.39 • El proceso de acuerdo en tres fases de TCP: intercambio de segmentos.

Para cerrar la conexión, uno de los hosts envía un segmento FIN, contestando el otro con un ACK y enviando luego otro segmento FIN, contestado con un ACK por el primero.

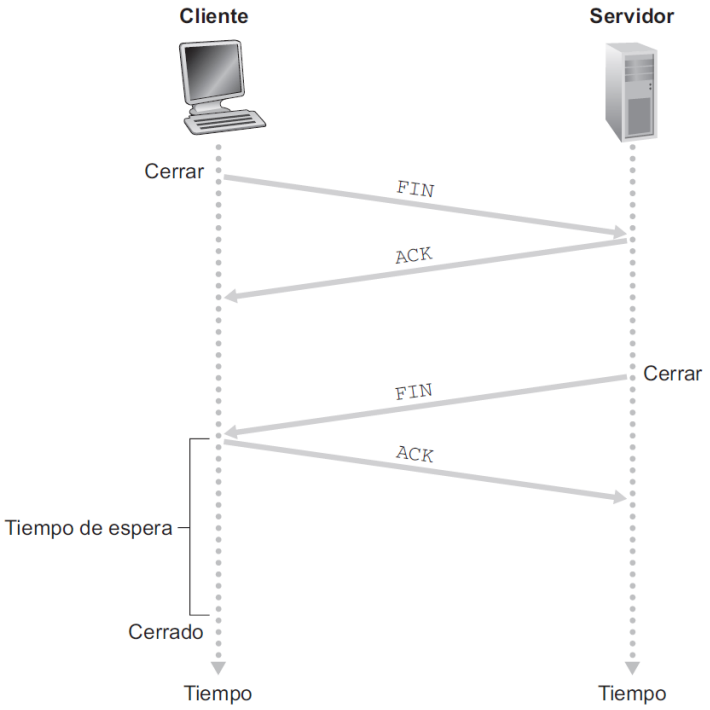


Figura 3.40 • Cierre de una conexión TCP.

Tanto el cliente como el servidor pueden pasar por múltiples estados; considerando el establecimiento y cierre de la conexión:

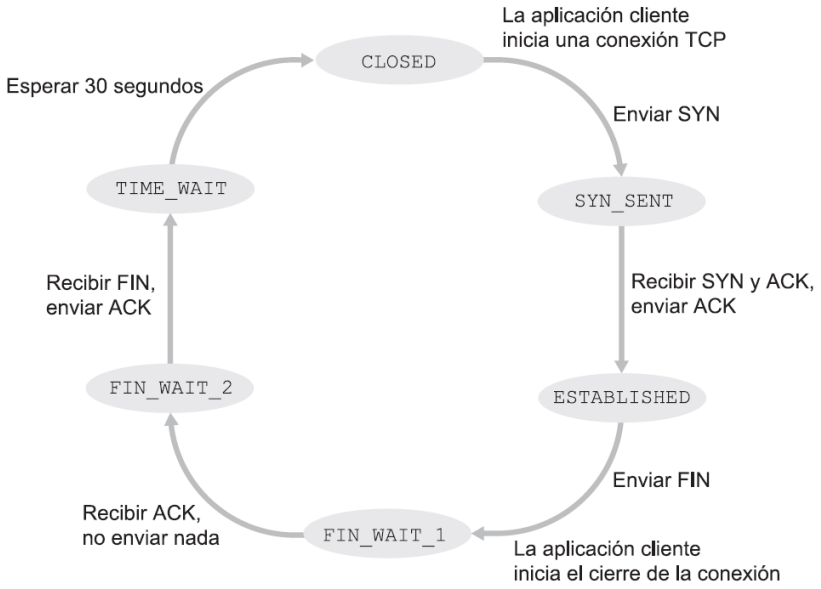


Figura 3.41 • Secuencia típica de estados TCP visitados por un cliente TCP.

