LA CAPA DE ENLACE DE DATOS

CUESTIONES DE DISEÑO DE LA CAPA DE ENLACE DE DATOS

Funciones de la capa de enlace de datos

La capa de enlace tiene que desempeñar varias funciones específicas, entre las que se incluyen:

1) Proporcionar una interfaz de servicio bien definida con la capa de red.
2) Manejar los errores de transmisión.
3) Regular el flujo de datos para que receptores lentos no sean saturados por emisores rápidos.

Para cumplir con estas metas, la capa de enlace de datos toma de la capa de red los paquetes y los encapsula en **tramas** para transmitirlos. Cada trama contiene un encabezado, un campo de carga útil (payload) para almacenar el paquete y un terminador o final. El manejo de las tramas es la tarea primordial de la capa de enlace de datos.

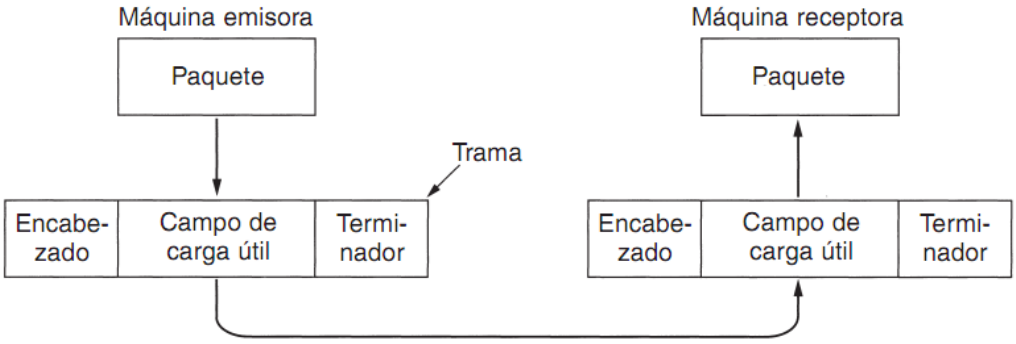


Figura 3-1. Relación entre los paquetes y las tramas.

Servicios proporcionados a la capa de red

La función de la capa de enlace de datos es suministrar servicios a la capa de red. El servicio principal es transferir datos de la capa de red en la máquina origen a la capa de red en la máquina destino. La transmisión real se realiza en la capa física, pero es más fácil pensar en términos de 2 procesos de la capa de enlace de datos que se comunican usando un protocolo de enlace de datos.

La capa de enlace de datos puede ofrecer distintos servicios:

a) Servicio no orientado a la conexión no confiable: la máquina de origen envía tramas independientes a la máquina destino sin pedir que ésta confirme la recepción. No se establece ninguna conexión de antemano, ni se libera después. Este tipo de servicios es apropiado cuando la tasa de errores es baja y para el tráfico en tiempo real.

b) Servicio no orientado a la conexión confiable: no se establece la conexión de antemano, pero se confirma de manera individual la recepción de cada trama enviada. De esta manera, el emisor sabe si la trama ha llegado bien o no. Si no ha llegado en un tiempo especificado puede enviarse nuevamente. Es posible que una confirmación de recepción perdida cause que una trama se envíe varias veces y por lo tanto, que se reciba varias veces. Este servicio es útil en canales inestables, como los de sistemas inalámbricos. Proporcionar confirmaciones de recepción en la capa de enlace de datos es sólo una optimización, no un requisito.

c) Servicio orientado a la conexión confiable: se establece una conexión entre las máquinas de origen y destino antes de transmitir los datos. Cada trama enviada está numerada (números de secuencia) y la capa de enlace garantiza que cada trama llegará a destino sólo una vez, y en el orden adecuado. Las transferencias tienen tres fases:

- La conexión se establece haciendo que ambos lados inicialicen las variables y los contadores necesarios para seguir la pista de las tramas que han sido recibidas y las que no.
- Se transmiten una o más tramas.
- La conexión se cierra y libera las variables, los búferes y otros recursos utilizados para mantener la conexión.

Entramado

A fin de proporcionar servicios a la capa de red, la capa de enlace de datos debe utilizar los servicios que la capa física le proporciona. La capa física acepta un flujo de bits puros e intenta entregarlo al destino. No se garantiza que el flujo de bits esté libre de errores. Es responsabilidad de la capa de enlace de datos detectar, y de ser necesario, corregir los errores.

Veremos 4 métodos:

Conteo de caracteres

Se trata de un campo en el encabezado para especificar el número de caracteres en la trama. Cuando la capa de enlace de la máquina destino ve la cuenta de caracteres, sabe cuántos le siguen y por ende dónde finaliza dicha trama. Esta cuenta puede alterarse por un error de transmisión y así, el receptor pierde la sincronía y será incapaz de localizar el inicio de la siguiente trama. Incluso si el destino sabe que la trama está mal porque la suma de verificación es incorrecta, no tiene forma de saber dónde comienza la siguiente trama.

Bandera, con relleno de byte

Cada trama inicia y termina con bytes especiales (banderas: FLAGS). Dos banderas continuas indican el fin de una trama e inicio de la siguiente. Puede ocurrir que estas banderas (patrones de 8 bits) aparezcan en los datos, e interferir en el entramado. Como solución, se agrega un byte de escape (ESC) justo antes de cada bandera accidental en los datos. La capa de enlace de datos del lado del receptor quita el byte de escape antes de entregar los datos a la capa de red. Por lo tanto, una bandera de entramado puede distinguirse de una en los datos por la ausencia o presencia del byte ESC que la antecede. Si un byte de escape aparece en medio de los datos, también se rellena con un byte ESC. Esta técnica se llama relleno de caracteres y está fuertemente atada a los caracteres de 8 bits.

Bandera, con relleno de bit

Permite que las tramas de datos contengan un número arbitrario de bits y admite códigos de caracteres con un número arbitrario de bits por carácter. Funciona de la siguiente manera: cada trama comienza y termina con "01111110". Cada vez que la capa de enlace emisora encuentra un patrón de 5 unos consecutivos en los datos inserta un bit 0 en el flujo de bits saliente. Cuando el receptor ve cinco bits 1 de entrada consecutivos, seguidos de un bit 0, automáticamente extrae (borra) el bit 0 de relleno. Si los datos de usuario contienen el patrón indicador "01111110", este se transmite como "011111010", pero se almacena en la memoria del receptor como "01111110". Con el relleno de bits, el límite entre las dos tramas puede ser reconocido sin ambigüedades mediante el patrón de banderas.

Estas técnicas de relleno de byte o bit son transparentes a la capa de red.

Violaciones de codificación de la capa física

Se aplica a las redes en las que la codificación en el medio físico contiene cierta redundancia. Por ejemplo, algunas LANs codifican un bit de datos usando dos bits físicos. Un bit 1 es un par alto-bajo, y un bit 0 es un par bajo-alto. El esquema implica que cada bit de datos contiene una transición a medio camino, lo que hace fácil para el receptor localizar los límites de los bits. Las combinaciones alto-bajo y bajo-alto no se usan para datos, pero en algunos protocolos se utilizan para delimitar tramas.

Muchos protocolos de enlace de datos usan, por seguridad, una combinación de cuenta de caracteres con uno de los otros métodos.

Control de errores

La manera normal de asegurar la entrega confiable y en forma ordenada de datos al receptor es proporcionando realimentación al emisor sobre lo que ocurre del otro lado de la línea. Por lo general, el protocolo exige que el receptor regrese tramas de control especiales que contengan confirmaciones de recepción positivas o negativas de las tramas que llegan. Si el emisor recibe una confirmación de recepción positiva sabe que la trama llegó correctamente. Por otra parte, una confirmación de recepción negativa significa que algo falló y que la trama debe enviarse otra vez.

Una complicación adicional surge con la desaparición de una trama completa. En este caso, el receptor no reaccionará en absoluto y el emisor se quedará esperando eternamente una confirmación de recepción. Esta posibilidad se maneja introduciendo temporizadores en la capa de enlace de datos. Cuando el emisor envía una trama, por lo general también inicia un temporizador. Generalmente la trama se recibirá de manera correcta y la confirmación de recepción llegará antes de que el temporizador expire, en cuyo caso se cancelará.

Si la trama o la confirmación de recepción se pierden, el temporizador expirará, alertando al emisor sobre un problema potencial. La solución es enviar de nuevo la trama. Para que el receptor no acepte la misma trama dos veces o más, generalmente es necesario asignar número de secuencia a las tramas que salen, a fin de que el receptor pueda distinguir las retransmisiones de los originales.

Control de flujo

Otro tema de diseño importante en la capa de enlace de datos es qué hacer con un emisor que quiere transmitir tramas de manera sistemática y a mayor velocidad que aquella con que puede aceptarlos el receptor. Aunque la transmisión esté libre de errores, en cierto punto el receptor no será capaz de manejar las

tramas conforme lleguen y comenzará a perder algunas.
Métodos de control de flujo:
Control de flujo basado en retroalimentación: el receptor regresa información al emisor autorizándolo para enviar más datos o indicándole su estado. El receptor puede decirle al emisor cuántas tramas puede enviarle, antes de enviarle una confirmación de recepción.
Control de flujo basado en tasa: el protocolo tiene un mecanismo integrado que limita la tasa a la que el emisor puede transmitir los datos, sin recurrir a retroalimentación por parte del receptor.

DETECCION Y CORRECCION DE ERRORES
Los errores en una transmisión pueden aparecer en ráfagas o de manera independiente. Los diseñadores de redes han diseñado 2 estrategias principales para manejar errores:
a) Incluir suficiente información redundante en cada bloque de datos transmitido para que el receptor pueda deducir lo que debió ser el símbolo transmitido. Esta técnica usa códigos de corrección de errores (Por ejemplo, código Hamming).
b) Incluir sólo suficiente redundancia para permitir que el receptor sepa que ha ocurrido un error y solicite una retransmisión. Esta técnica usa códigos de detección de errores (Por ejemplo Suma de verificación – CRC; Paridad).
En los canales que son altamente confiables es más económico usar códigos de detección de errores y simplemente retransmitir los bloques defectuosos que surgen ocasionalmente. En los canales que causan muchos errores es mejor agregar redundancia suficiente a cada bloque para que el receptor pueda descubrir cuál era el bloque original transmitido, en lugar de confiar en una retransmisión, que también podría tener errores.

Supongamos que una trama tiene m bits de datos y r bits de redundancia o verificación. La unidad de n=m+r bits se llama *palabra codificada*.
Distancia de hamming: cantidad de posiciones en que difieren 2 palabras codificadas. Las propiedades de detección y corrección de errores dependen de su distancia de hamming.

- Para detectar d errores se necesita un código con distancia d+1. O sea, agregarle 1 bit de redundancia. Ejemplo:
  Bit de paridad: se envía 1011010, agregando 1 bit de paridad:
  - Par: 10110100
  - Impar: 10110101

  Un código con 1 bit de paridad tiene una distancia de 2, por lo que cualquier error de 1 bit produce una palabra con paridad equivocada.
- Para corregir d errores, se necesita un código con distancia 2d+1.
  Ejemplo: Sea el código de 4 palabras válidas:
  0000000000; 0000011111; 1111100000; 1111111111. → Distancia de hamming=5
  Entonces, puede corregir errores dobles, 5=2d+1 → d=2.

Códigos de corrección de errores
Hamming
Código para corregir errores de 1 bit: los bits de la palabra codificada se numeran en forma consecutiva comenzando por el bit 1 a la izquierda. Los bits que son potencia de 2 (1, 2, 4, 8, 16, etc.) son de verificación. El resto se rellena con los m bits de datos. Cada bit de verificación obliga a que la paridad de un grupo de bits, incluyéndose, sea par (o impar). Un bit puede estar incluido en varios cálculos de paridad. Para ver a cuál bit de verificación contribuye el bit de datos en la posición k, se reescribe k como suma de potencias de 2.
Cuando llega una palabra codificada, el receptor inicializa a 0 un contador y luego examina cada bit de verificación para ver si tiene paridad correcta. Si no, suma k al contador. Al finalizar, si el contador es 0 la palabra se acepta como válida. Si el contador es diferente de cero, contiene el número del bit incorrecto. Por ejemplo, si los bits de verificación 1, 2 y 8 tienen errores, el bit invertido es el 11, pues es el único comprobado por los bits 1, 2 y 8.
Código para corregir errores de ráfaga: se dispone como matriz una secuencia de k palabras codificadas consecutivas, una por fila. Para corregir errores en ráfaga, los datos deben transmitirse una columna a la vez, comenzando por la columna del extremo izquierdo. Cuando los k bits han sido enviados, se envía a segunda columna, y así sucesivamente. Cuando la trama llega al receptor, la matriz se reconstruye, una columna a la vez. Si ocurre un error en ráfaga de longitud k, cuando mucho se habrá afectado 1 bit de cada una de las k

palabras codificadas; sin embargo, el código de Hamming puede corregir un error por palabra codificada, así que puede restaurarse la totalidad del bloque. Este método usa kr bits de verificación para inmunizar bloques de km bits de datos contra un solo error en ráfaga de longitud k o menos.

Código de detección de errores

Suma de verificación: consiste en agrupar el mensaje a transmitir en tramas de longitud determinada y asociar cada cadena con un número entero (decimal). Después se suma el valor de todas esas tramas y se agrega el resultado al mensaje a transmitir pero cambiado de signo.
Finalmente el receptor suma todas las cadenas/tramas, y si el resultado es 0, no hay error.
Código polinomial o CRC: Código que usa la aritmética modular para detectar mayor cantidad de errores. Está basado en el tratamiento de cadenas de bits como polinomios con coeficientes 0 y 1. Una trama de k bits se considera como la lista de coeficientes del polinomio con k términos que va desde x^{k-1} a x^0; tal polinomio es de grado k-1. El emisor y receptor deben acordar por adelantado un polinomio generador que tiene como propiedad minimizar la redundancia.
Cálculos que realiza el equipo transmisor para calcular su CRC:

- Agrega tantos ceros a la derecha del mensaje original como el grado del polinomio generador, generando un nuevo polinomio.
- Divide el mensaje "nuevo" entre el polinomio generador.
- El resto que se obtiene se suma al mensaje "nuevo".
- Se envía el resultado obtenido.

