Capa de enlace de datos

Las funciones específicas de la capa de enlace de datos son:

- Definir formas de acceso al medio.
- Agrupar los bits en tramas.
- Regular el flujo de datos.
- Controlar de errores.
- Proveer una interfaz de servicio a la capa de red.

Subcapa de control de enlace – LLC

- Los servicios que le provee a la capa de red pueden ser:

  Tipo 1 – Sin acuse y sin conexión: no espera confirmación de recepción, no establece conexión, no hay corrección de errores. Es apropiada cuando la tasa de errores es baja o para comunicaciones en tiempo real.
  Tipo 2 – Con acuse y con conexión: Se establece una conexión entre las máquinas antes de comenzar el envío. Se garantiza que las tramas lleguen en orden y sin errores. Ideales para comunicaciones punto a punto.
  Tipo 3: - Con acuse y sin conexión: Se confirma la recepción de cada trama enviada, y en caso de que esta no llegue puede reenviarse. Es apropiada para canales inestables.

- Reordenamiento y enmarcado de tramas

Una trama tiene la siguiente forma:

Cabecera	Control	Datos	Final	Redundancia

Cabecera: permite identificar el comienzo de la trama.
Control: contiene información de control.
Final: permite identificar el final de la trama.
Redundancia: contiene información para el control de errores.

La LLC se ocupa de enmarcar estas tramas para que el receptor entienda dónde comienza y termina. Hay diferentes formas de hacerlo:

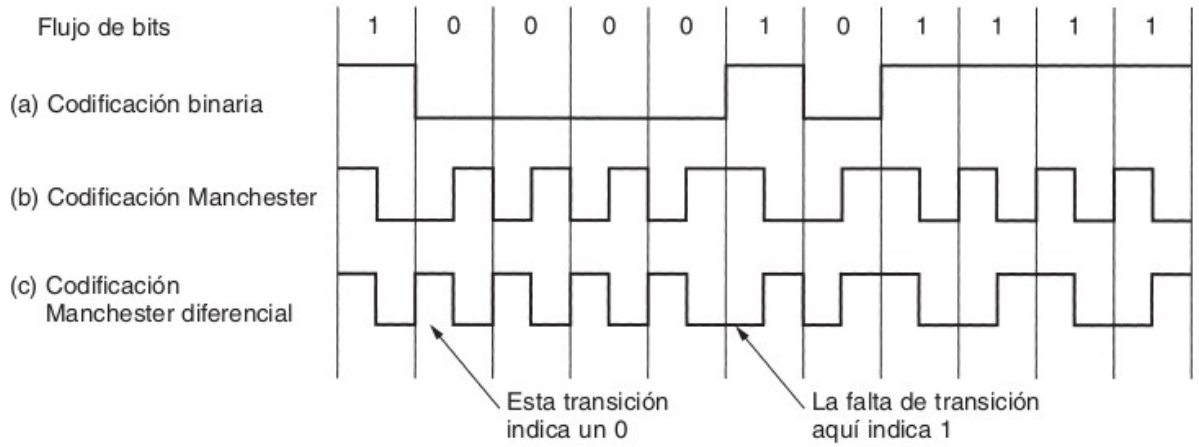
Cuenta caracteres
Consiste en agregarle un campo longitud a la trama. Entonces la capa de enlace de datos ve la cuenta de caracteres y sabe cuantos caracteres siguen y por lo tanto dónde termina cada trama.
El problema es que si se produce un error en este campo, el destino perderá la sincronía y será incapaz de localizar el inicio de la siguiente trama. Incluso si se detecta que la trama esta errónea, solicitar una retransmisión tampoco ayuda porque el destino no sabe cuantos caracteres tiene que saltar para llegar al inicio de la retransmisión.

Banderas de inicio y parada con inserción de caracter.

Este método consiste en la inserción de un caracter de inicio y otro de fin. Anteriormente se usaban caracteres diferentes pero en la actualidad se utiliza el mismo, se lo denomina bandera. De esta forma se soluciona el problema de sincronización, pues si el receptor pierde sincronía, sólo tendrá que buscar la bandera para encontrar el final de la trama anterior y el comienzo de la actual.
El problema de éstos caracteres de enmarque es que pueden confundirse con los datos. En éstos casos, cuando el transmisor detecta que hay un caracter idéntico al de terminación de la trama entre los datos, le antepone otro que advierte que debe ignorar el significado de fin del mismo.
A este carácter que se le llama de escape.
Cuando un caracter de escape aparece entre los datos el transmisor lo duplica, así el receptor entiende que en realidad se quiso transmitir uno de éstos.
Éste método tiene como desventaja que depende del conjunto de caracteres utilizado por cada maquina en particular.

Banderas de inicio y fin con inserción de bit
Es algo similar al método anterior pero a nivel de bits. Por ejemplo se conviene que la secuencia 01111110 se debe interpretar como delimitación de tramas. Si esta secuencia aparece entre los datos se aplica la siguiente regla: "Si dentro de los datos vienen mas de 5 bits seguidos en 1, se inserta un 0 luego del 5 bit en 1". El receptor cada vez que vea 5 bits en 1 seguidos removerá el 0 que le sigue.
Éste método soluciona el problema de los distintos conjuntos de caracteres que puede utilizar cada maquina, operando a nivel de bits.

Violación de código de la capa física
Éste método requiere que a nivel físico se transmita una señal cuya codificación sea distinta a la utilizada para representar 0ros y 1nos. Como por ejemplo la codificación Manchester, donde se representa el 1 como alto-bajo, el cero como bajo-alto y la señal de fin-inicio como alto-alto.