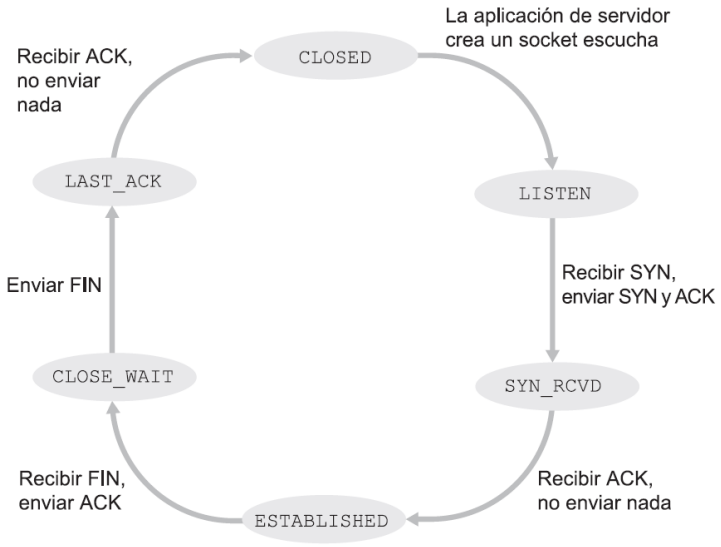


Figura 3.42 • Secuencia típica de estados TCP visitados por un servidor TCP.

Control de congestión

La congestión en una red puede traer los siguientes costos:

- Grandes retardos (dos emisores para un receptor y un router de capacidad ilimitada)
- Retransmisión para compensar pérdidas (dos emisores para un receptor con un router de buffers finitos)
- Retransmisiones innecesarias que ocupan el ancho de banda del router (dos emisores para un receptor con un router de buffers finitos)
- Desperdicio de capacidad de transmisión en routers anteriores cuando uno descarta un paquete (cuatro emisores, routers de buffers finitos, rutas de múltiples saltos)

Según si la capa de red proporciona alguna ayuda para controlar la congestión, se pueden clasificar los métodos en “terminal a terminal” y “asistido por la red”.

Los mecanismos de control de congestión asistido por la red pueden tomar dos formas:

- Directa: mediante un paquete de asfixia generado por un router hacia el emisor
- A través del receptor: el router marca un campo de un paquete que se transmite al receptor, y este le notifica por medio de la red al emisor de la congestión.

ATM

ATM usa circuitos virtuales (VC) para la conmutación de paquetes, pudiendo los enrutadores conocer el comportamiento de cada emisor individual. ABR es el servicio de transferencia de datos de ATM. ABR es elástico, pudiendo transmitir más cuando hay poca congestión y limitándose cuando hay mucha. En jerga de ATM, celda = paquete y dispositivo de conmutación = router.

ABR transmite celdas de datos con algunas celdas de gestión de recursos (RM) intercaladas, las cuales permiten realizar el control de congestión. Estas celdas RM las pueden generar los hosts y los dispositivos de conmutación, por lo que sirven para realimentación directa y a través del receptor.

El control de congestión de ABR se basa en la velocidad. Mecanismos:

- Bit EFCI (Explicit Forward Congestion Indication): un dispositivo de conmutación puede poner el bit EFCI de una celda de datos para indicar congestión. Al llegar al destino una celda RM, si la última celda de datos tenía EFCI = 1, este pone el bit CI (Congestion Indication) de la celda RM en 1 y la devuelve al emisor.
- Bits CI y NI (No Increase, número de incremento): un dispositivo de conmutación pone el bit NI de una celda RM en 1 si hay congestión leve, y el CI en 1 si es severa. El receptor devuelve la misma celda RM al emisor, a menos que por el mecanismo del bit EFCI le corresponda poner CI en 1.
- Configuración de ER (Explicit Rate): el campo ER de las celdas RM contienen un número, cuyo valor puede ser disminuido por un dispositivo de conmutación congestionado. Este campo establece la velocidad mínima soportable de todos los dispositivos de conmutación existentes en la ruta.