El equipo receptor debe comprobar el código CRC para ver si no hubo errores: divide el código recibido entre el polinomio generador y comprueba el resto. Si es 0, es correcto. Si no, se debe reenviar el mensaje.

PROTOCOLOS ELEMENTALES DE ENLACE DE DATOS

Supuestos implícitos del modelo de comunicaciones:

- En las capas física, de enlace y de red hay procesos independientes que se comunican pasando mensajes de un lado a otro.
- La máquina A desea mandar un flujo de datos a B usando un servicio confiable orientado a la conexión. B también quiere mandar un flujo de datos a A simultáneamente.
- La capa de red está siempre disponible.
- Nunca se entrega a la capa de red el encabezado de una trama para mantener completamente separados el protocolo de red y el de enlace de datos.
- Formato de una trama (frame):
  - kind: indica si hay datos en la trama.
  - seq, ack: número de secuencia y confirmaciones de recepción respectivamente.
  - info (de una trama de datos): contiene sólo un paquete.
- Relación paquete-trama: la capa de red construye un paquete tomando un mensaje de la capa de transporte, y agregándole el encabezado de la capa de red. Este paquete se pasa a la capa de enlace de datos para incluirlo en el campo info de una trama saliente. Cuando ésta llega a destino la capa de enlace extrae de ella el paquete y luego, lo pasa a la cada de red.
- La capa de red puede habilitarse y deshabilitarse. Cuando la capa de enlace habilita la de red, ésta tiene permitido interrumpir cuando tenga que enviar un paquete. Cuando una capa de red está inhabilitada, no puede causar tales eventos (si no hay espacio en el buffer emisor, evita que se sature).
- Los números de secuencia van de 0 a MAX_SEQ y avanzan circularmente.

Un protocolo simplex sin restricciones (Protocolo 1) – UTOPIA.

Los datos se transmiten sólo en una dirección; las capas de red tanto del emisor como del receptor siempre están listas, el tiempo de procesamiento puede ignorarse, hay espacio infinito de búfer y el canal de comunicación entre las capas de enlace de datos nunca tiene problemas ni pierde tramas.
El protocolo consiste en dos procedimientos diferentes, uno emisor y otro receptor. El emisor se ejecuta en la capa de enlace de datos de la máquina de origen y el receptor se ejecuta en la capa de enlace de datos de la máquina de destino. El único tipo de evento posible es la llegada de una trama sin daños.
El emisor está en un ciclo while infinito que sólo envía datos a la línea tan rápidamente como puede. El cuerpo del ciclo consiste en tres acciones:

- Obtener un paquete de la capa de red.
- Construir una trama de salida.
- Enviar la trama a su destino.

El receptor inicialmente espera que algo ocurra, siendo la única posibilidad la llegada de una trama sin daños. En algún momento la trama llega, se elimina del búfer de hardware y se coloca en una variable para que el código receptor pueda obtenerla. Por último, la parte de datos se pasa a la capa de red y la capa de enlace se retira para esperar la siguiente trama.

Protocolo simplex de parada y espera (Protocolo 2)
Los mismos supuestos que el protocolo anterior pero con espacio finito de búfer del receptor y capacidad finita de procesamiento de datos.
Con este protocolo se trata de evitar que el emisor sature de datos al receptor enviando datos a mayor velocidad de la que éste último puede procesarlos. La solución es hacer que el receptor proporcione retroalimentación al emisor.
Tras haber pasado un paquete a su capa de red, el receptor regresa al emisor una pequeña trama ficticia, que autoriza al emisor para transmitir la siguiente trama. Tras haber enviado una trama, el protocolo exige que el emisor espere hasta que llegue la pequeña trama ficticia (la confirmación de recepción).
Aunque el tráfico de datos es simplex, las tramas viajan en ambas direcciones. Este protocolo implica una alternancia estricta de flujo: 1º emisor, después receptor, 1º emisor, después receptor, 1º emisor, después receptor, etc. Por lo que sería suficiente con un canal semiduplex.
Funciona igual que el protocolo anterior, solo que ahora el emisor deberá esperar a recibir la trama de confirmación para poder obtener el siguiente paquete a enviar.

Protocolo simplex para un canal con ruido (Protocolo 3)
Consideremos un canal de comunicación normal que comete errores. Las tramas pueden llegar dañadas o perderse por completo. Si la trama está dañada, el hardware lo detecta cuando calcula la suma de verificación (CRC). Si la trama está dañada pero pese a ello la suma de verificación es correcta, el protocolo puede fallar.
Usamos el protocolo 2 con un temporizador. Cuando se envía cada trama, el emisor inicia un temporizador que se ajusta de modo que expire cuando haya transcurrido un intervalo suficiente para que la trama llegue a destino, se procese y regrese la confirmación de recepción. Si la confirmación de recepción no llega antes de que el temporizador expire, el emisor la retransmite.
Puede ocurrir que la trama de confirmación se pierda y el dato ya fue aceptado y entregado a la capa de red, entonces expirará el temporizador y se reenviará la trama llegando duplicada a la capa de red. Solucionamos esto poniendo un número de secuencia en el encabezado de cada trama que envía la máquina emisora, y en cada instante de tiempo, el receptor esperará un número de secuencia determinado. Basta con un número de secuencia de 1 bit (0 o 1), ya que la única ambigüedad es entre una trama y su antecesor o sucesor inmediato. Se supone que si m+2 llegó confirmada también llegó m+1 y m.
Cuando llega una trama al receptor, su número de secuencia se verifica para ver si es duplicado, si no lo es, se acepta, se pasa a la capa de red y se genera la confirmación de recepción. Cualquier trama que contenga un número de secuencia equivocado se rechaza como duplicado.
Diferencia con los protocolos 1 y 2: tanto el emisor como el receptor tienen una variable cuyo valor se recuerda mientras la capa de enlace está en estado de espera. El emisor recuerda el número de secuencia de la siguiente trama a enviar, y el receptor el de la siguiente trama esperada.
Los duplicados y las tramas dañadas no se pasan a la capa de red.

PROTOCOLOS DE VENTANA CORREDIZA
Se usa un solo circuito para enviar datos en ambas direcciones. Las tramas de datos de A a B se mezclan con las confirmaciones de recepción de A a B. El receptor puede saber si la trama es de datos o de confirmación de recepción analizando el campo kind en el encabezado de una trama de entrada.
Cuando llega una trama de datos, en lugar de enviar inmediatamente una trama de control independiente, el receptor espera hasta que la capa de red le pase el siguiente paquete. La confirmación de recepción se anexa a la trama de datos de salida (usando el campo ack del encabezado de la trama). De esta manera la confirmación viaja gratuitamente en la siguiente trama de datos de salida.
La técnica de retardar temporalmente las confirmaciones de recepción para que puedan viajar en la siguiente trama de datos de salida se conoce como superposición (piggybacking).
Ventajas:

- Mejor aprovechamiento del ancho de banda disponible del canal.
- Enviar menos tramas implica menos interrupciones y menos segmentos de búfer en el receptor.

Para manejar el tiempo que debe esperar un paquete para superponer la confirmación de recepción, la capa de enlace de datos debe recurrir a un esquema particular, como esperar un número fijo de milisegundos. Si

llega rápidamente un nuevo paquete, la confirmación de recepción se superpone a él; si no ha llegado ningún paquete nuevo al final de este periodo, la capa de enlace de datos manda una trama de confirmación de recepción independiente.

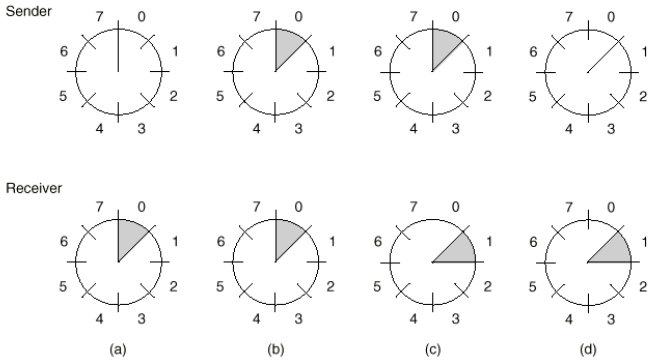
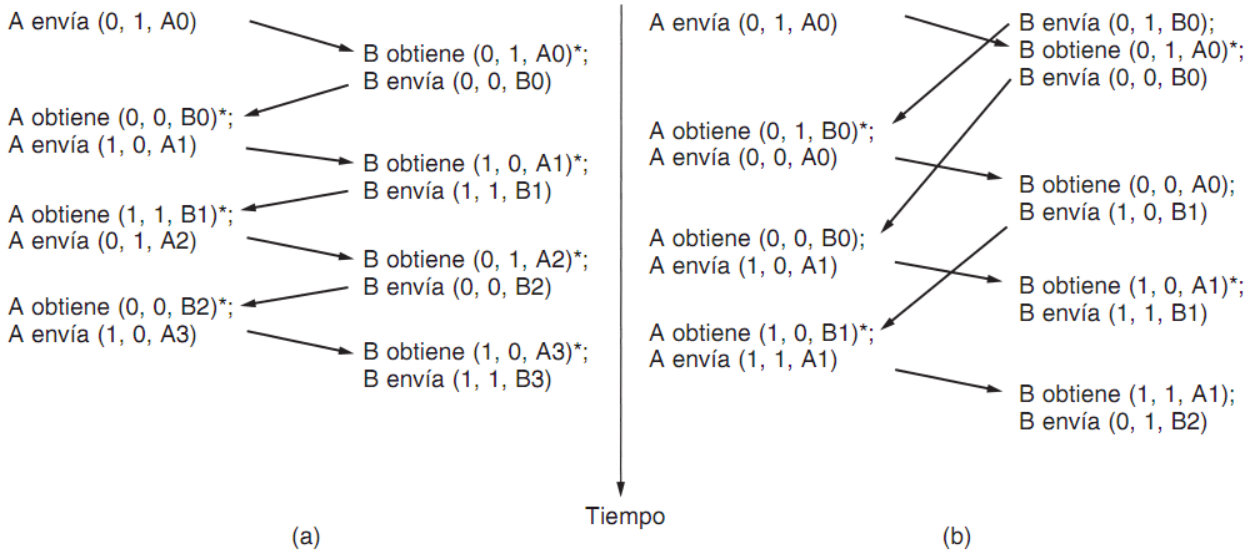


Fig. 3-12. A sliding window of size 1, with a 3-bit sequence number. (a) Initially. (b) After the first frame has been sent. (c) After the first frame has been received. (d) After the first acknowledgement has been received.

Funcionamiento general: en cualquier instante el emisor mantiene un grupo de números de secuencias que corresponde a las tramas que tiene permitido enviar. Estas tramas caen dentro de la **ventana emisora**. El receptor mantiene una **ventana receptora** correspondiente al grupo de tramas que tiene permitido aceptar. La ventana del emisor y la del receptor no necesitan tener los mismos límites inferior y superior, ni siquiera el mismo tamaño.
El protocolo debe entregar los paquetes a la capa de red del destino en el mismo orden en que se pasaron a la capa de enlace de datos de la máquina emisora.
Los números de secuencia en la ventana del emisor representan tramas enviadas, o que pueden ser enviadas, pero cuya confirmación de recepción aún no se ha confirmado. Cuando llega un paquete nuevo de la capa de red, se le da el siguiente número de secuencia, y el extremo superior de la venta avanza en uno. Al llegar una confirmación de recepción, el extremo inferior avanza en uno. La ventana mantiene siempre una lista de tramas sin confirmación de recepción.
Si el tamaño de la ventana es n, el emisor necesita n búferes para contener las tramas sin confirmación de recepción. Si la ventana llega a crecer a su tamaño máximo, la capa de enlace de datos emisora deberá hacer que la capa de red se detenga hasta que se libere un búfer.
La ventana de la capa de enlace de datos receptora corresponde a las tramas que puede aceptar. Toda trama que caiga fuera de la ventana se descartará. Cuando se recibe una trama cuyo número de secuencia es igual al extremo inferior de la ventana, se pasa a la capa de red, se genera la confirmación de recepción y se avanza la ventana en uno. La ventana del receptor conserva siempre el mismo tamaño inicial. Si el tamaño de la ventana es 1, la capa de enlace de datos sólo acepta tramas en orden. Con ventanas más grandes esto no es así. La capa de red, en contraste, siempre recibe los datos en el orden correcto.
En todos los protocolos de ventana corrediza, cada trama contiene un número de secuencia que va de 0 hasta 2^n-1, donde n es la cantidad de bits del número de secuencia.

Un protocolo de ventana corrediza de 1 bit (Protocolo 4)
El tamaño máximo de ventana es de 1 bit. Este protocolo usa parada y espera ya que envía una trama y espera su confirmación antes de transmitir la siguiente.
Normalmente una de las 2 capas de enlace comienza a transmitir. La máquina que arranca obtiene el primer paquete de la capa de red, construye una trama a partir de él y la envía. Al llegar esta (o cualquier) trama, la capa de enlace de la máquina receptora revisa el número de secuencia para saber si es duplicado. Si la trama es la esperada se pasa a la capa de red y la ventana del receptor se recorre hacia arriba.
El campo de confirmación de recepción contiene el número de la última trama recibida sin error. Si es igual al número de secuencia de la trama que está tratando de enviar el emisor, éste sabe que ha terminado con la trama almacenada en el búfer y que puede obtener el siguiente paquete de su capa de red. Si el número de secuencia no concuerda, debe continuar intentando enviar la misma trama. Por cada trama que se recibe, se regresa una.
Si ambas máquinas (A y B) comienzan a transmitir de manera simultánea, la mitad de las tramas contienen duplicados, aún cuando no hay errores de transmisión.