- Control de errores

Una vez que solucionamos el problema de enmarcar las tramas, llegamos al problema de cómo asegurar que todas las tramas se entreguen y en el orden apropiado a la capa de red del destino. Esto no tendría importancia si fuese un servicio no orientado a la conexión y no confiable.
Para asegurarnos la entrega confiable de datos es necesario que el receptor regrese tramas de control especiales que contengan información de recepción

positiva o negativa de que las tramas llegan.
Una complicación adicional puede surgir si la trama desaparece. En este caso al receptor nunca le llegará ninguna trama entonces tampoco enviará tramas especiales de recepción. Este problema es solucionado colocando un temporizador en la capa de enlace de datos. Luego de enviar la trama éste se activa, y si luego de un tiempo no tiene noticias, la reenviará. En otro caso se cancelará.
Además puede pasar que se pierda la confirmación de que la trama llego correctamente. En este caso el emisor reenviará la trama pero el receptor ya la recibió. El receptor no la aceptara otra vez porque a las tramas salientes se le asignan números a fin de que el receptor sepa si es un original o una retransmisión.

Códigos de corrección y detección de errores.
Los diseñadores de redes han desarrollado dos estrategias principales para manejar errores. Una es incluir suficiente información redundante en cada bloque enviado para que el receptor pueda deducir que carácter se quiso enviar, esta usa códigos de corrección de errores, se la llama corrección de errores hacia adelante. La otra es incluir información redundante hasta el punto de que el receptor pueda reconocer que hubo un error y pedir retransmisión, esta utiliza códigos de detección de errores.

Si el canal es lento, nos conviene detectar el error y corregirlo. En cambio si tenemos un canal de velocidad media, conviene hacer un pedido de retransmisión.
Dentro de los controles de detección tenemos:

- Bit de paridad
- Checksum
- CRC o suma de verificación.

Dentro de los controles de corrección tenemos:

- Hamming
- BHC o generalización de Hamming.

- Control de flujo

Otro tema de diseño importante que se presenta en esta capa, es qué hacer cuando un emisor quiere transmitir tramas a mayor velocidad que aquella con la que puede aceptarlas el receptor. El emisor envía tramas a alta velocidad hasta que satura por completo al receptor. Aunque la transmisión esté libre de errores, en cierto punto el receptor no será capaz de manejar las tramas a medida que llegan y las perderá.
Se utilizan dos métodos para controlar este problema. En el primero el control de flujo está basado en retroalimentación, el receptor regresa información al emisor autorizándolo para enviar más datos o indicándole su estado.
En el segundo, el control de flujo está basado en la tasa, es decir se le limita la tasa a la que el emisor puede transmitir los datos.

Subcapa de acceso al medio – MAC

En la introducción vimos que hay dos formas de transmitir datos entre dos máquinas: redes de difusión o redes punto a punto.

En las redes de difusión, el asunto clave es determinar el turno para hablar de cada una de las máquinas conectadas a esa red, con le objetivo de evitar choques y pérdida de información.
Los protocolos para determinar quien sigue en un canal multiacceso perteneces a la MAC.

Protocolos de acceso múltiple

- ALOHA puro

La idea es que el usuario que tenga algo que enviar lo envié. Por supuesto habrá colisiones y como consecuencia las tramas se dañaran, pero debido a la propiedad de retroalimentación de los canales de difusión, el emisor podrá saber si la trama fue destruida o no mediante una confirmación de recepción. Si la trama se destruyó, el emisor esperará un tiempo aleatorio y luego la enviará de nuevo.
Funciona bien en canales con pocos usuarios y poca información. Uso del canal = 18%

- ALOHA ranurado

En este sistema, se divide el tiempo en intervalos discretos. Los paquetes se transmiten dentro de estas ranuras, sincronizadas por una estación especial. Se aumento el uso del canal a un 36%.
Estos protocolos no pueden escuchar lo que están haciendo las demás estaciones, lo cual hace que existan muchas colisiones. Los protocolos en los que las estaciones escuchan una portadora, se llaman protocolos de detección de portadora.

- CSMA: antes de transmitir escucha el canal, según el tipo de persistencia que tenga el protocolo actuará de forma diferente:
    - Persistente 1: si el canal está desocupado transmite, sino espera que se desocupe. El canal se aprovecha un 50%.
      El retardo de propagación juega un rol importante, pues si una estación comienza a transmitir y otra esta lista para enviar y detectar el canal, existe la posibilidad de que si la señal de que se esta enviando algo no le llega a la otra estación, y ésta comience a transmitir y se provoque una colisión.
      Aun si el retardo fuese cero habría colisiones pues, si una estaciona está transmitiendo y en el medio de ésta transmisión otras dos estaciones están listas para enviar, al finalizar lo que se esté enviando estas dos saldrán a querer enviar sus datos y habrá una colisión. Si las estaciones fuesen menos impacientes habría menos colisiones.
    - No persistente: Si el canal está ocupado, espera un tiempo aleatorio y lo vuelve a escuchar. El canal se aprovecha un 90%
      Conduce a un mejor aprovechamiento del canal pero produce mas retardo que la persistente-1.
    - Persistente p: si el canal está desocupado transmite con probabilidad p. El canal se aprovecha un 95%.

- CSMA/CD: cuando detecta una colisión frena el envío, espera un tiempo aleatorio y luego recomienza los algoritmos de detección de portadora.

Ninguno de éstos protocolos garantiza la entrega confiable de la trama, incluso en la ausencia de colisiones, el receptor podría no haberla recibido por alguna otra razón. Tampoco garantiza que la trama se transmita en un tiempo acotado, pues podría demorar un tiempo grande hasta tener la oportunidad de ser transmitida.

Protocolos por turno.

- Reparto estático del canal: por división de frecuencias o por ranuras de tiempo.
- Paso de testigo: una trama especial (token) es transmitida periódicamente , va circulando por todas las estaciones. Si alguna de ellas desea transmitir, anexa sus datos al token, sino la deja pasar. Si el token pasa por alguna estación receptora, entonces deja los datos correspondientes y sigue...