Un emisor ABR de una red ATM ajusta la velocidad a la que envía celdas en función de los valores de CI, NI y ER de las celdas RM devueltas.

TCP

TCP detecta congestión en la red cuando finaliza un temporizador y se debe reenviar un segmento, o cuando se reciben cuatro ACKs para el mismo segmento. Para controlar la velocidad a la que envía segmentos según la congestión en la red, modifica una variable de ventana de congestión.

Se toman los siguientes principios:

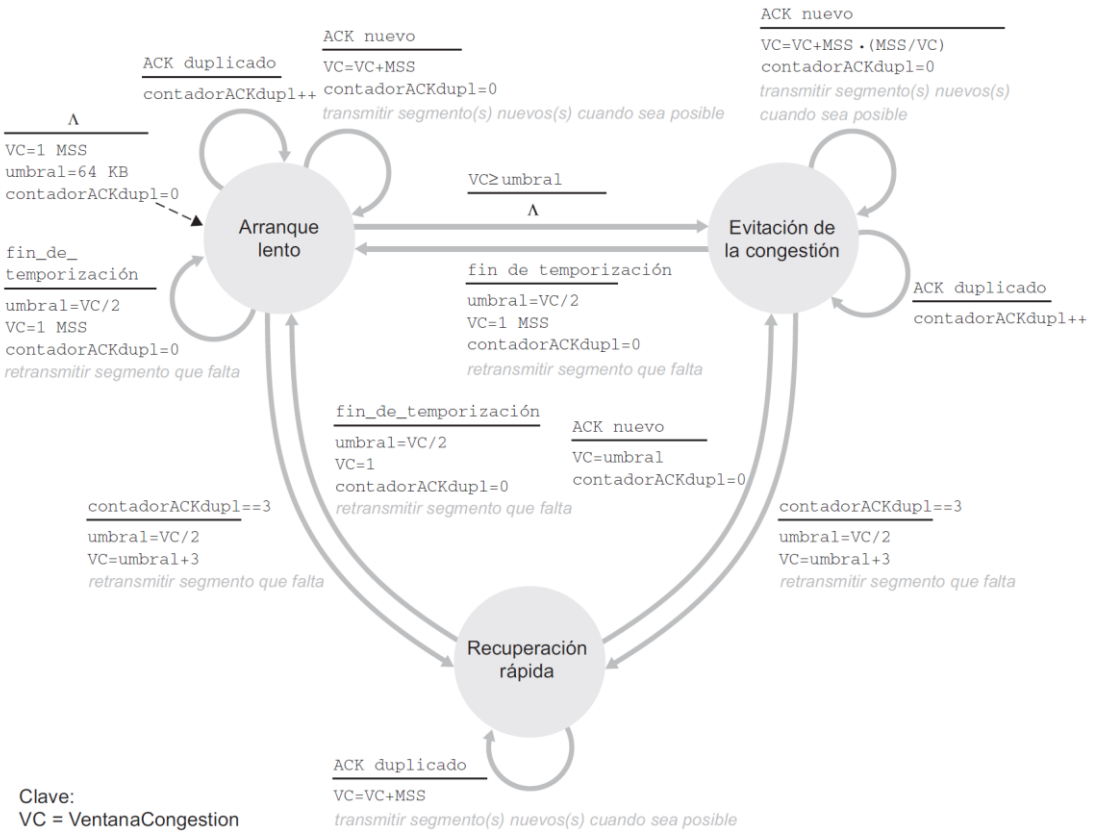
- Segmento perdido => congestión => reducir velocidad del emisor
- Segmento reconocido (ACK) => entrega a tiempo => aumentar velocidad del emisor
- Tanteo del ancho de banda: TCP aumenta la velocidad hasta que se pierde un paquete, en esta situación reducirla y, más tarde, repetir.