Dos escenarios para el protocolo 4. (a) Caso normal.
(b) Caso anormal. La notación es (secuencia, confirmación de recepción, número de paquete).
Un asterisco indica el lugar en que una capa de red acepta un paquete.

Protocolo que usa retroceso N (Protocolo 5)

Cuando el tiempo de transmisión requerido para que una trama llegue al receptor, más el necesario para que la confirmación de recepción regrese es prolongado, puede tener implicaciones importantes para la eficiencia del aprovechamiento del ancho de banda.

Este protocolo consiste en permitir que el emisor envíe hasta w tramas antes de bloquearse. Eligiendo correctamente el w, el emisor podrá transmitir tramas continuamente durante un tiempo igual al tiempo de tránsito de ida y vuelta sin llenar la ventana.

El producto del ancho de banda por el retardo de ida y vuelta indica cuál es la capacidad del canal, el emisor necesita la capacidad de llenarlo sin detenerse para poder funcionar con una eficiencia máxima.

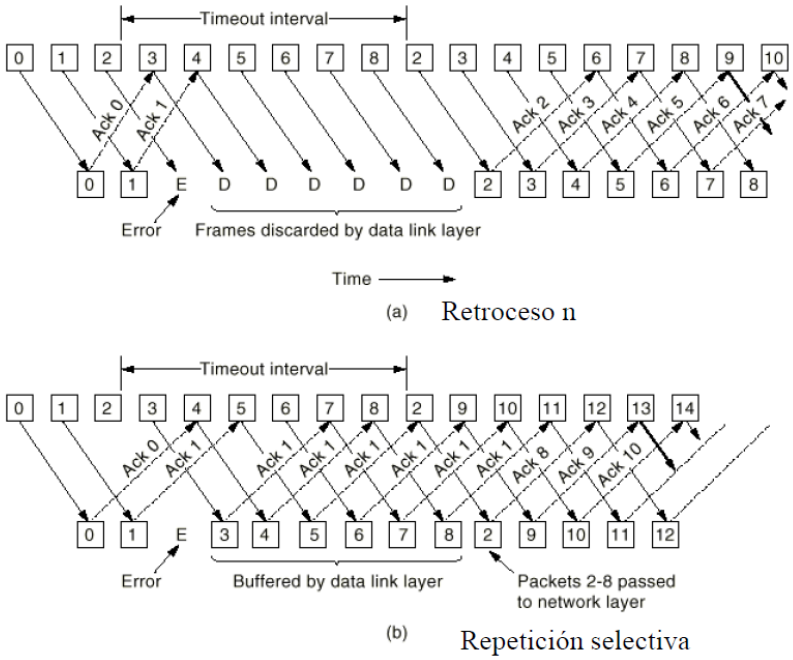
Esta técnica se llama canalización. Si la capacidad del canal es de b bps, el tamaño de la trama de l bits y el tiempo de propagación de ida y vuelta R segundos, entonces el tiempo requerido para transmitir una sola trama es de l/b segundos.

El envío de tramas en canalización por un canal de comunicación inestable presenta problemas serios. Si una trama a la mitad de una serie larga se daña o se pierde, llegarán grandes cantidades de tramas sucesivas al receptor antes de que el emisor se entere de que algo anda mal. Cuando llega una trama dañada al receptor debe descartarse, pero ¿qué debe hacerse con las tramas correctas que le siguen? Recuerde que la capa de enlace de datos receptora está obligada a entregar los paquetes a la capa de red en secuencia.

Para manejar los errores durante la canalización podemos usar una técnica llamada **retroceso n**. Consiste en que el receptor simplemente descarte todas las tramas subsecuentes, sin enviar confirmaciones de recepción para las tramas descartadas. Esta estrategia corresponde a una ventana de recepción de tamaño 1. La capa de enlace de datos se niega a aceptar cualquier trama excepto la siguiente que debe entregar a la capa de red. Si la ventana del emisor se llena antes de terminar el temporizador, el canal comenzará a vaciarse. En algún momento, el emisor terminará de esperar y retransmitirá en orden todas las tramas cuya recepción aún no se ha confirmado, comenzando por la dañada o perdida. Esta estrategia puede desperdiciar bastante ancho de banda si la tasa de errores es alta.

Otra estrategia general para el manejo de errores cuando las tramas se colocan en canalizaciones se conoce como **repetición selectiva**. Se descarta una trama dañada recibida, pero las tramas recibidas en buen estado después de ésa se almacenan en el búfer. Cuando el emisor termina, sólo la última trama sin confirmación se retransmite. Si la trama llega correctamente, el receptor puede entregar a la capa de red, en secuencia, todas las tramas que ha almacenado en el búfer. La repetición selectiva con frecuencia se combina con el hecho de que el receptor envíe una confirmación de recepción negativa (NAK) cuando detecta un error. Las confirmaciones de recepción negativas estimulan la retransmisión antes de que el temporizador correspondiente expire, mejorando el rendimiento.

La repetición selectiva corresponde a una ventana del receptor mayor que 1. Cualquier trama dentro de la ventana puede ser aceptada y mantenida en el búfer hasta que todas las que le preceden hayan sido entregadas a la capa de red. Esta estrategia puede requerir cantidades grandes de memoria en la capa de enlace de datos si la ventana es grande.



Canalización y recuperación de un error. (a) Efecto de un error cuando el tamaño de la ventana del receptor es 1. (b) Efecto de un error cuando el tamaño de la ventana del receptor es grande.

Dado que un emisor puede tener que retransmitir en un momento dado todas las tramas no confirmadas, debe retener todas las tramas retransmitidas hasta saber con certeza que han sido aceptadas por el receptor. Al llegar una confirmación de recepción para la trama n, las tramas n-1, n-2, y demás, se confirman automáticamente. Esta propiedad es importante cuando algunas tramas previas portadoras de confirmaciones de recepción se perdieron o dañaron.

Tamaño de ventana:

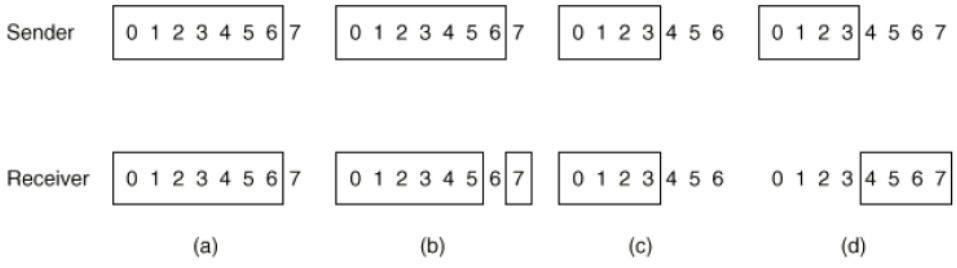
- Retroceso n: *Número de secuencia –1*
- Repetición selectiva: *Número de secuencia/2*

Protocolo que usa repetición selectiva (Protocolo 6)

Se permite que el receptor acepte y coloque en búferes las tramas que siguen a una trama dañada o perdida.

En este protocolo, tanto el emisor como el receptor mantienen una ventana de números de secuencia aceptables. El tamaño de la ventana del emisor comienza en 0 y crece hasta un máximo predefinido MAX_SEQ. La ventana del receptor, en cambio, siempre es de tamaño fijo e igual a MAX_SEQ. El receptor tiene un búfer reservado para cada número de secuencia en su ventana fija. Cada búfer tiene un bit asociado que indica si está lleno o vacío. Cuando llega una trama, su número de secuencia es revisado para ver si cae dentro de la ventana. De ser así, y no haya sido recibida aún, se acepta y almacena.

La recepción secuencial introduce ciertos problemas:



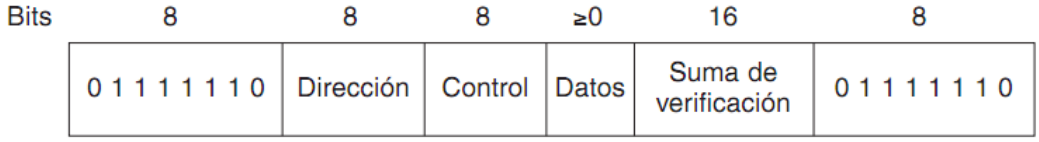
(a) situación original con una ventana de tamaño 7.
(b) después de que se han enviado y recibido siete tramas, pero su recepción no se ha confirmado.
(c) situación inicial con un tamaño de ventana 4.
(d) después de que se han enviado y recibido cuatro tramas, pero su recepción no se ha confirmado.

La esencia del problema es que una vez que el receptor ha avanzado su ventana, el nuevo intervalo de números de secuencias válidos se superpone con el anterior. Para evitar esto, el tamaño máximo de la ventana debe ser menos de la mitad del intervalo de los números de secuencia.

EJEMPLOS DE PROTOCOLOS DE ENLACE DE DATOS

HDLC – Control de enlace de datos de alto nivel

Este protocolo y todos sus antecesores y sucesores (SDLC → ADCCP → HDLC → LAP → LAPB) se basan en un mismo principio: todos son orientados a bits y usan el relleno de bits para lograr la transparencia de los datos. Todos los protocolos orientados a bits utilizan la siguiente estructura de trama:



Formato de trama para protocolos orientados a bits.

El campo de *Dirección* es de importancia primordial en las líneas con múltiples terminales ya que sirve para identificar una de las terminales. En líneas punto a punto a veces se usan para distinguir los comandos de las respuestas.

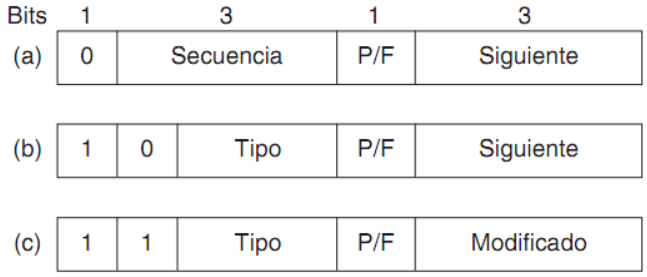
El campo de *Control* se usa para números de secuencia, confirmaciones de recepción y otros.

El campo *Datos* puede contener cualquier información y una longitud arbitraria. A mayor tamaño, menos eficiencia tiene la suma de verificación.

La trama está delimitada por otra secuencia de bandera "01111110". La trama mínima contiene 3 campos y un total de 32 bits y excluye banderas a ambos lados.

El campo de *Suma de verificación* es un código de redundancia cíclica.

Hay 3 tipos de tramas: de información, de supervisión y no numeradas.



Campos de control de (a) trama de información
(b) trama de supervisión (c) trama no numerada.

El protocolo emplea una ventana corrediza, con un número de secuencia de 3 bits. El campo *Secuencia* es el número de secuencia de la trama. El campo *Siguiente* es una confirmación de recepción superpuesta. Todos los protocolos se apegan a la convención de que, en lugar de superponer el número de la última trama recibida correctamente, usan el número de la primera trama no recibida.

El bit *P/F* significa Sondeo/Final (Poll/Final). Cuando se usa como *P*, la computadora está invitando a la terminal a enviar datos. Todas las tramas enviadas por la terminal, excepto la última, tienen el bit *P/F* establecido en *P*. El último se establece en *F*.

Los diferentes tipos de tramas de supervisión se distinguen por el campo *Tipo*:

- Tipo 0: "Receive ready". Trama de confirmación de recepción que sirve para indicar la siguiente trama esperada. Se usa cuando no hay tráfico de regreso.
- Tipo 1: "Reject". Trama de confirmación de recepción negativa. Sirve para indicar que se detectó un error. El campo Siguiente indica la primera trama en la secuencia que no se ha recibido de forma correcta.
- Tipo 2: "Receive not ready" (receptor no listo). Reconoce todas las tramas hasta, pero sin incluir siguiente, le dice al emisor que detenga el envío.
- Tipo 3: "Selective reject". Solicita la retransmisión de sólo la trama especificada.

Las tramas de control no numeradas se usan para propósitos de control, aunque también pueden servir para llevar datos cuando se solicita un servicio no confiable sin conexión.

Las tramas de control pueden perderse o dañarse igual que las de datos, por lo que también debe confirmarse su recepción. Para esto se usa una trama de control especial llamada UA (confirmación de recepción no numerada). Solo puede estar pendiente una trama de control por lo que nunca hay ambigüedades sobre la trama de control que está siendo confirmada.

La capa de enlace de datos en Internet

Internet consiste en un conjunto de máquinas individuales (host y enrutadores) y la infraestructura de comunicación que las conecta.

PPP – Protocolo punto a punto

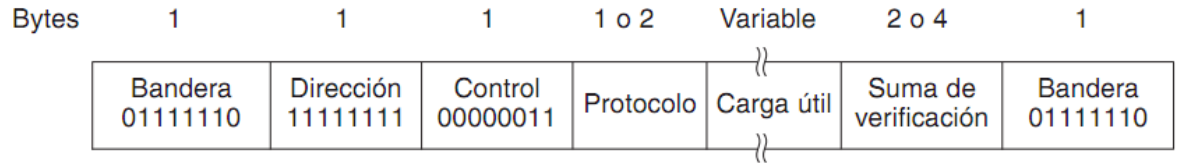
Internet necesita un protocolo punto a punto para diversos propósitos, entre ellos para el tráfico enrutador a enrutador y tráfico usuario doméstico a ISP. Este protocolo es PPP.

PPP realiza detección de errores, soporta múltiples protocolos, permite la negociación de direcciones IP en el momento de la conexión, permite la autenticación y tiene muchas otras funciones.