Ethernet – IEEE 802.3

Ethernet es un conjunto de estándares y protocolos que refieren a una comunicación alámbrica.
Ethernet y IEEE 802.3 difieren en aspectos menores, es por ello que muchos lo usan como sinónimos.
El emisor no se entera si las tramas llegaron a destino o no y tampoco existe una autoridad central para garantizar el acceso al medio.
La eficiencia de Ethernet disminuye levemente respecto del numero de estaciones de la red y aumenta con el numero de bytes presentes en la trama.
Utiliza el protocolo CSMA/CD persistente – 1 para el control de acceso al medio.
Hay diferentes formas de lograr el cableado:

Nombre	Cable	Seg. Max	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 económico
10Base-F	Fibra Óptica	2000 m	1024	Mejor entre edificios

Para transmitir la información por el medio de comunicación utiliza la codificación Manchester.

Trama Ethernet: Debe tener una longitud mayor a 64 bytes y menor a 1518.

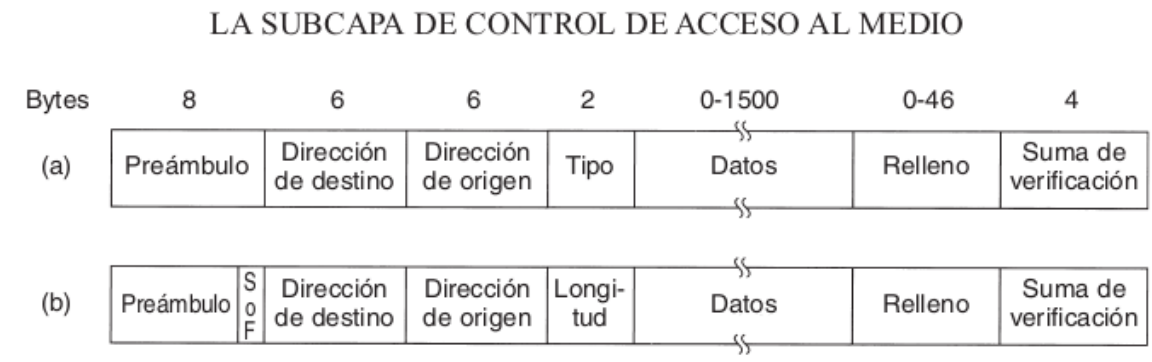
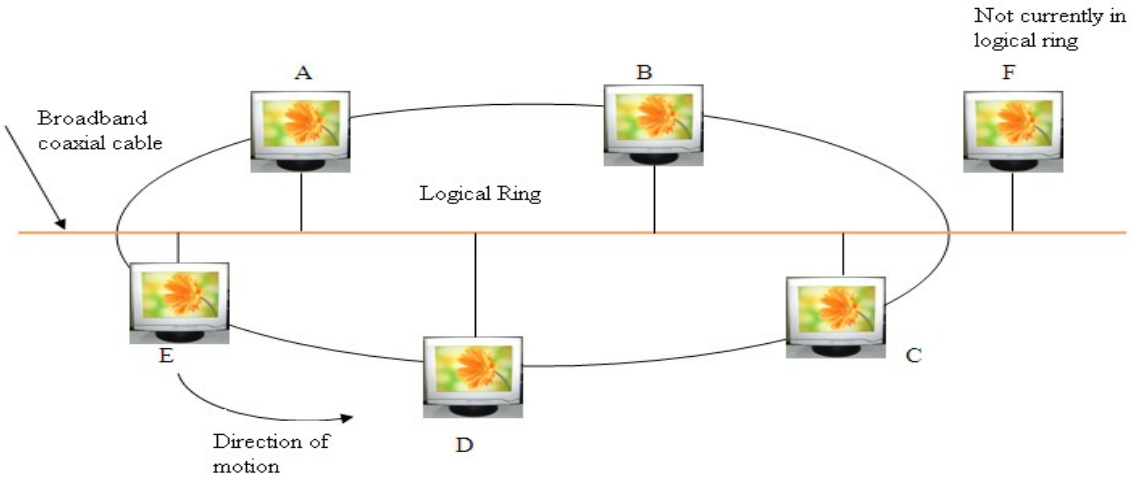


Figura 4-17. Formatos de trama. (a) Ethernet DIX. (b) IEEE 802.3.

Preámbulo: combinación de bits que permite la sincronización entre el emisor y el receptor.
Inicio: octeto de inicio donde comienza la información.
Relleno: se agrega cuando la cantidad de datos no es suficiente al mínimo requerido.
CRC: verificación de redundancia cíclica.
Una trama con una longitud menor a 64 Bytes se descarta porque se interpreta como posibles restos de una trama colisionada.
Posteriormente salieron mejores versiones de Ethernet como Fast Ethernet con una velocidad de 100Mbps y Gigabit Ethernet con una velocidad de 1Gbps.

Token Bus – IEEE 802.4

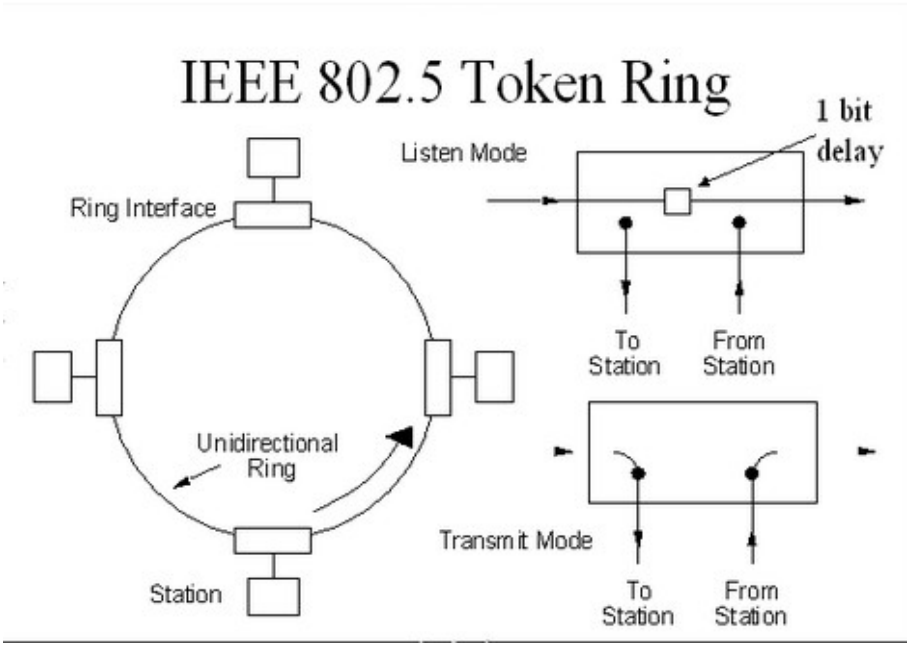
Es de utilidad para el uso industrial. No se puede decir lo mismo de Ethernet ya que no se pueden definir prioridades de transmisión y por las características de su protocolo MAC, podría hacer esperar mucho a una estación para transmitir.