Hay un algoritmo de control de congestión de TCP, estandarizado en RFC 2581. Tiene tres componentes principales:

- Arranque lento: la ventana de congestión se inicializa en 1 MSS (tamaño máximo de segmento). Iterativamente, va enviando segmentos de tamaño 1 MSS. Primero, manda 1 segmento y, al recibir el ACK, incrementa la ventana en 1 MSS. Procede a mandar 2

segmentos, e incrementa la ventana en 1 MSS por cada ACK. Continúa con 4 segmentos, luego 8 y así sucesivamente, hasta que se pierde un segmento.
En este momento, se reinicia el proceso de arranque lento, restableciendo a 1 MSS el valor de la ventana y coloca el valor de la variable umbral en ventana/2.
También puede terminar el arranque lento al alcanzar o superar el umbral, pasando al modo de evitación de la congestión.
Por último, si se reciben tres segmentos ACK duplicados, se realiza una retransmisión rápida y entra en el estado de recuperación rápida.

- Evitación de la congestión: incrementar la ventana de congestión en 1 MSS por cada RTT. Esto se puede lograr, por ejemplo, sumando MSS / ventana por cada ACK recibido. Al perderse un segmento, la ventana se fija en 1 y el umbral en ventana / 2. Al recibirse 3 ACKs duplicados, coloca umbral = ventana / 2 y ventana = umbral + 3 y entra en estado de recuperación rápida.
- Recuperación rápida (opcional): incrementar la ventana de congestión en 1 MSS por cada ACK duplicado del segmento que causó que TCP entre en este estado. Cuando llega un ACK nuevo, se va al estado de evitación de la congestión, colocando ventana = umbral. Cuando hay un fin de temporización, se va al estado de arranque lento, colocando ventana = 1 MSS y umbral = ventana / 2.



Por su funcionamiento, se dice que el control de congestión de TCP es de crecimiento aditivo y decrecimiento multiplicativo (AIMD). En un gráfico, tiene un comportamiento de “dientes de sierra”:

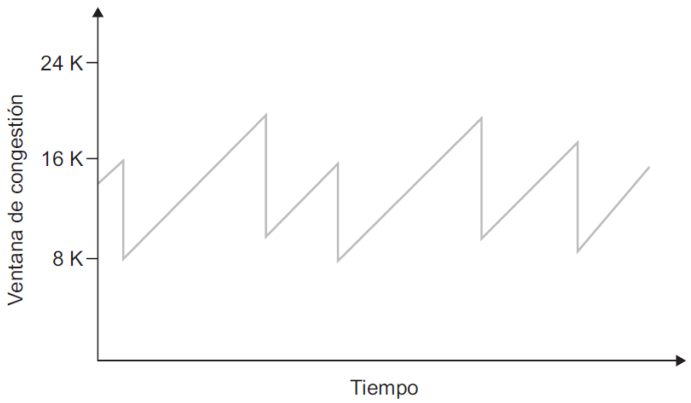


Figura 3.54 • Control de congestión con crecimiento aditivo y decrecimiento multiplicativo.

TCP es equitativo, pues reparte el ancho de banda entre las distintas conexiones TCP que atraviesan un nodo de a partes iguales.

UDP, al no tener un mecanismo de control de gestión, no es equitativo. Es por esto que las transmisiones UDP pueden expulsar tráfico TCP.

Unidad 5 – Capa de Aplicación

Las aplicaciones pueden tener una arquitectura:

- Cliente-servidor: un host activo, servidor, da servicio a las solicitudes de otros hosts, clientes, activos o intermitentes. Se puede agrupar varios hosts para formar un cluster (servidor virtual, centro de datos).
- P2P (peer-to-peer): comunicación directa entre parejas de hosts conectados de forma intermitente. Hay autoescalabilidad. Hay tres retos: el ancho de banda de los ISP residenciales, la seguridad y el incentivo a los usuarios a ofrecer sus recursos.