Proporciona tres características:

1. Un método de entramado que delinea sin ambigüedades el final de una trama y el inicio de la siguiente. El formato de la trama también maneja detección de errores.
2. Un protocolo de control de enlace para activar líneas, probarlas, negociar opciones y desactivarlas ordenadamente cuando ya no son necesarias. Este protocolo se llama LCP (protocolo de control de enlace).
3. Un mecanismo para negociar opciones de capa de red con independencia del protocolo de red usado. El método escogido consiste en tener un NCP (protocolo de control de red) distinto para cada protocolo de capa de red soportado.

El formato de trama de PPP se escogió de modo que fuera muy parecido al de HDLC. La diferencia principal es que PPP está orientado a caracteres, no a bits.



Formato de trama completa PPP para el modo de operación no numerado.

Todas las tramas PPP comienzan y terminan con una bandera estándar de HDLC (01111110), que se rellena con bytes si ocurre dentro del campo de carga útil. Luego está el campo *Dirección*, que siempre se establece al valor binario 11111111 para indicar que todas las estaciones deben aceptar la trama.

El campo de *Dirección* va seguido del campo de *Control*, cuyo valor predeterminado es 00000011. Este valor indica una trama no numerada. PPP no proporciona de manera predeterminada transmisión confiable usando números de secuencia y confirmaciones de recepción.

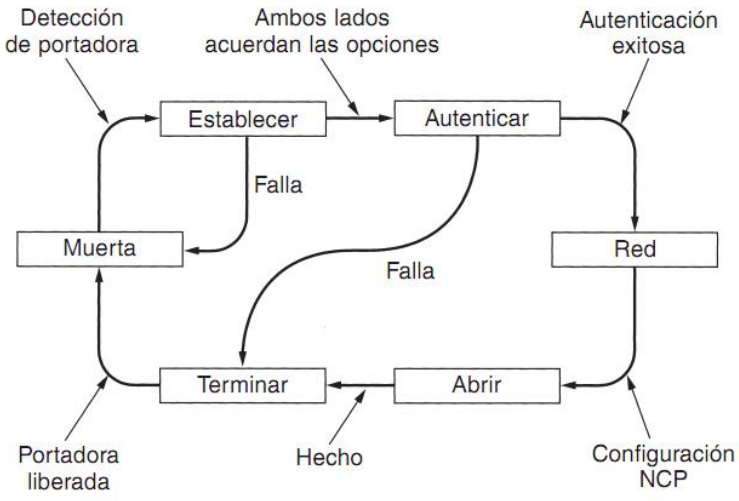
El cuarto campo PPP es el de *Protocolo*. Su tarea es indicar la clase de paquete que está en el campo de *Carga útil*.

El campo de *Carga útil* es de longitud variable, hasta algún máximo negociado. Si la longitud no se negocia con LCP durante el establecimiento de la línea, se usa una longitud predeterminada de 1500 bytes. De ser necesario se puede incluir un relleno después de la carga.

El campo *Suma de verificación* normalmente es de 2 bytes, pero puede extenderse a 4 bytes.

PPP es un mecanismo de entramado multiprotocolo adecuado para utilizarse a través de módems, líneas seriales de bits HDLC, SONET, y otras capas físicas.

En el siguiente diagrama se muestran las fases por las que pasa una línea cuando es activada, usada y desactivada:



El protocolo inicia con la línea que tiene el estado MUERTA, significa que no hay portadora de capa física y que no existe conexión. Una vez establecida la conexión física, la línea pasa a ESTABLECER. En este punto comienza la negociación de opciones LCP para acordar los parámetros PPP por usar, que de tener éxito pasa a AUNTENTICAR. Al entrar en la fase RED, se invoca al protocolo NCP apropiado para configurar la red.

Si la configuración tiene éxito se llega a ABRIR y puede comenzar el transporte de datos. Al terminar el transporte, la línea pasa a la fase TERMINAR donde regresa a MUERTA al liberarse la portadora.
Generalmente la PC requiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes IP para todos, por lo que normalmente el proveedor de internet asigna dinámicamente a cada PC que acaba de conectarse para que la use durante su sesión. Se usa el NCP de IP para asignar la dirección IP. Cuando termina la conexión se usa de nuevo NCP para finalizar la conexión de la capa de red y liberar IP. Después se usa LCP para cancelar la conexión de la capa de enlace.

LA SUBCAPA DE CONTROL DE ACCESO AL MEDIO

En cualquier red de difusión, el asunto clave es la manera de determinar quién puede utilizar el canal cuando hay competencia por él. Los canales de difusión a veces se denominan canales multiacceso o canales de acceso aleatorio.

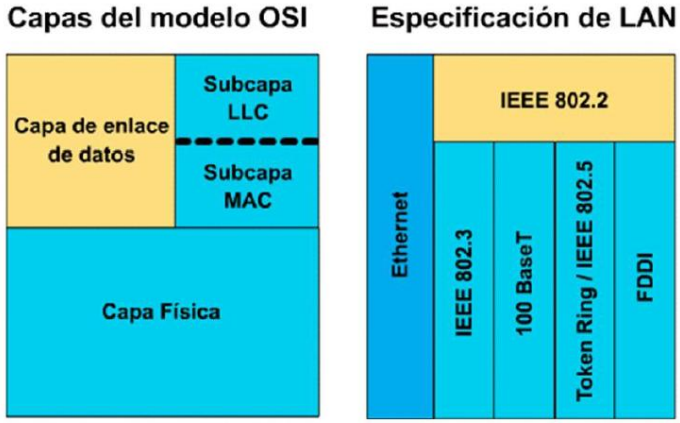
Los protocolos usados para determinar quién sigue en un canal multiacceso pertenecen a una subcapa de la capa de enlace de datos llamada subcapa MAC (Control de Acceso al Medio). La subcapa MAC tiene especial importancia en las LANs, ya que casi todas usan un canal multiacceso como base de su comunicación. Las WANs, en contraste, usan enlaces punto a punto, excepto en las redes satelitales.

Desde el punto de vista técnico, la subcapa MAC es la parte inferior de la capa de enlace de datos.

La IEEE subdividió la capa de enlace de datos en dos subcapas:

- La subcapa LLC (Logical Link Control) o subcapa de control de enlace lógico.
- La subcapa MAC (Media Access Control) o subcapa de control de acceso al medio.

Comparando OSI e IEEE 802.3:



- La subcapa LLC: Fue creada con el propósito de proporcionar a las capas superiores (capa de red) una interfaz independiente de la tecnología empleada en la capa de enlace de datos y en la capa física.
- La subcapa MAC: Los protocolos usados para determinar quién sigue en un canal multiacceso pertenecen a una Subcapa de la Capa de enlace llamada MAC (Control de Acceso al Medio). Se encarga de la topología lógica de la red y del método de acceso a ésta. Cada tecnología de red tiene una subcapa MAC diferente. En la subcapa MAC residen las direcciones MAC.

EL PROBLEMA DE ASIGNACION DEL CANAL

Aquí trataremos la forma de asignar un solo canal de difusión entre usuarios competidores.

Asignación estática del canal en LANs y MANs

La manera tradicional de asignar un solo canal entre varios usuarios competidores es la **FDM** (Multiplexión por división de frecuencias). Si hay N usuarios, el ancho de banda se divide en N partes de igual tamaño y a cada usuario se le asigna una parte. Dado que cada usuario tiene una banda de frecuencia privada, no hay interferencia entre los usuarios.

Si el espectro se divide en N regiones, y hay menos de N usuarios interesados en comunicarse actualmente, se desperdiciará una buena parte de espectro valioso. Si más de N usuarios quieren comunicarse actualmente, a algunos de ellos se les negará el permiso por falta de ancho de banda, aún cuando algunos de los usuarios que tengan asignada una banda de frecuencia apenas transmitan o reciban algo. Cuando algunos usuarios están inactivos, su ancho de banda simplemente se pierde. Además, como en casi todos los sistemas de cómputo el tráfico de datos se hace en ráfagas, la mayoría de los canales estarán inactivos casi todo el tiempo.

Los mismos argumentos que se aplican a la FDM se aplican a la **TDM** (Multiplexión por División de Tiempo). A cada usuario se le asigna la N-ésima ranura de tiempo. Si un usuario no usa la ranura asignada, simplemente se desperdicia.

Eficiencia: como el tiempo promedio de retardo T con λ tramas/segundo y $1/\mu$ bits/trama

a) Un solo canal con velocidad de datos C bps: $T = \frac{1}{\mu C - \lambda}$

b) El canal con velocidad de datos C bps se divide en N subcanales: $T_{FDM} = \frac{1}{\mu\left(\frac{C}{N}\right) - \left(\frac{\lambda}{N}\right)} = \frac{N}{\mu C - \lambda} = NT$

Asignación dinámica de canales en LANs y MANs

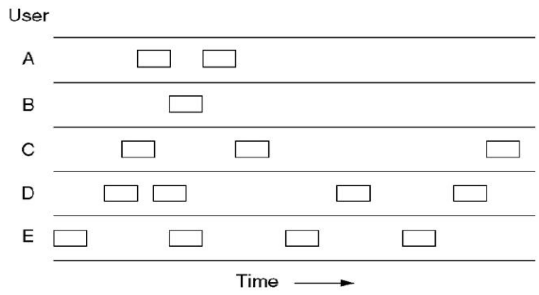
Todo el trabajo hecho en esta área se basa en lo siguiente:

1) Modelo de estación: el modelo consiste en N estaciones (terminales) independientes, cada una con un programa o usuario que generan tramas para transmisión. Una vez que se genera una trama, la estación se bloquea y no hace nada hasta que la trama se haya transmitido con éxito.
2) Supuesto de canal único: hay un solo canal disponible por el que podrán transmitir y recibir todas las estaciones.
3) Supuesto de colisión: Cuando dos tramas se transmiten simultáneamente se traslapan en el tiempo y la señal resultante se altera. Todas las estaciones pueden detectar colisiones. Una trama en colisión debe transmitirse nuevamente. No hay otros errores excepto aquellos generados por las colisiones.
4) Tiempo continuo o ranurado: En un sistema continuo cada estación puede transmitir cuando quiera, no hay reloj maestro que divida el tiempo en intervalos discretos. En un sistema ranurado el tiempo se divide en intervalos discretos (ranuras), las estaciones comienzan a transmisir al inicio de una ranura.
5) Detección de la portadora/Sin detección de la portadora: las estaciones pueden saber/no pueden saber si el canal está en uso o no antes de intentar usarlo.

PROTOCOLOS DE ACCESO MULTIPLE

ALOHA puro

La idea básica es permitir que los usuarios transmitan cuando tengan datos por enviar. Por supuesto, habrá colisiones y las tramas en colisión se dañarán. Debido a la propiedad de retroalimentación de la difusión, un emisor siempre puede saber si la trama fue destruida o no escuchando el canal, de la misma manera que los demás usuarios. Si por alguna razón no es posible escuchar mientras se transmite, se necesitan confirmaciones de recepción. Si la trama fue destruida, el emisor espera un tiempo aleatorio y la envía de nuevo.



En ALOHA puro, las tramas son trasmitidas en tiempos completamente arbitrarios, **no se verifica si el canal está ocupado antes de transmitir**.

No requiere sincronización global del tiempo.

La velocidad real de transporte de los sistemas ALOHA se maximiza al tener tramas con un tamaño uniforme en lugar de tramas de longitud variable.

Cada vez que dos tramas traten de ocupar el canal al mismo tiempo habrá una colisión y ambas se dañarán.

Eficiencia:

- Las tramas son de longitud fija
- La estación tiene dos estados: escribiendo y esperando. Se bloquea esperando la transmisión exitosa de una trama.
- Número infinito de usuarios generando nuevas tramas, según una distribución de Poisson con una media de N tramas por tiempo de trama. $0 < N < 1$ tramas por tiempo de trama. $N>1$ colisión.
- También existe la retransmisión de tramas que sufrieron colisiones por lo que $G \geq N$
  (Si $N \cong 0 \Rightarrow G \cong N$, poca colisión). G es intentos por tiempo de trama.
- El rendimiento por tiempo de trama $S = GP0$, con P0, la probabilidad de que la transmisión de la trama tenga éxito

Ventajas: Se adapta a un número variable de estaciones.

Desventajas: Tiene un rendimiento máximo de 18,4% y requiere almacenar la trama transmitida debido a posible retransmisiones.

Una trama no sufrirá colisión si no se envían otras tramas durante el tiempo de transmisión desde su envío.

Sea t el tiempo de transmisión de su envío, si cualquier otro usuario genero una trama entre el tiempo t_0 y el tiempo t_0 +t el final de la trama chocará con el comienzo de la trama sombreada.

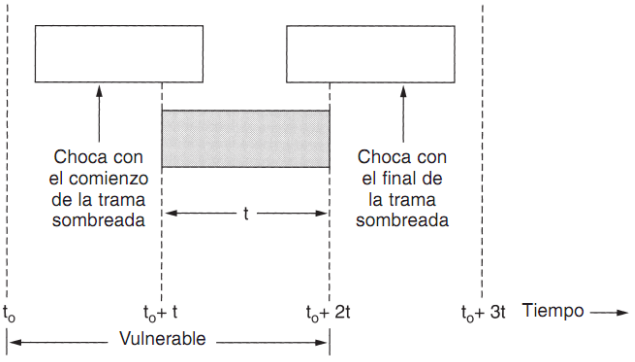


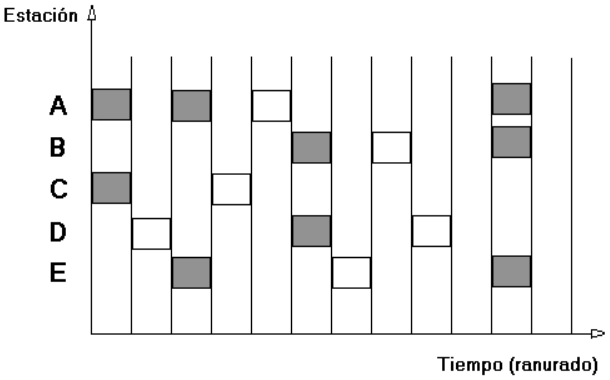
Figura 4-2. Periodo vulnerable para la trama sombreada.