Esta es una nueva norma, basada en paso de testigo, con topología lógica de anillo pero implementación física lineal.
En este caso vemos un cable coaxial de banda ancha de 75 ohms con velocidades de 10Mbps y una longitud del cable no mayor a 100m.
Como dijimos usa el protocolo de paso de testigo, que a diferencia de CSMA/CD, todas las estaciones escuchan pero solo podrán transmitir las que posean el testigo en cada momento.
Existen dos tipos de tramas, las de control y las de datos. La de control se va modificando a medida que las estaciones toman control del testigo. Sus formatos son parecidos a las tramas Ethernet.

Token Ring – IEEE 802.5

En realidad no es un protocolo MAC pues opera físicamente como un punto a punto. Las tramas se transmiten bit a bit entre máquinas adyacentes.



Para la capa física se especifica UTP operando de 4 a 16 Mbps. El perímetro no debe superar los 360m. Un problema es que si se rompe una conexión el anillo desaparece. Esto se soluciona colocando un MAU que concentra todas las conexiones en un centro de estrella física. Osea que el anillo se concentra en un solo lugar.

Comparación entre 802.3, 802.4 y 803.5

Ethernet es simple, tanto en operatoria como en instalación. Es eficiente con tramas de datos largas pero si aumenta el tráfico aumentan las colisiones y es menos segura.
Token Bus es más elaborada, requiere un equipo más sofisticado, se orienta a la industria aunque también se usa en oficinas. La ventaja que tiene es que se le puede dar prioridad a determinadas estaciones y un trafico de datos sin colisiones.
Token Ring es simple y económico, pero depende del buen estado y velocidad de las estaciones, pues si una de ellas se sale de servicio se cae toda la red. Un MAU solucionaría esto pero su costo es elevado.

Dispositivos para extender redes

- Repetidor: Opera en la capa física. Es un dispositivo análogo conectado a dos segmentos de cable. Una señal que aparece en uno de ellos, es amplificada y enviada al otro. Los repetidores se manejan con voltios.
- Concentrador (hub): Opera en la capa física. Tiene numerosos puertos de entrada que une de manera eléctrica. Las tramas que llegan a cualquiera de estos puertos, se envían a todas las demás. Constituye un solo dominio de colisión. Todas las líneas que convergen en el hub deben operar a la misma velocidad. No amplifica las señales por lo general.
- Puente (bridge): Opera en la capa de enlace. Conecta dos o mas LAN's. Cuando llega una trama, el software del puente extrae la dirección de destino y la busca en una tabla para saber por donde enviar la trama.

Cada puerto constituye su propio dominio de colisión. Puede conectar diferentes tipos de red y diferentes velocidades.
- Conmutador (switch): Opera en la capa de enlace. Mucha gente se refiere a conmutador y puente como cosas indistintas. La diferencia en realidad esta en que un conmutador se usa con mayor frecuencia para conectar computadoras individuales, mientras que un puente conecta LAN's, por ello los switch deben contar con mucha mas cantidad de puertos.
- Enrutador (router): Opera en capa de red. Envía paquetes de una red a otra por la ruta mas adecuada en cada momento.

LAN's Inalámbricas

El medio de comunicación de estas redes es a través de ondas electromagnéticas (de radio o infrarrojo) en lugar del cableado estándar. La banda de frecuencias utilizadas no pueden ser asignadas de forma aleatoria por el fabricante, ya que existen regulaciones legales en cada país para controlar el uso eficiente y adecuado del espectro como así también la potencia de transmisión irradiada.
Actualmente se pueden identificar tres tipos de LAN's inalámbricas:
- WPAN (Wireless Personal Area Network): Están pensadas para cubrir un área del tamaño de una habitación. Tradicionalmente los infrarrojos dominaron este tipo de red. Es a baja velocidad y distancias cortas. La tecnología Bluetooth es el estándar que rige este tipo.
- WLAN (Wireless Local Area Network): Son redes que cubren el ámbito de una casa u oficina.
- WWAN (Wireless Wide Area Network): Son redes que cubren áreas amplias como por ejemplo una ciudad. Las telefonías móviles desarrollan este tipo de redes.

WI-Fi – WLAN – IEEE 802.11

El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles mas bajos del modelo OSI.
En general los protocolos de la rama 802.xx definen técnicas de redes de área local.

Arquitectura

Esta basado en una arquitectura celular donde el sistema se subdivide en celdas, donde cada celda o BSS se controla por una estación base o AP. El sistema puede estar formado por una única celda con un único AP o por varias celdas donde los AP's están unidos por un enlace troncal. Este sistema en su conjunto se llama sistema de distribución o DS.

Capa Física

- Codificación/decodificación de señales.
- Generación/remoción de cabeceras.
- Transmisión/recepción de bits.
- Especificaciones del medio de transmisión.

El estándar IEEE 802.11 ha tenido muchas cambio y evoluciones desde su origen. Algunas de ellas son: FHSS, OFDMa OFDMg, etc.

Capa de Enlace

Funciones de la MAC:

- Recepción/Transmisión: Ensamblado de datos en una trama con campos de direccionamiento y detección de errores.
- Administra el acceso al medio de transmisión.

Funciones de la LLC:

- Provee una interfase de servicio hacia las capas superiores, realiza controles de flujo y errores.