Un socket es la interfaz o API entre la capa de aplicación y la de transporte. Mediante él, la aplicación elige el protocolo de transporte y quizás algunos parámetros.

Los protocolos de capa de transporte se pueden clasificar según los siguientes servicios:

- Transferencia de datos fiable: todos los paquetes llegan, en orden y sin duplicados.
- Tasa de transferencia (garantizada): para aplicaciones sensibles al ancho de banda (no elásticas).
- Temporización: garantía se entregar cada bit en no más de cierto tiempo.
- Seguridad: pueden ser muy variados, como la confidencialidad (cifrado), integridad y autenticación.

Internet tiente como protocolos de transporte a TCP y UDP. Para lograr aquí el direccionamiento de procesos, se usan direcciones IP con puertos.

Un protocolo de la capa de aplicación define cómo los procesos de una aplicación que se ejecutan en distintos hosts se pasan los mensajes. Define:

- Los tipos de mensajes intercambiados
- Sintaxis de los tipos de mensajes
- Semántica de los campos
- Reglas para determinar cuándo y cómo un proceso envía y responde mensajes

Web y HTTP

HTTP (Hyper Text Transfer Protocol) es el protocolo de aplicación de la Web y está definido en RFC 1945 y RFC 2616. Se implementa en dos programas: un cliente (navegador) y un servidor. Usa TCP.

El servidor no almacena información del estado del cliente (sin memoria del estado).

Por defecto, HTTP usa por defecto conexiones persistentes (una sola conexión para todas las solicitudes y respuestas), pero se lo puede configurar para que no (una conexión por solicitud y respuesta). Las conexiones no persistentes se pueden acelerar al realizarlas en paralelo.

HTTP tiene dos tipos de mensajes:

- Solicitud HTTP: se separa en líneas: 1 de solicitud (método, URL, versión), algunas cabeceras (nombre: valor), una línea en blanco y el cuerpo. Algunos métodos son GET, HEAD, POST, PUT, PATCH, DELETE.

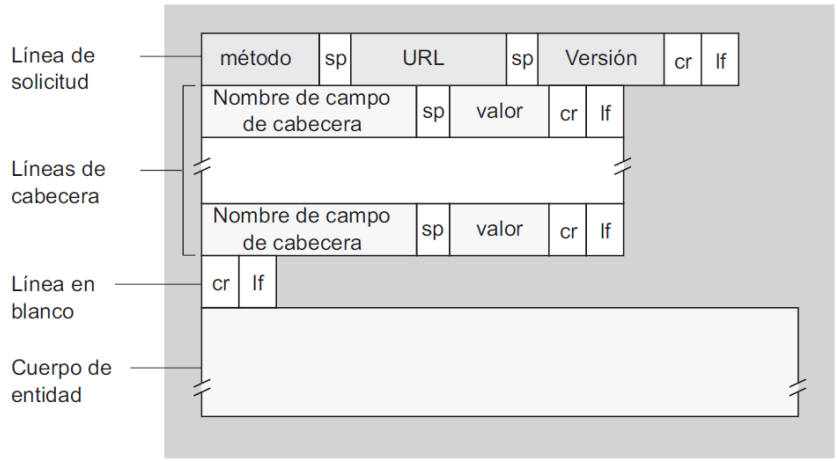


Figura 2.8 • Formato general de un mensaje de solicitud HTTP.

- Respuesta HTTP: se separa en líneas: 1 de estado inicial (versión, código, mensaje), algunas cabeceras (nombre: valor), una línea en blanco y el cuerpo. Las familias de código son 100, 200, 300, 400 y 500.