ALOHA ranurado

Se divide el tiempo en intervalos discretos, cada uno de los cuales corresponde a una trama. Cada estación tiene permitido enviar sólo al inicio de una ranura de tiempo. Cuando se produzca una colisión, las tramas se superpondrán totalmente en vez de parcialmente. Esto hace que el rendimiento aumente un 50% respecto de ALOHA puro.

Ventajas: Eficiencia de este protocolo es el doble de ALOHA puro (36,8%) y se adapta a un número variable de estaciones.

Desventajas: se requiere de sincronización entre las estaciones para determinar ranuras comunes de tiempo para todas ellas, y almacenar la trama transmitida debido a posibles retransmisiones.



Protocolos de acceso múltiple con detección de portadora

En las redes de área local es posible que las estaciones detecten lo que están haciendo las demás estaciones y adapten su comportamiento en base a ello.

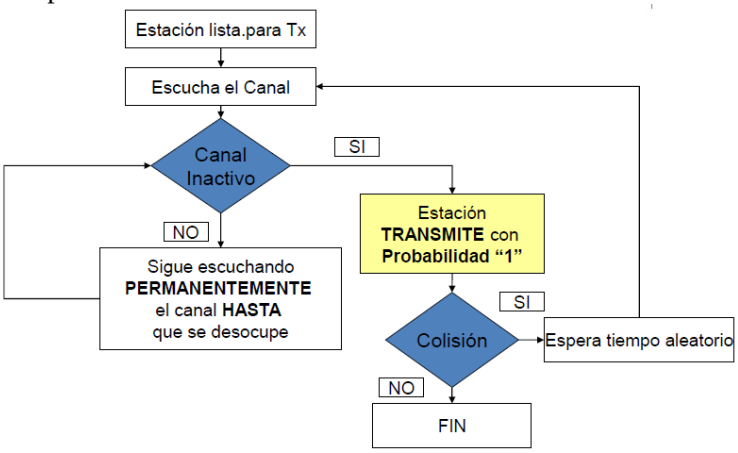
Los protocolos en los que las estaciones escuchan una portadora (una transmisión) y actúan de acuerdo con ellos se llaman protocolos de detección de portadora.

CSMA persistente-1

Cuando una estación tiene datos por transmitir, primero escucha el canal para saber si otra estación está transmitiendo; si el canal está ocupado, la estación espera hasta que quede libre. Cuando detecta un canal libre, transmite la trama. Si ocurre una colisión, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo. Este protocolo se llama así porque la estación transmite con una probabilidad de 1 cada vez que encuentre que el canal está inactivo.

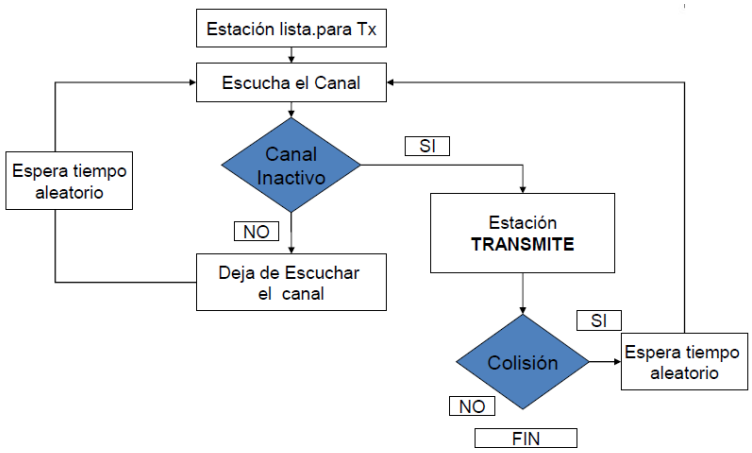
El retardo de propagación tiene un efecto importante en el desempeño del protocolo. Puede pasar que justo después de que una estación comienza a transmitir, otra estación esta lista para enviar y detectar el canal. Si la señal de la primera estación no ha llegado todavía a la segunda, esta última detecta un canal inactivo y enviará datos produciendo se una colisión. Cuanto mayor sea el retardo de propagación, más importante el efecto y peor rendimiento del protocolo.

Que el retardo de propagación sea cero no significa que no habrá colisiones. Si dos estaciones quedan listas a la mitad de transmisión de una tercera, ambas esperarán hasta el fin de la transmisión y comenzarán a transmitir simultáneamente produciendo una colisión.



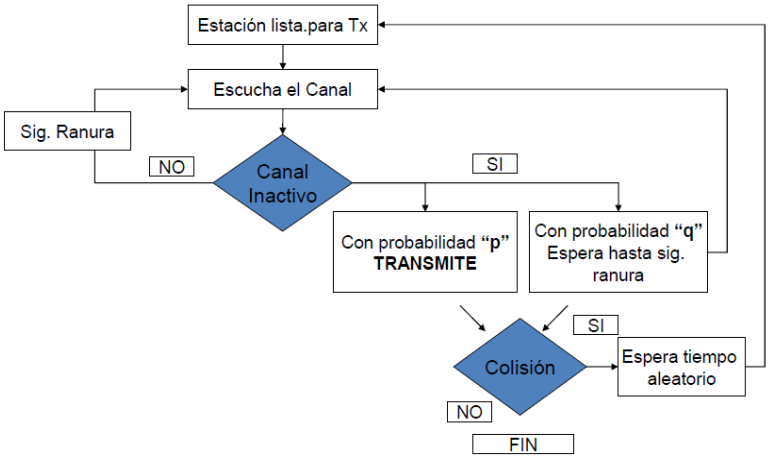
CSMA no persistente

Antes de empezar a transmitir, la estación escucha el canal; si nadie está transmitiendo la estación empieza a hacerlo. Sin embargo, si el canal ya está en uso, la estación no estará escuchando continuamente a fin de tomarlo de inmediato al detectar el final de la transmisión previa, en cambio, espera un tiempo aleatorio para repetir el algoritmo. Este algoritmo conduce a un mejor uso del canal pero produce mayores retardos que el CSMA persistente-1.



CSMA persistente-p

Se aplica a canales ranurados. Cuando una estación está lista para enviar, escucha el canal. Si este está libre, la estación transmite con probabilidad p. Con una probabilidad q=1-p, se espera hasta la siguiente ranura. Si esa ranura también está inactiva, la estación transmite o espera nuevamente, con probabilidades p y q. Este proceso se repite hasta que la trama ha sido transmitida o hasta que otra estación ha comenzado a transmitir. En el segundo caso, la estación actúa como si hubiera ocurrido una colisión (espera un tiempo aleatorio y comienza de nuevo). Si al inicio la estación detecta que el canal está ocupado, espera hasta la siguiente ranura y aplica el algoritmo anterior.

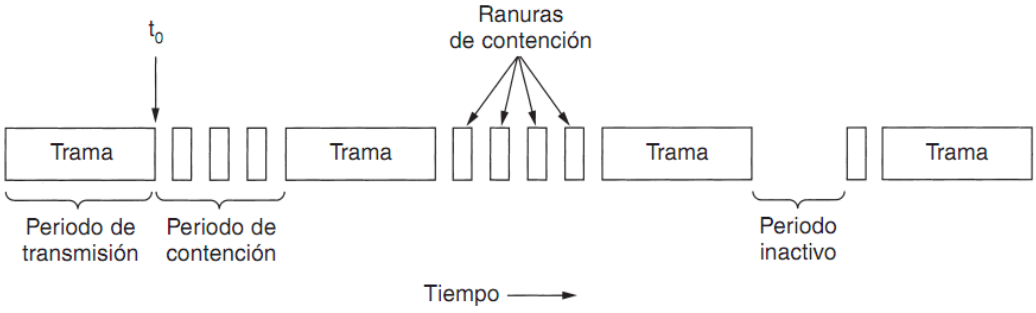


CSMA con detección de colisiones

Si dos estaciones detectan que el canal está inactivo y comienzan a transmitir en forma simultánea, ambas detectarán la colisión casi de inmediato. En lugar de terminar de transmitir sus tramas, que de todos modos resultarán alteradas, deben detener la transmisión de manera abrupta, tan pronto como detecten la colisión, ahorrando tiempo y ancho de banda.

Una vez que una estación detecta una colisión, aborta la transmisión, espera un tiempo aleatorio e intenta nuevamente, suponiendo que ninguna otra estación ha comenzado a transmitir durante ese lapso. Este modelo CSMA/CD consistirá en periodos alternantes de contención y transmisión, ocurriendo periodos de inactividad cuando todas las estaciones están en reposo.

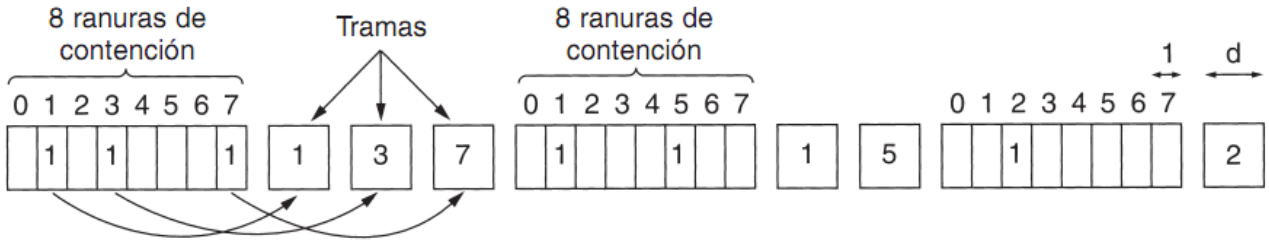
CSMA/CD puede estar en uno de tres estados: contención, transmisión, o reposo.



El CSMA/CA puede estar en uno de tres estados: contención, transmisión o inactivo.

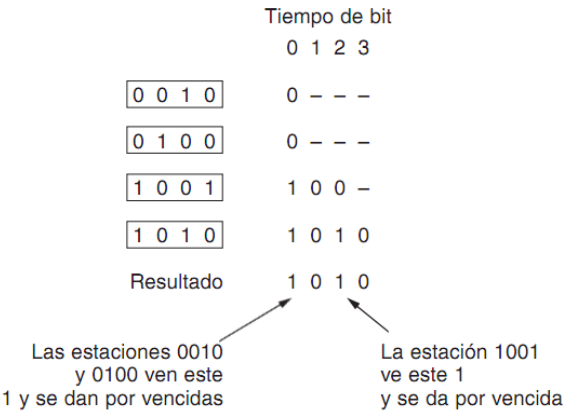
La estación emisora debe monitorear de manera continua el canal en busca de ráfagas de ruido que puedan indicar una colisión. Por esta razón CSMA/CD con un canal es un sistema semidúplex.
El tiempo que se tarda en detectar las colisiones es como máximo el doble del tiempo de propagación de un extremo a otro del cable.
Se modela el intervalo de contienda como un ALOHA ranurado (slotted) con un ancho 2τ.
La colisión debe poder detectarse; por ello la codificación de la señal debe permitir la detección (no puede haber bits de 0 voltios).

Protocolos libres de colisiones
Examinaremos algunos protocolos que resuelven la contención por el canal sin que haya colisiones, ni siquiera en el periodo de contención.
Supondremos que hay N estaciones, cada una con una dirección única de 0 a N-1 incorporada en hardware. El hecho de que algunas estaciones estén inactivas parte del tiempo no importa. También damos por hecho que el retardo de propagación no importa.
Protocolo de mapa de bits
Cada periodo de contención consiste en exactamente N ranuras. Si la estación 0 tiene una trama por enviar, transmite un bit 1 durante la ranura 0 (ninguna otra estación puede transmitir durante esta ranura). En general, la estación j puede anunciar que tiene una trama por enviar introduciendo un bit 1 en la ranura j. Una vez que han pasado las N ranuras, cada estación sabe cuáles son todas las estaciones que quieren transmitir. En este punto las estaciones comienzan a transmitir en orden numérico.



Protocolo básico de mapa de bits.

Nunca habrá colisiones ya que todos están de acuerdo en quien continúa. Una vez que la última estación lista haya transmitido su trama, comienza otro periodo de contención de N bits.
Aquellos protocolos en los que el deseo de transmitir se difunde antes de la transmisión se llaman **protocolos de reservación**.
La eficiencia del canal cuando la carga es baja es fácil de calcular. La sobrecarga por trama es de N bits, y la cantidad de datos es de d bits, dando una eficiencia de d/(N+d).
Si la carga es alta y todas las estaciones tienen algo que enviar todo el tiempo, el periodo de contención de N bits se distribuye en N tramas, arrojando una sobrecarga de solo 1 bits por trama, o una eficiencia de d/(d+1).
No escala bien para miles de estaciones.
Conteo descendente binario
Una estación que quiere utilizar el canal ahora difunde su dirección como una cadena binaria de bits, comenzando por el bit de orden mayor. Se supone que todas las direcciones tienen la misma longitud. A los bits de cada posición de las diferentes estaciones se les aplica un OR booleano a todos juntos. Se asume de manera implícita que los retardos de transmisión son insignificantes, de manera que todas las estaciones ven los bits inmediatamente.
Regla de arbitraje: una vez que una estación ve que una posición de bits de orden alto, que en su dirección es 0, ha sido sobrescrita con un 1, se da por vencida. La dirección que gana la contienda, ahora puede transmitir la trama. Después de lo cual comienza otro ciclo de contienda.
Este protocolo tiene la propiedad de que estaciones con números grandes tienen una prioridad mayor que las que tienen números pequeños.
Eficiencia del canal: $\frac{d}{d+\log_2 N}$



Modificación Mok y Ward:
Se baja la prioridad de cliente cuando logra uso del canal. Se agregan bits para manejarla prioridad.
- ppppnnnn (p=prioridad, n=número dispositivo).