Control de acceso al medio MAC- Protocolo de la subcapa MAC

En Ethernet se transmite la trama y se asume que llega correctamente, en los enlaces de radio esto es diferente ya que las bandas de frecuencias utilizadas están sujetas a ruidos. Es por ello que el protocolo de la subcapa MAC para 802.11 es muy diferente al de Ethernet.

Para empezar, puede pasar que A quiera comunicarse con C pero no lo puede hacer directamente porque no la alcanza, y que se produzca una colisión en la estación B porque ambas transmitieron al mismo tiempo. Este es el problema de la estación oculta.

También existe el problema de la estación expuesta y es cuando A esta transmitiendo a D y B quiere transmitirle a C, entonces como escucha el canal y ve que A está transmitiendo, piensa erróneamente que se producirá una colisión.

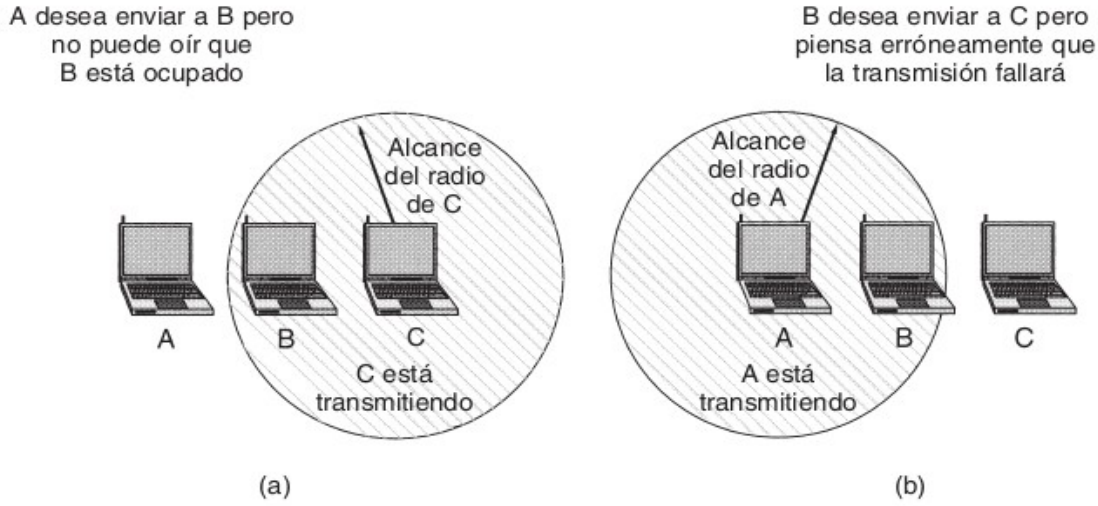


Figura 4-26. (a) El problema de la estación oculta. (b) El problema de la estación expuesta.

Como solución a estos problemas, IEEE 802.11 implementa dos métodos de funcionamiento. El primero llamado DCF (Función de Coordinación Distribuida), no utiliza ningún tipo de control central. Y el segundo llamado PCF (Función de Coordinación Puntual) utiliza la estación base para controlar toda la actividad en su celda.

Todas las implementaciones soportan DCF pero PCF es opcional.

Cuando se emplea DCF, 802.11 utiliza un protocolo llamado CSMA/CA (Colision Avoid). En este se utiliza tanto la detección del canal físico como la del canal virtual.

En el primero, cuando una estación quiere transmitir, detecta el canal. Si este esta desocupado comienza a transmitir la trama completa, la cual podría ser destruida en el receptor debido a interferencias. Si el canal esta ocupado,

espera hasta que este inactivo para empezar a transmitir. Si ocurre una colisión, se trata de transmitir la trama mas tarde.
El otro modo de operación se basa en MACAW y utiliza la detección del canal virtual, como en la imagen siguiente. Es esta caso se ve que A desea enviar a B, C es una estación que esta al alcance de A (y probablemente también de B) y D es una estación que esta dentro del alcance de B pero no de A. Cuando A quiere enviarle datos a B, A manda un RTS a B, en la que le pide permiso para enviarle la trama. B le concede el permiso, por ello emite un CTS. Ahora A envía sus datos y cuando termina B le manda un ACK avisándole que todo llego correctamente.
Desde el punto de vista de C y D, como ambos notan que se va a producir un intercambio, se imponen a si mismas que el canal esta ocupado, indicado por NAV (Vector de asignación de red). Esto es un temporizador que se desactivara cuando la transmisión haya terminado.

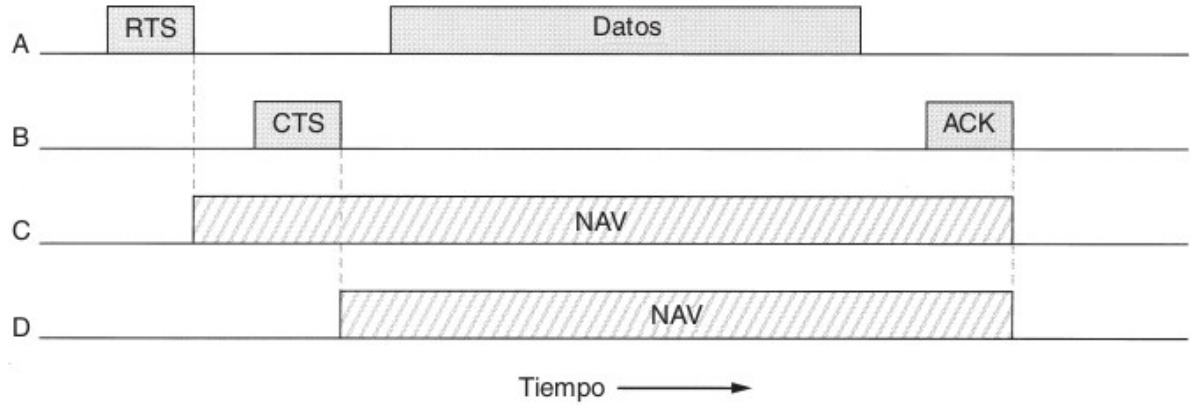


Figura 4-27. El uso de la detección de canal virtual utilizando CSMA/CA.