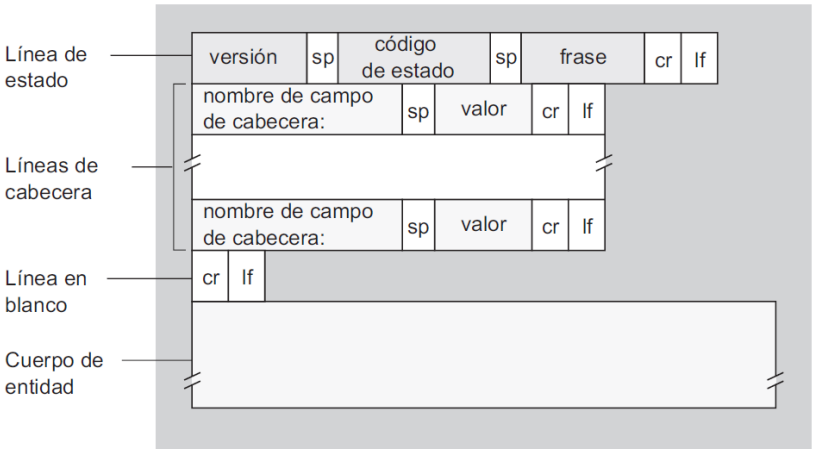


Figura 2.9 • Formato general de un mensaje de respuesta HTTP.

HTTP suele usar cookies para mantener la sesión de los usuarios. Se gestionan con las solicitudes y las respuestas, almacenan los datos en el navegador y el servidor mantiene un registro de ellas en una base de datos.

Un servidor proxy permite tener una caché web, reduciendo el tiempo de respuesta y el tráfico en el enlace de acceso a Internet de una institución.

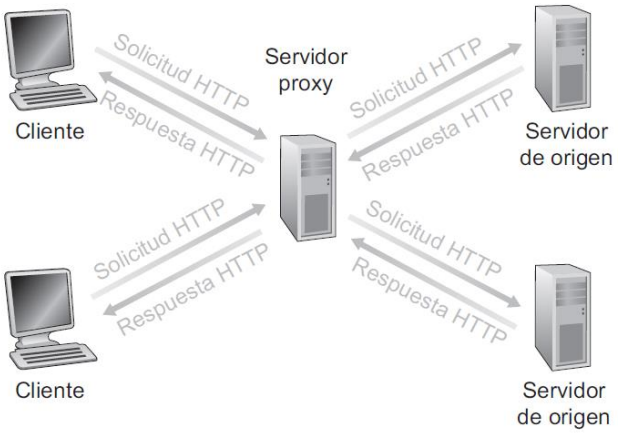


Figura 2.11 • Clientes que solicitan objetos a través de una caché web.

FTP

FTP (File Transfer Protocol) permite a un host transferir archivos desde o hacia un host remoto. Se utiliza un usuario y contraseña. El usuario interactúa con FTP mediante un agente de usuario FTP.

Usa dos conexiones FTP paralelas para transferir un archivo: una de control y una de datos. Se dice que envía su información de control fuera de banda.

Mantiene un estado del usuario, asociando la conexión de control con una cuenta de usuario específica y conociendo el directorio actual del usuario.

FTP tiene comandos (del cliente al servidor) y respuestas (del servidor al cliente) que se envían a través de la conexión de control en formato ASCII de 7 bits.

Comandos:

- USER nombre_de_usuario: para identificar al usuario
- PASS contraseña: para enviar la contraseña al servidor
- LIST: listar todos los archivos existentes en el directorio actual
- RETR nombre_de_archivo: recuperar un archivo del directorio actual
- STOR nombre_de_archivo: almacenar un archivo en el directorio actual

Respuestas:

- 331 Username OK, password required
- 125 Data connection already open; transfer starting
- 425 Can’t open data connection
- 452 Error writing file

Correo electrónico

Tiene tres componentes principales: agentes de usuario (MUA), servidores de correo (MTA) y SMTP (Simple Mail Transfer Protocol). El MUA transfiere los correos al MTA, y otro MUA los puede recuperar.