- Eficiencia de uso de canal: $\frac{d}{d+2\log_2 N}$

Protocolos de acceso múltiple por división de longitud de onda

Consiste en dividir el canal en subcanales usando FDM, TDM o ambas y asignarlos de manera dinámica según se necesite. Los esquemas como este se usan en las LANs de fibra óptica para permitir que diferentes conversaciones usen distintas longitudes de onda al mismo tiempo.

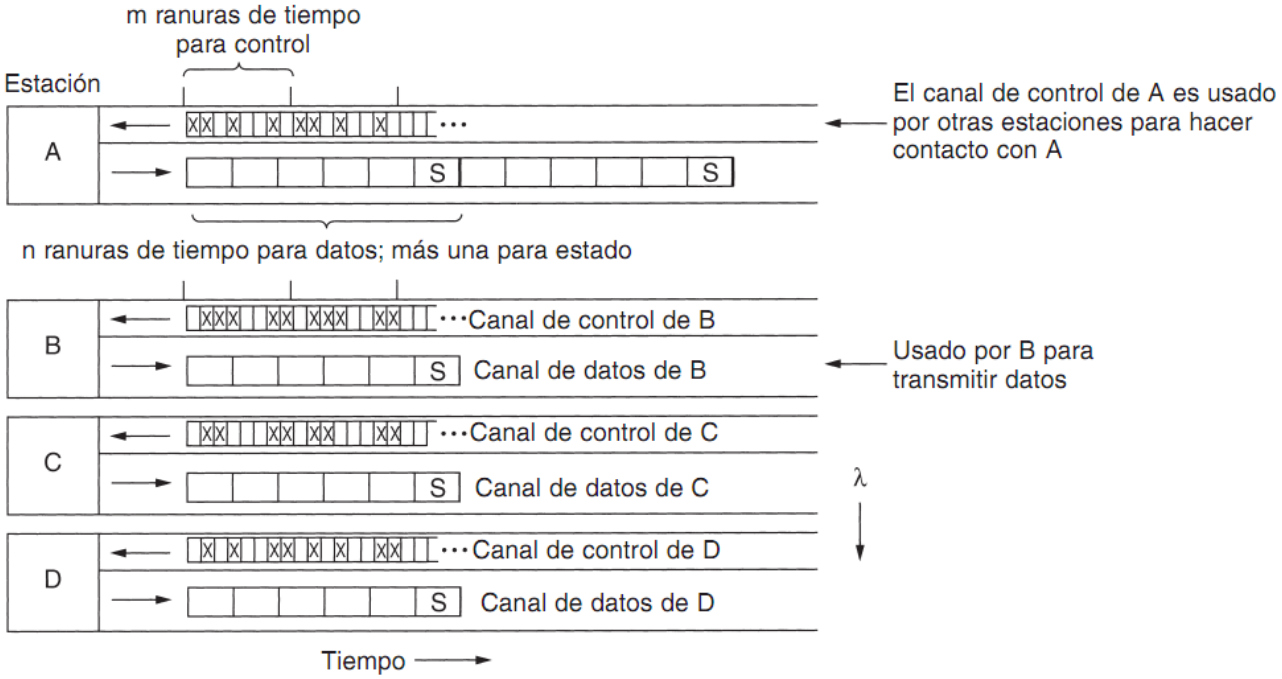
WDMA – Acceso múltiple por división de longitud de onda

Se asignan dos canales a cada estación, por lo que cada una tiene 2 emisores y 2 receptores. Un receptor de longitud de onda fija para escuchar su propio canal de control y uno sintonizable para seleccionar al emisor de datos a escuchar. Un emisor de longitud de onda fija para la salida de tramas de datos, y uno sintonizable para enviar por el canal de control de otra estación. Se proporciona un canal estrecho como canal de control para señalizar la estación, y uno ancho para que la estación pueda enviar tramas de datos.

Todos los canales se sincronizan con un solo reloj global.

El protocolo reconoce 3 clases de tráfico:

1) Orientado a la conexión con tasa de datos constante: Se usa una variación de este protocolo. Cuando A solicita una conexión, simultáneamente dice algo como ¿Está bien si te envío una trama cada vez que ocurra la ranura 3? Si B puede aceptar, se establece una conexión de ancho de banda garantizado. Si no, A puede intentarlo después con una propuesta distinta.
2) Orientado a la conexión con tasa de datos variable, como transferencia de archivos (A comunicación con B). Primero A sintoniza su receptor de datos con el canal de datos de B y espera la ranura de estado (indica cuales ranuras están ocupadas/libres). A elige una de las ranuras de control libre, e introduce su mensaje de solicitud de conexión. Ya que B revisa de manera constante su canal de control, ve la solicitud y la acepta asignando la ranura solicitada a A. Esta asignación se anuncia en la ranura de estado del canal de datos de B. Cuando A ve el anuncio, sabe que tiene una conexión unidireccional. Si A solicita una conexión bidireccional, B repite ahora el mismo algoritmo con A. A ahora envía a B un mensaje de control, avisando que hay un mensaje en x ranura. Cuando B recibe el mensaje de control, sintoniza su receptor al canal de salida de A para leer la trama de datos.
3) Trafico de datagramas, como paquetes UDP: Usa otra variación del protocolo. En lugar de escribir un mensaje de solicitud de conexión en la ranura de control que acaba de encontrar, escribe un mensaje diciendo que hay datos para él en la ranura x. Si B esta libre durante la siguiente ranura de datos x, la transmisión tendrá éxito. Si no, se perderá la trama de datos.



Acceso múltiple por división de longitud de onda.

NOTA: Es posible arreglárselas con un solo emisor y un solo receptor sintonizables por estación haciendo que el canal de cada estación se divida en m ranuras de control seguidas de n+1 ranuras de datos. La desventaja es que los emisores tienen que esperar más tiempo para capturar una ranura de control, y las tramas de datos consecutivas están más distantes porque se interpone cierta información de control.

Protocolos de LANs inalámbricas

Suponemos que todos los emisores de radio tienen algún alcance fijo. Cuando el receptor está dentro del alcance de dos emisores activos, la señal resultante generalmente se altera y resulta inútil. En algunas LANs inalámbricas no todas las estaciones están dentro del alcance de todas las otras.

El alcance de radio es tal que A y B están en el mismo alcance y potencialmente pueden interferir entre sí. C también puede interferir tanto con B como con D pero no con A.

LAN inalámbrica. (a) A transmitiendo. (b) B transmitiendo.

Cuando A está transmitiendo hacia B, si C detecta el medio, no podrá escuchar a A porque está fuera de su alcance y deducirá falsamente que puede transmitir a B. Si C comienza a transmitir, interferirá en B, eliminando la trama de A. El problema de que una estación no pueda detectar a un competidor potencial por el medio debido a que dicho competidor está muy lejos se denomina **problema de estación oculta**.

Cuando B está transmitiendo a A, si C detecta el medio, escuchará una transmisión y concluirá equivocadamente que no puede enviar a D. Ésta situación se denomina **problema de estación expuesta**.

Ya no consideraremos los sistemas de tipo CSMA (detecta si hay actividad alrededor de la estación que está detectando la portadora) porque el problema es que antes de comenzar una transmisión, una estación realmente necesita saber si hay actividad o no alrededor del receptor.

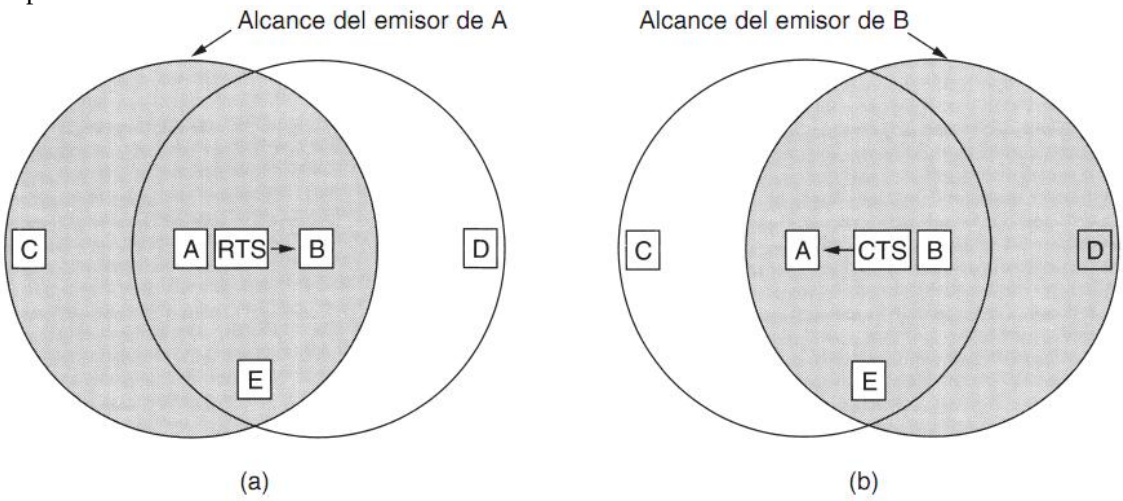
En un sistema basado en ondas de radio de corto alcance, pueden ocurrir transmisiones simultáneas si las ondas tienen destinos diferentes y éstos están fuera de alcance entre sí.

MACA (Acceso múltiple con prevención de colisiones)

Se basa en el concepto de que el emisor estimule al receptor a enviar una trama corta, de manera que las estaciones cercanas puedan detectar esta transmisión y eviten ellas mismas hacerlo durante la siguiente trama de datos (grande).

A envía una trama a B: A comienza por enviar una trama RTS (solicitud de envío) a B. Esta trama corta (30 bytes) tiene la longitud de la trama de datos que seguirá posteriormente. Después B contesta con una trama CTS (libre para envío). La trama CTS contiene la longitud de los datos (copiada de la RTS), una vez que se recibe CTS, A comienza a transmitir.

Cualquier estación que escuche RTS está bastante cerca de A y debe permanecer en silencio durante el tiempo suficiente para que CTS se transmita de regreso a A sin conflicto. Cualquier estación que escuche el CTS está bastante cerca de B y debe permanecer en silencio durante la siguiente transmisión de datos, cuya longitud puede determinar examinando la trama CTS.



El protocolo MACA. (a) A enviando a B un RTS. (b) B respondiendo a A con un CTS.

Aun así pueden ocurrir colisiones. Supongamos que dos estaciones A y B envían tramas RTS al mismo tiempo. Estas chocarán y se perderán. En este caso, el emisor espera un tiempo aleatorio y reintenta.

MACAW (MACA inalámbrico)

Cambios en el MACA para mejorar su desempeño:

- Se descubrió que sin confirmación de recepción de la capa de enlace de datos, las tramas no eran

retransmitidas sino hasta que la capa de transporte notaba su ausencia, mucho después. Como solución introdujeron una trama ACK tras cada trama de datos exitosa.

- Decidieron también que CSMA puede servir para evitar que una estación transmita un RTS al mismo tiempo y destino que otra estación cercana, por lo que se agregó la detección de portadora.
- También decidieron ejecutar el algoritmo de retroceso por separado para cada flujo de datos en lugar de para cada estación.
- Agregaron un mecanismo para que las estaciones intercambiaran información sobre congestionamientos.

ETHERNET

Ethernet e IEEE 802.3 son idénticos, excepto por dos diferencias mínimas que analizaremos pronto.

Cableado Ethernet

Se usan 4 tipos de cableado. En orden de aparición, ellos son:

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

Los tipos más comunes de cableado Ethernet.

Primero llego el cable 10Base5, llamado Ethernet grueso. Este es totalmente rígido, no se dobla y tiene marcas cada 2.5 metros para indicar los puntos de derivación. Las conexiones al cable 10Base5 se hacen usando derivaciones vampiro, en las que se introduce cuidadosamente una punta hasta la mitad del núcleo del cable coaxial (se pincha). La notación 10Base5 significa: el primer número es la velocidad en Mbps, después viene la palabra Base que indica transmisión en banda base y por último, si el medio es coaxial, su longitud se da redondeada a unidades de 100 metros. Por eso podemos decir que opera a 10Mbps y maneja segmentos de hasta 500 metros.

Para 10Base5 se sujeta firmemente un transceptor alrededor del cable, de modo que su derivación haga contacto con el núcleo interno. El transceptor contiene la electrónica que maneja detección de la portadora y detección de colisiones. Al detectarse una colisión, el transceptor también pone una señal especial no válida en el cable para asegurar que todos los demás transceptores se den cuenta de que ha ocurrido una colisión.

Un cable de derivación conecta el transceptor a una tarjeta de interfaz en la computadora. Esta tarjeta tiene un chip controlador que transmite tramas al transceptor y recibe tramas de él.

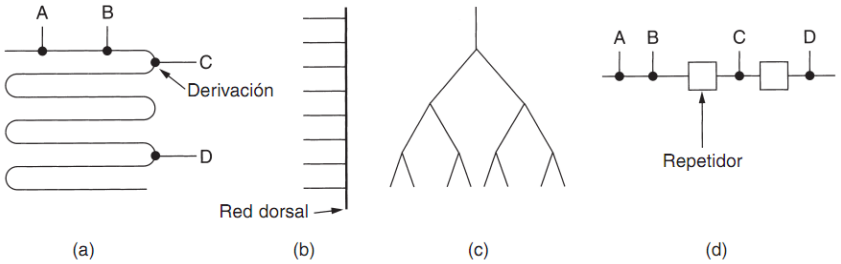
Después, apareció el cable **10Base2**, llamado **Ethernet delgado**. A diferencia del grueso, este se dobla con facilidad. Las conexiones se hacen usando conectores BNC estándar de la industria para formar uniones T. Los conectores son más fáciles de usar y más confiables. Ethernet delgado es mucho más fácil de instalar y más confiable, pero solo puede extenderse 185 metros por segmento, cada uno de los cuales puede manejar sólo 30 máquinas.