Como las redes inalámbricas son muy inestables y ruidosas debido a las interferencias de los hornos microondas, por lo tanto una trama con mayor longitud tendrá menos chances de llegar sana a su destino. Para solucionar este problema, 802.11 permite dividir las tramas en fragmentos, cada uno con su propia suma de verificación.
El emisor no podrá enviar el fragmento *k+1* si todavía no le llego la confirmación del *k*.
Una vez que se reservo el canal mediante un CTS y RTS pueden enviarse múltiples fragmentos en fila. Esto se llama ráfaga de fragmentos.

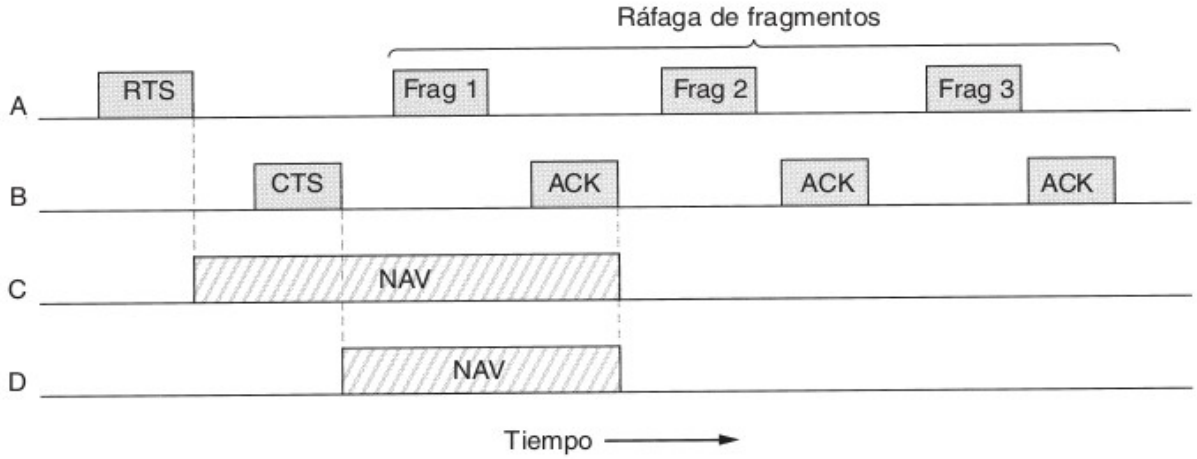
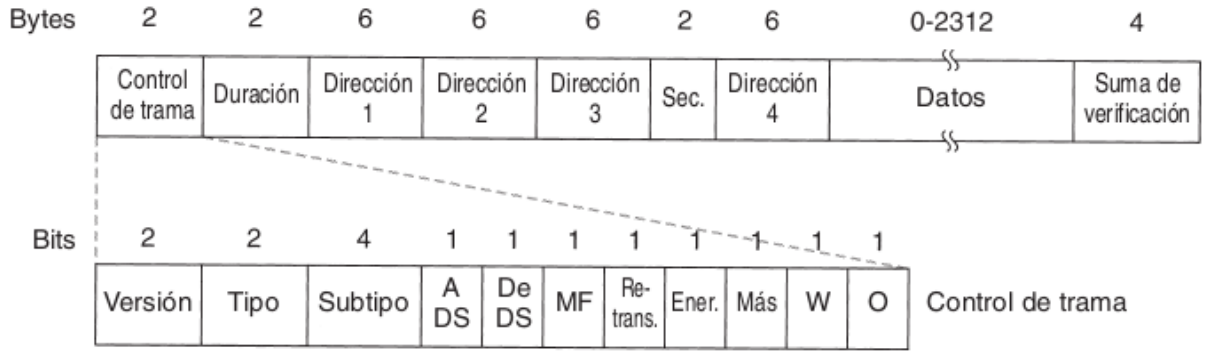


Figura 4-28. Una ráfaga de fragmentos.

Tramas en 802.11

- Tramas de datos: usadas para la transmisión de datos.
- Tramas de control: usadas para el control de acceso al medio (ACK,RTS,CTS).
- Tramas de gestión: se transmiten de la misma forma que una trama de datos pero solo contienen información sobre administración y tampoco son transportadas a capas superiores.



Control de trama:

- Versión: Indica la versión de protocolo de 802.11 MAC.
- Tipo: Indica el tipo de trama utilizado.
- Subtipo: Indica algún tipo de acción de cada una de las tramas.
- A DS y De DS: Indican si una trama va hacia o viene al sistema de distribución.
- Más Fragmentos: Cuando un paquete es fragmentado por la MAC, el segundo paquete y todos los restantes poseen este bit en 1.
- Retransmisión: Cualquier trama retransmitida tiene este bit en 1. Para evitar analizar tramas por duplicado.
- Administración de energía: es utilizado por la estación base para poner al receptor en estado de hibernación o sacarlo de tal estado.
- Más datos: Este bit es usado por el AP para indicar si hay mas tramas para esa estación.
- Privacidad inalámbrica: Este bit esta activado si la trama esta protegida por un protocolo de seguridad.
- Orden: De estar activado este bit, indica que las tramas y fragmentos serán transmitidos en estricto orden.

Duración: En la trama de datos indica cuanto tiempo ocuparan el canal la trama y su confirmación de recepción. En la trama de control, indica la duración del NAV.

Dirección 1: Es siempre la del receptor. Si A DS esta activado, sera la dirección del AP, sino la de la estación.
Dirección 2: Es siempre la del transmisor. Si De DS esta activado, representa la dirección del AP, sino la de la estación.
Dirección 3: Cuando el bit de De DS esta activo, representa la dirección de la fuente origen. Si A DS esta activado, representa la dirección de destino.
Dirección 4: Se usa en casos especiales cuando las tramas son transmitidas de un AP a otro.