SMTP transfiere mensajes desde los servidores de correo de los emisores a los de los destinatarios. Los servidores mantienen colas con los mensajes a enviar.

Los mensajes SMTP constan de líneas de cabecera (nombre: valor), seguidas por una línea en blanco y el cuerpo. Todos los correos requieren una cabecera From y otra To, con otras adicionales como Subject.

Para acceder a los correos que residen en el servidor, un MUA puede usar protocolos como:

- POP3 (Post Office Protocol 3): el MUA abre una conexión TCP al puerto 110 al servidor de correo y luego pasa por tres fases: autorización (mandando usuario y contraseña), transacción (recuperar mensajes) y actualización (eliminando los mensajes que se haya marcado y cerrando la sesión). El MUA ejecuta comandos, y recibe respuestas: OK o ERR.
- IMAP (Internet Mail Access Protocol): más complejo de POP3, permite por ejemplo organizar los correos dentro del servidor y realizar búsquedas. Cada mensaje se asocia con una carpeta, yendo los nuevos a inbox. Permite también obtener los mensajes por partes.
- HTTP

DNS

DNS (Domain Name System) es un protocolo que permite traducir nombres de host a direcciones IP. Usa UDP en el puerto 53. Es común que otros protocolos de capa de aplicación lo utilicen.

DNS ofrece otros servicios, como alias de host, alias del servidor de correo y distribución de correo.

Se utilizan mensajes de solicitud con el nombre de host deseado, y mensajes de respuesta con todas las direcciones IP correspondientes.

No es buena idea tener un único servidor DNS centralizado, pues tiene problemas como ser el único punto de fallo, requerir constante mantenimiento, manejar mucho volumen de tráfico y la distancia demasiado grande de ciertos host.

Por esto, se utilizan servidores DNS con una topología jerárquica y distribuida, con servidores DNS raíz, de nivel superior (TLD, Top-Level Domain) y autoritativos. También hay servidores DNS locales, que no pertenecen estrictamente a la jerarquía.

El funcionamiento puede seguir los siguientes esquemas:

- Iterativo: el host solicita al servidor local las direcciones IP de un nombre de host, y este servidor se lo solicita al raíz. El raíz contesta con la dirección IP del TLD, por lo que el local procede a preguntarle lo mismo, y este contesta con la dirección del autoritativo. Finalmente, se le solicita al autoritativo las direcciones, este las devuelve y el local se las devuelve al host.
- Recursivo: El host se comunica con el local, el local con el raíz, el raíz con el TLD y el TLD con el autoritativo, formando una especie de cadena.

Una gran mejora que se puede implementar son las cachés DNS en los servidores locales, para reducir la cantidad de consultas.

Los servidores DNS almacenan los registros de recursos (RR), los cuales tienen cuatro campos: nombre, valor, tipo y TTL.

Los tipos son:

- A: vincula nombre de host con dirección IP
- NS: vincula nombre de dominio con nombre de host de un servidor DNS autoritativo
- CNAME: vincula un alias a un nombre de host canónico
- MX: vincula alias a un nombre canónico de un servidor de correo

Los mensajes DNS, tanto de solicitud como respuesta, usan el mismo formato:

- Cabecera (12 bytes):
    - Identificación: para vincular una consulta con su respuesta
    - Indicadores: banderas, como por ejemplo si es consulta o respuesta, o si se desea usar recursión
    - 4 campos “número de”, correspondientes a la longitud de las cuatro secciones de datos siguientes
- Cuestiones: para la consulta a realizar, indicando l nombre y el tipo de RR a consultar
- Respuestas: contiene los RR devueltos
- Autoridad: contiene registros de otros servidores autoritativos
- Información adicional

Para agregar registros a la base de datos DNS, se debe hacer por medio de una entidad registradora. Estas son acreditadas por la ICANN.