Estos dos tipos sufren muchas rupturas, malas derivaciones o conectores flojos. Para rastrear el problema se inyecta un pulso de forma conocida en el cable. Si el pulso incide en un obstáculo o en el final del cable, se generará un eco que viajará de regreso. Si se cronometra cuidadosamente el intervalo entre el envío del pulso y la recepción del eco, es posible ubicar el origen del eco (reflectometría en el dominio del tiempo).

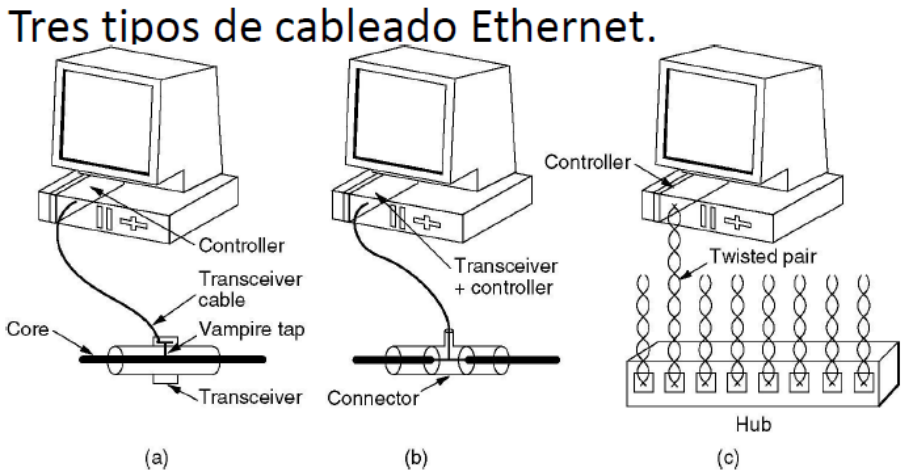
Como solución a estos problemas, surge el cable **10Base-T (par-trenzado)**, en el que todas las estaciones tienen cables que conducen a un concentrador central (hub), en el que se conectan de manera eléctrica. Los concentradores no almacenan en el búfer el tráfico de entrada. Agregar o eliminar estaciones es más sencillo con esta configuración y las rupturas de cable pueden detectarse con facilidad.

Desventaja: longitud máxima de cable es de solo 100 metros.

Otra opción de cableado más rápida que 10Base-T es **10Base-F**, que usa **fibra óptica**. Es cara debido al costo de los conectores y los terminadores pero tiene excelente inmunidad al ruido y permite separaciones entre concentradores de kilómetros (longitud máxima de 2000m).



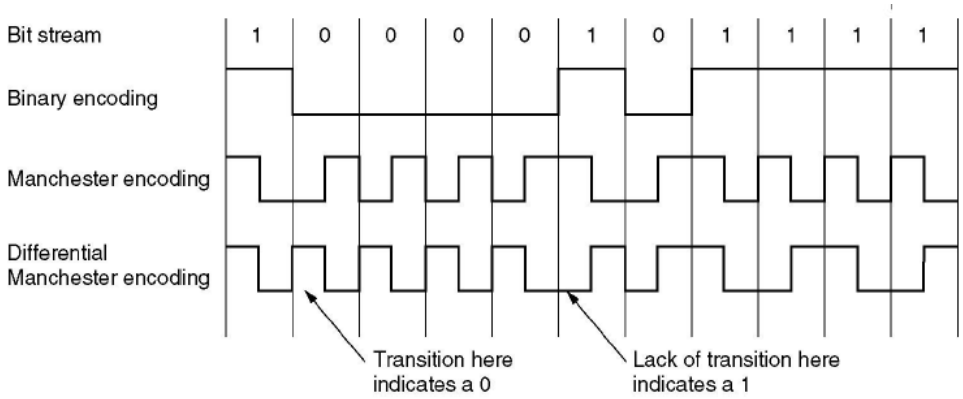
Topologías de cableado. (a) Lineal. (b) Columna vertebral. (c) Segmentada.



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

Para permitir redes mayores, se pueden conectar múltiples cables mediante repetidores, que amplifican y retransmiten las señales en ambas direcciones. Un sistema puede tener múltiples segmentos de cable y muchos repetidores pero ningún par de transceptores puede estar separado por más de 2.5 km (longitud máxima) y ninguna ruta de transceptores puede atravesar más de 4 repetidores.

Codificación Manchester:
Ninguna de las versiones de Ethernet utiliza codificación binaria directa con 0 voltios para un bit 0 y 5 voltios para un bit 1, pues conduce a ambigüedades. No puede distinguirse entre un emisor inactivo (0 voltios) y un bit 0 (0 voltios). Este problema se puede resolver utilizando +1 voltios para un 1 y -1 voltios para un 0, pero puede pasar que un receptor muestree la señal a una frecuencia ligeramente distinta a la que haya utilizado el emisor para generarla y esto causa pérdida de sincronismo.
Lo que se necesita es un mecanismo para que los receptores determinen sin ambigüedades el comienzo, el final o la mitad de cada bit con referencia a un reloj externo.
En la codificación Manchester cada periodo de bit se divide en dos intervalos iguales. Un bit 1 binario se envía teniendo el voltaje alto durante el primer intervalo y bajo durante el segundo. Un bit 0, justo lo inverso: primero bajo y después alto. Este esquema asegura que cada periodo de bit tenga una transición a la mitad, facilitando la sincronización del receptor con el emisor.
Desventaja: requiere el doble de ancho de banda que la codificación binaria común, ya que los pulsos son de la mitad de ancho.
Codificación Manchester Diferencial:
Igual que el anterior pero un bit 1 se indica mediante la ausencia de transición al principio del intervalo y un bit 0 por la presencia de transición al inicio del intervalo. Ofrece mejor inmunidad al ruido. Requiere de un equipo más complejo.
Todos los sistemas Ethernet utilizan codificación Manchester debido a su sencillez. La señal alta es de +0.85 voltios, y la señal baja es de -0.85 voltios, dando un valor de DC de 0 voltios. Ethernet no utiliza Manchester Diferencial pero otras LANs sí la utilizan.



(a) Codificación Binaria. (b) Codificación Manchester.
(c) Codificación Manchester Diferencial.

El protocolo de subcapa MAC de Ethernet

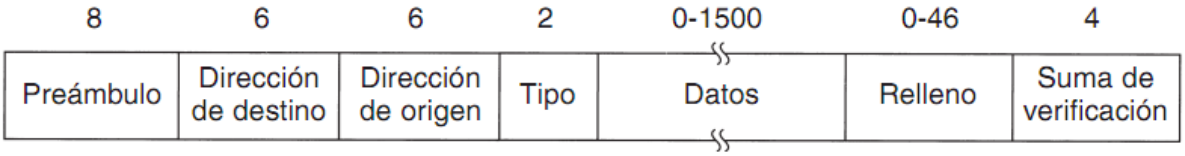
Cada trama inicia con un preámbulo de 8 bytes, cada uno de los cuales contiene el patrón de bits 10101010 con el objetivo de sincronizar emisor y receptor. Se les pide que sigan sincronizados por el resto de la trama, usando la codificación Manchester para mantener un registro de los límites de bits.

La trama contiene 2 direcciones, una para el origen y otra para el destino. El bit de orden mayor de la dirección de destino es 0 para direcciones ordinarias y 1 para direcciones de grupo. Las direcciones de grupo permiten que varias estaciones escuchen en una sola dirección. Cuando una trama se envía a una dirección de grupo todas las estaciones del grupo la reciben. Esto se llama multidifusión (multicast). La dirección que consiste únicamente en bits 1 está reservada para difusión (broadcast). Una trama multidifusión se envía a un grupo seleccionado de estaciones de la Ethernet; una trama de difusión se envía a todas las estaciones de la Ethernet.

Otra característica importante del direccionamiento es el empleo del bit 46 (adyacente al de orden mayor) para distinguir las direcciones locales de las globales. Las direcciones locales son asignadas por cada administrador de la red. Las direcciones globales son asignadas por el IEEE para asegurar que no haya 2 estaciones en ningún lugar del mundo con la misma dirección global.

A continuación está el campo tipo que indica al receptor qué hacer con la trama; especifica a qué proceso darle la trama.

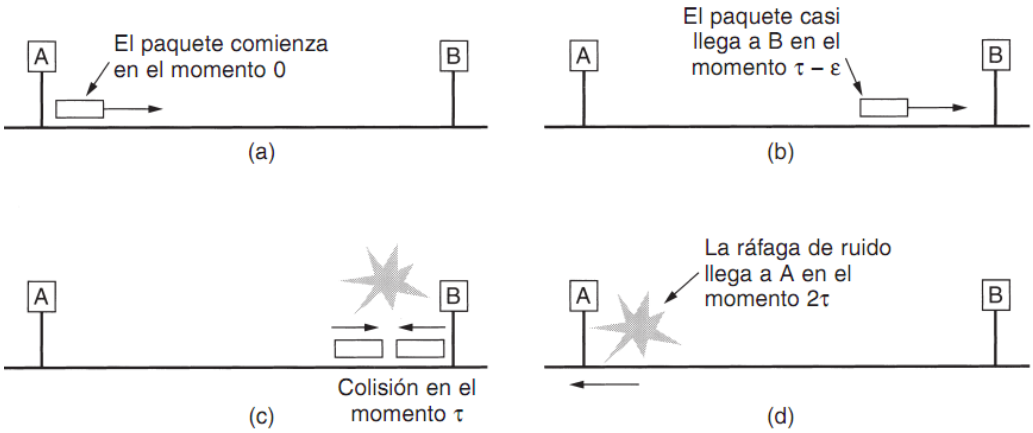
Después están los datos, de hasta 1500 bytes.



Formato de trama Ethernet DIX

Además de haber una longitud de trama máxima también hay una longitud de trama mínima. Razones:

- Cuando un transceptor detecta una colisión, trunca la trama actual. Lo que significa que los bits perdidos y las piezas de las tramas aparecen todo el tiempo en el cable. Para que Ethernet pueda distinguir con facilidad las tramas válidas de la basura, necesita que dichas tramas tengan una longitud de por lo menos 64 bytes, desde la dirección de destino a la suma de verificación (incluyéndolas). Las tramas con menos de 64 byte se rellenan con el campo de Relleno al tamaño mínimo.
- Para evitar que una estación complete la transmisión de una trama corta antes del que el primer bit llegue al extremo más alejado del cable, donde podría tener una colisión con otra trama. Cuando una estación detecta que está recibiendo más potencia de la que está enviando, sabe que ha ocurrido una colisión entonces aborta su transmisión y genera una ráfaga de ruido de 48 bits para avisar a las demás estaciones.



La detección de una colisión puede tardar hasta 2τ

Llamemos τ al tiempo que tarda una trama en llegar al otro extremo. Si una estación intenta transmitir una trama muy corta, es concebible que ocurra una colisión, pero la transmisión se completa antes de que la ráfaga de ruido legue de regreso, en el momento 2τ. El emisor entonces supondrá incorrectamente que la trama se envió con éxito. Para evitar que esta situación ocurra, todas las tramas deben tardar más de 2τ para enviarse, de manera que la transmisión aún esté llevándose a cabo cuando la ráfaga de ruido regrese al emisor.

Para una LAN con 10 Mbps con una longitud máxima de 2.5 km y 4 repetidores, el tiempo de ida y vuelta se ha determinado a aproximadamente 50 microsegundos en el peor casos, incluyendo el tiempo para pasar a través de los repetidores. ¿Por qué? La distancia máxima permitida para Ethernet es de 2500 kilómetros, a 10 Mbps y 4 repetidores.

Nota: Consideramos la velocidad de la luz $2x10^8$ m/s.

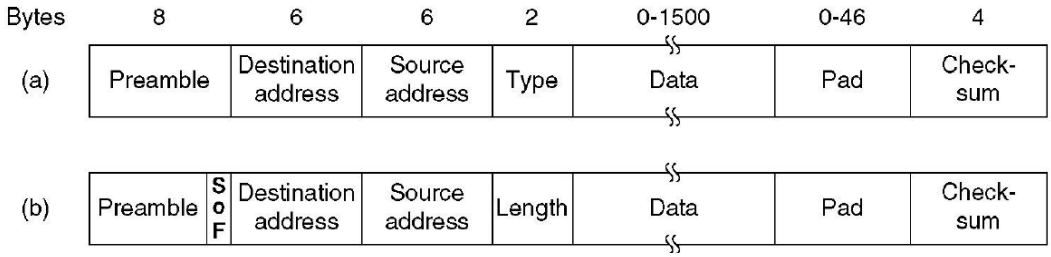
Entonces, si en 1 segundo son $2x10^8$ metros; en 12,5 microsegundos recorremos los 2500 metros. Pero nos interesa saber el tiempo de ida y vuelta, por lo que debemos hacer 12,5*2 obteniendo así aproximadamente 50 microsegundos de transmisión en el peor caso.

Ahora, si en 1 segundo transmite $10x10^6$ en 50 microsegundos transmite 500 bits. Pero para agregar un margen de seguridad, se redondeo a un número exacto de bytes; y el más próximo es 512 bits = 64 byte. Entonces, si transmite 500 bits en 50 microsegundos, 512 bit los transmite en 51,2 microsegundos. Las tramas con menos de 64 bytes se rellenan con 64 bytes con el campo de relleno.

El campo final de Ethernet es la suma de verificación. Si algunos de los bits de datos se reciben erróneamente, es muy probable que la suma de verificación esté mal y se detectará el error. El algoritmo es un CRC. Detecta errores pero no corrige.

Diferencias entre IEEE 802.3 y Ethernet DIX:

IEEE 802.3 redujo el preámbulo a 7 bytes y usa el último como delimitador de Inicio de trama, por compatibilidad con 802.4 y 802.5. Además, cambió el campo de Tipo por un campo de Longitud. No había forma de que el receptor supiera qué hacer con la trama entrante. Esto se solucionó agregando un pequeño encabezado a la porción de datos que brinde esa información.