Control de secuencias (Sec) : Este campo es usado para representar el orden de fragmentos dentro de una misma trama y para el reconocimiento de duplicados. Está formado por un número de fragmento y el número de secuencia.

Control de enlace lógico LLC

Especifica los mecanismos para el direccionamiento de estaciones conectadas al medio y para intercambio de datos entre usuarios de la red. Esta basado en el protocolo HDLC. Establece tres tipos de servicio: sin conexión y sin reconocimiento, con conexión, con reconocimiento y sin conexión.

WPAN

Se usan generalmente para conectar dispositivos periféricos, dos ordenadores, etc. La tecnología aplicada en estas redes procura hacer efectivo el uso de recursos. Se trataron de diseñar los protocolos mas simples y óptimos para cada necesidad.

- Bluetooth – 802.15.1: Velocidad máxima de 1 Mbps, el alcance puede variar, consume poca energía.
- HomeRF: Velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros. Este estándar se abandonó.
- Zigbee – 802.15.4: Muy bajo costo, bajo consumo de energía. Puede alcanzar una velocidad de 250 Kbps con un alcance máximo de 100 metros.
- Infrarrojas: tienen un alcance de pocos metros y velocidades bajas. Se utiliza ampliamente para aparatos electrónicos del hogar.

Bluetooth – 802.15.1

Funcionamiento.
Cada dispositivo tiene un microchip llamado transceptor que transmite y recibe en la frecuencia de 2.4 GHz. Cada dispositivo tiene una dirección única de 48 bits. Estos dispositivos se clasifican en clase 1,2 o 3 según su potencia de transmisión.
No hace falta que los dispositivos estén alineados y pueden incluso estar en habitaciones diferentes.

Clase	Potencia Máxima	Alcance
Clase 1	100 mW	100 m
Clase 2	2.5 mW	10 m
Clase 3	1 mW	1 m

Arquitectura

La unidad básica de un sistema Bluetooht es una piconet. Esta consta de un nodo maestro y hasta 7 nodos esclavos activos a una distancia de 10 metros.

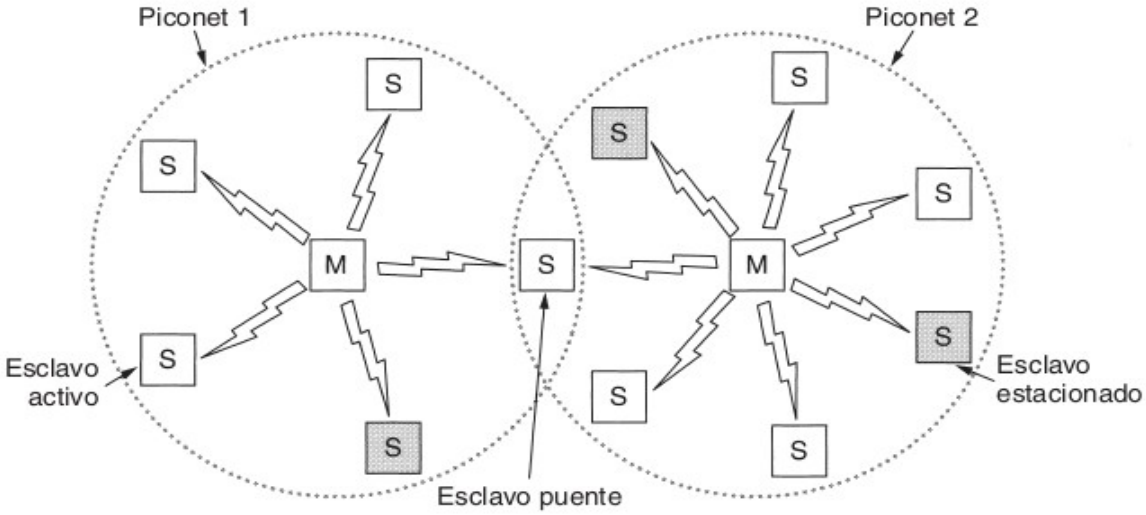


Figura 4-35. Dos piconets se pueden conectar para conformar una scatternet.

Puede haber hasta 255 nodos estacionados en la red. Lo unico que un nodo estacionado puede hacer es responder a una señal de activacion por parte del maestro.

En una misma sala se pueden encontrar varias piconets que pueden conectarse mediante un nodo puente y formar una scatternet.

Trama

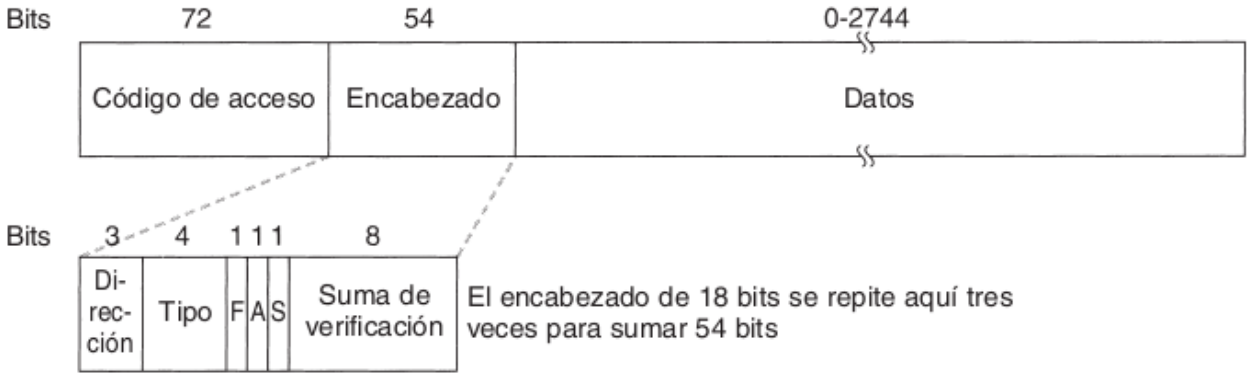


Figura 4-38. Trama de datos típica de Bluetooth.

Código de acceso: Identifica al maestro de cada piconet. Su propósito es que los esclavos que se encuentren en el rango de los dos maestros sepan que trafico esta destinado para ellos.

Encabezado: contiene los campos comunes de la subcapa MAC

Dirección: Permite identificar para cual de los 8 dispositivos activos esta dirigida la trama.

Tipo: Indica el tipo de trama, el tipo de corrección de errores que se utiliza en el campo de datos y cuantas ranuras de longitud tiene la trama.

F(Flow): Un esclavo pone este bit en 1 cuando su buffer esta lleno y no puede recibir mas datos.
A(Acknowledgement): Se utiliza para incorporar un ACK a la trama.
S(Secuence): Sirve para numerar las tramas con el propósito de detectar retransmisiones.

Este encabezado se repite tres veces. El receptor comprueba estas copias de cada bit, y si coinciden se acepta. De lo contrario se impone la opinión de la mayoría.

Pila de protocolos Bluetooh

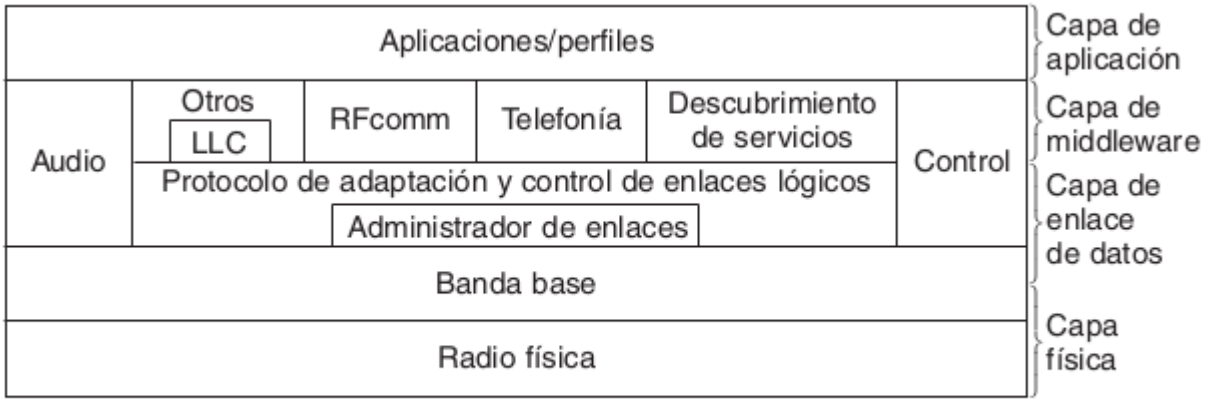


Figura 4-37. Versión 802.15 de la arquitectura de protocolos de Bluetooth.

Capa de radio Física: Translada los bits del esclavo al maestro o viceversa.

Capa de Banda Base: Es lo más parecido a una subcapa MAC. Transforma los bits en tramas. El maestro de cada piconet define una serie de ranuras de tiempo; los esclavos transmiten en las ranuras impares y los maestros en las pares. Las tramas se transmiten mediante enlaces de dos tipos:

- ACL (Asíncrono no orientado a la conexión): utilizado para el envío de datos conmutados en paquetes irregulares. Estos datos provienen de la capa L2CAP del emisor y van a esa misma capa pero del receptor. El trafico de ACL se entrega con "el mejor esfuerzo", no hay garantías. Si una trama se pierde se debe retransmitir. Un esclavo puede tener un solo ACL con su maestro.
- SCO (Síncrono Orientado a la conexión): utilizado para datos en tiempo real. Por la importancia del tiempo, las tramas nunca se retransmiten sino que utilizan la corrección de errores para darle una confiabilidad alta. Se asigna una ranura fija por cada dirección.

Administrador de enlace: Se encarga de sincronizar los positivos bluetooth para el control de la banda base. Establece la conexión, negociación de los parámetros y cambios en las políticas de enlace.
Posee algunas funciones sobre el control de la piconet , se encarga de establecer enlaces ACL o SCO y configurarlo. Cambien tiene funciones de seguridad, encargándose de la autenticación y el cifrado.

Capa de adaptación y control de enlace lógico: tiene tres funciones principales:

- Acepta paquetes de hasta 64KB y los divide en tramas para transmitirlo.

Luego las tramas se vuelven a unir en el otro extremo.
- Maneja la multiplexación y demultiplexación de paquetes. Además determina cual protocolo de las capas superiores lo manejara al paquete.
- Se encarga de la calidad de los requerimientos del servicio en el establecimiento del enlace y durante la operación normal. Durante el establecimiento de enlaces negocia el tamaño máximo de carga útil permitido, es decir controla el flujo.

VLAN (Virtual LAN)

Una VLAN es una LAN virtual. Puede interesarles a los administradores de red generarlas por ejemplo:
- Reflejar la estructura de la organización de la empresa.
- Seguridad.
- Utilización de las LANs (algunos sectores más que otros).
- Para evitar tormentas de difusión. Como la mayoría de las LANs soporta difusión, puede pasar que cuando las interfaces de red se averían empiezan a generar flujos interminables de tramas de difusión y se generan tormentas de difusión que provocan que las tramas ocupen toda la capacidad de la LAN y que las máquinas se atasquen procesando y descartando tramas difundidas.

Como físicamente es difícil modificar estructuras de LANs cada vez que se modifique la organización empresarial, y con el objetivo de lograr una mayor flexibilidad, los expertos en redes comenzaron a trabajar una forma de volver a cablear edificios enteros mediante software.
El concepto que surgió se denomina VLAN y además fue estandarizado por el comité 802.
Para configurar una red VLAN, el administrador decidirá: cuantas VLANs habrá, que computadoras habrá en cada VLAN, como se llamaran cada una de ellas.
Las VLANs se fundamentan en conmutadores especialmente diseñados para este propósito, aunque también podrían contar con algunos concentradores.
Para que estas funcionen correctamente, en los puentes o conmutadores, deben configurarse tablas que indicaran cuales VLANs se pueden acceder a través de que puertos