Formatos de trama (a) Ethernet DIX (b) IEEE 802.3

Algoritmo de retroceso exponencial binario

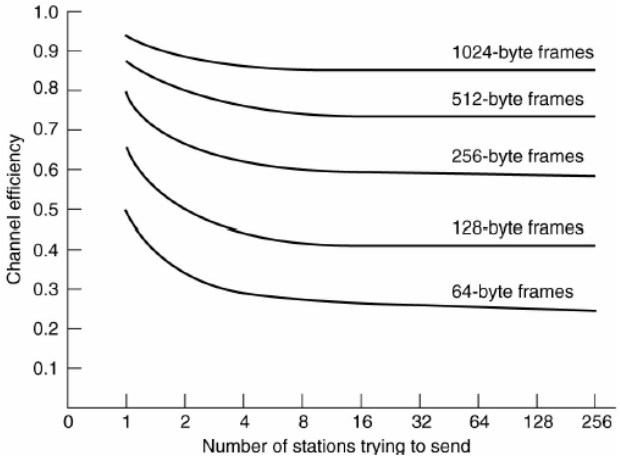
Indica cómo se realiza el proceso de aleatorización cuando ocurre una colisión.

Tras una colisión, el tiempo se divide en ranuras discretas cuya longitud es igual al tiempo de propagación de ida y vuelta del peor caso en el cable (2τ), es decir 51,2 microsegundos o 512 tiempos de bit.

Tras la primera colisión, cada estación espera 0 o 1 tiempos de ranura antes de intentarlo de nuevo. Si ambas eligen el mismo número aleatorio, entrarán otra vez en colisión. Después de la segunda cada una escoge 0, 1, 2 0 3 al azar y espera ese número de tiempos de ranura. En general, tras i colisiones, se elige un número aleatorio entre 0 y 2^i-1, y se salta ese número de ranuras. Tras haber alcanzado 10 colisiones, el intervalo de

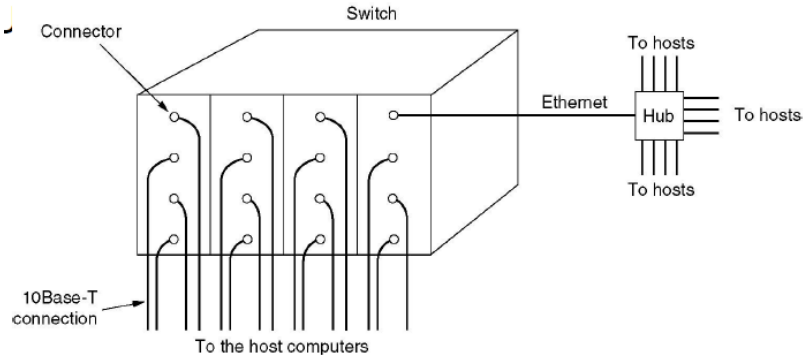
aleatorización se congela en un máximo de 1023 ranuras. Tras 16 colisiones, el controlador informa de un fracaso a la computadora. La recuperación posterior es responsabilidad de las capas superiores.
Haciendo que el intervalo de aleatorización crezca de manera exponencial a medida que ocurren más y más colisiones, el algoritmo asegura un retardo pequeño cuando sólo unas cuantas estaciones entran en colisión, pero también asegura que la colisión se resuelva en un intervalo razonable cuando hay colisiones entre muchas estaciones. Truncar el retroceso a 1023 evita que el límite crezca demasiado.

Eficiencia de Ethernet a 10 Mbps con tiempo de ranuras de 512 bits:



Ethernet conmutada

Surgió como solución al aumento de tráfico por incorporación de nuevos usuarios. Consiste en un conmutador (switch) que tiene una matriz de conmutación de alta velocidad (1Gbps) y espacio para 4 a 32 tarjetas de línea, cada una de las cuales contiene de 1 a 8 conectores. Lo más común es que cada conector tenga una conexión de cable de par trenzado 10Base-T a una sola computadora host.



Ejemplo sencillo de Ethernet conmutada.

Cuando una estación quiere transmitir una trama Ethernet, envía una trama estándar al conmutador. La tarjeta que la recibe la revisa para ver si está destinada a una de las otras estaciones conectadas a la misma tarjeta. Si es así, la trama se copia ahí. Si no, se envía a través de la matriz de conmutación de alta velocidad a la tarjeta de la estación destino. Dicha matriz funciona a más de 1 Gbps usando un protocolo patentado.
Si dos máquinas conectadas a una misma tarjeta de conexión transmiten tramas al mismo tiempo puede ocurrir lo siguiente (dependiendo de la manera en que haya sido construida la tarjeta):

1) Si todos los puertos de la tarjeta forman una LAN local dentro ella, las colisiones en esta LAN se detectan y manejan igual que cualquier otra colisión en una red CSMA/CD, en las que las retransmisiones usan el algoritmo de retroceso exponencial binario. Sólo es posible una transmisión por tarjeta en un momento dado, pero todas las tarjetas pueden estar transmitiendo en paralelo. Cada tarjeta forma su propio dominio de colisión, independiente de los demás. Con sólo una estación por dominio de colisión, las colisiones son imposibles y el desempeño mejora.
2) Cada puerto de entrada se almacena en un búfer, por lo que las tramas de entrada se almacenan en la RAM de la tarjeta mientras van llegando. Permite que todos los puertos de entrada reciban y transmitan al mismo tiempo, para una conexión en paralelo completamente dúplex. Una vez que llega por completo la trama la tarjeta puede determinar si la trama está destinada a otro puerto de la misma tarjeta o a otro distante. En el primer caso se transmite directamente, en el segundo, debe transmitirse a través de la matriz de conmutación. Con este diseño cada puerto es un dominio de

colisión independiente, por lo que nunca ocurren colisiones.
Ya que el conmutador sólo espera tramas Ethernet en cada puerto de entrada, es posible utilizar alguno de los puertos como concentradores. A medida que llegan tramas al concentrador, luchan por el canal de la manera usual, con colisiones y retroceso binario. Las tramas que tienen éxito llegan al conmutador y ahí se tratan como cualquier otra trama de entrada.

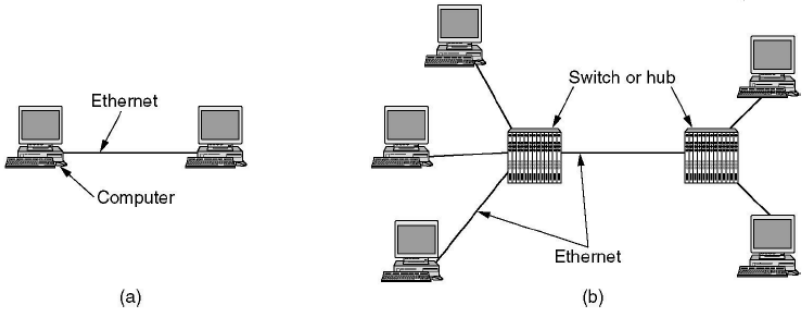
Fast Ethernet
Se decidió crear una Ethernet mejorada por tres razones principales:
- La necesidad de compatibilidad hacia atrás con las LANs Ethernet existentes.
- El miedo de que un nuevo protocolo tuviera problemas no previstos.
- El deseo de terminar el trabajo antes de que la tecnología cambiara.

La idea básica era mantener todos los formatos anteriores, interfaces y reglas de procedimientos, y sólo reducir el tiempo de bits de 100 nseg a 10 nseg.
Todos los sistemas Fast Ethernet utilizan concentradores y conmutadores; no se permiten cables con múltiples derivaciones vampiro ni conectores BNC.
El cableado original de Fast Ethernet:

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

100Base-T4: utiliza velocidad de señalización de 25MHs. Para alcanzar el ancho de banda necesario requiere cuatro cables de par trenzado. De los 4 cables de par trenzado, uno siempre va al concentrador, uno siempre sale del concentrador y los otros 2 son intercambiables a la dirección actual de transmisión.
100Base-TX: los cables pueden manejar velocidades de reloj de 125MHz. Sólo se utilizan dos cables de par trenzado por estación, uno para enviar y otro para recibir. Es dúplex total; las estaciones pueden enviar y recibir al mismo tiempo a 100Mbps.
Con frecuencia en conjunto 100Base-T4 y 100Base-TX se llaman 100Base-T.
100Base-FX: utiliza 2 filamentos de fibra multimodo, una para cada dirección, por lo que también es dúplex total con 100Mbps en cada dirección. La distancia entre una estación y el concentrador puede ser de hasta 2 km.
En un concentrador todas las líneas entrantes se conectan lógicamente, formando un solo dominio de colisión. Se aplican todas las reglas estándar, entre ellas el algoritmo de retroceso exponencial binario, por lo que el sistema funciona de la misma manera que la Ethernet antigua. En particular, sólo una estación a la vez puede transmitir. En otras palabras, los concentradores requieren comunicación semidúplex.
En un conmutador, cada trama entrante se almacena en el búfer de una tarjeta de conexión y se pasa a través de una matriz de conmutación de alta velocidad de la tarjeta de origen a la de destino, si es necesario. La matriz de conmutación no se ha estandarizado, ni lo necesita debido a que se encuentra completamente oculta dentro del conmutador.

Gigabit Ethernet
Todas las configuraciones de Gigabit Ethernet son de punto a punto. La configuración más simple consiste en dos computadoras conectadas entre sí de manera directa. Sin embargo, el caso más común es tener un conmutador o un concentrador conectado a múltiples computadoras y posiblemente a conmutadores o concentradores adicionales. En ambas configuraciones cada cable Ethernet individual tiene exactamente dos dispositivos en él.



(a) Ethernet de dos estaciones. (b) Ethernet con múltiples estaciones.

Soporta 2 modos diferentes de funcionamiento: modo de dúplex total y modo semidúplex. El modo “normal” es el de dúplex total, el cual permite tráfico en ambas direcciones al mismo tiempo. Este modo se utiliza

cuando hay un conmutador central conectado a computadoras (o a otros conmutadores) en el periférico. En ésta configuración, todas las líneas se almacenan en el búfer a fin de que cada computadora y conmutador pueda enviar tramas siempre que lo desee. En la línea entre una computadora y un conmutador, la computadora es el único emisor posible en esa línea al conmutador y la transmisión tiene éxito aún cuando el conmutador esté enviando actualmente una trama a la computadora (porque la línea es de dúplex total).
El otro modo de operación, semidúplex, se utiliza cuando las computadoras están conectadas a un concentrador en lugar de a un conmutador. Un concentrador no almacena en el búfer las tramas entrantes. En su lugar, conecta en forma eléctrica todas las líneas internamente, simulando el cable con múltiples derivaciones que se utiliza en la Ethernet clásica. En este modo las colisiones son posibles, por lo que es necesario el protocolo CSMA/CD estándar. Debido a que una trama mínima (64 bytes) ahora puede transmitirse 100 veces más rápido que en la Ethernet clásica, la distancia máxima es 100 veces menor, o 25 metros, para mantener la propiedad esencial de que el emisor aún transmita cuando la ráfaga de ruido vuelva a él, incluso en el peor caso.
El comité 802.3z consideró un radio de 25 metros como inaceptable y agregó 2 características al estándar para incrementar el radio:

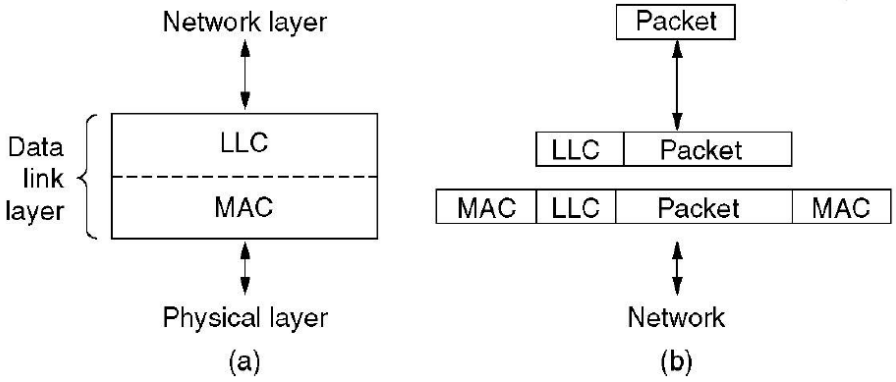
- La primera, llamada **extensión de portadora**, esencialmente indica al hardware que agregue su propio relleno después de la trama normal para extenderla a 512 bytes. Este relleno es agregado por el hardware emisor y eliminado por el hardware receptor, el software no toma parte en esto.
- La segunda, llamada **ráfagas de trama**, permite que un emisor transmita una secuencia concatenada de múltiples tramas en una sola transmisión. Si la ráfaga total es menor que 512 bytes, el hardware la rellena nuevamente. Si suficientes tramas están esperando la transmisión, este esquema es muy eficiente y se prefiere antes que la extensión de portadora.

Estas nuevas características amplían el radio de red a 200 metros.
Cableado de Gigabit Ethernet:

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

Gigabit Ethernet soporta control de flujo, que consiste en que un extremo envíe una trama de control especial al otro extremo indicándole que se detenga por algún tiempo.

Estándar IEEE 802.2: control lógico del enlace
Hay sistemas en los que se desea un protocolo de enlace de datos con control de errores y control del flujo. El protocolo LLC (Control Lógico del Enlace) puede operar encima de todos los protocolos Ethernet y 802. Además, esconde las diferencias entre los distintos tipos de redes 802, proporcionando un formato único y una interfaz con la capa de red. Este formato, interfaz y protocolo están basados en HDLC. El LLC forma la mitad superior de la capa de enlace de datos, con la subcapa MAC debajo de él.



(a) Posición del LLC. (b) Formatos del protocolo.

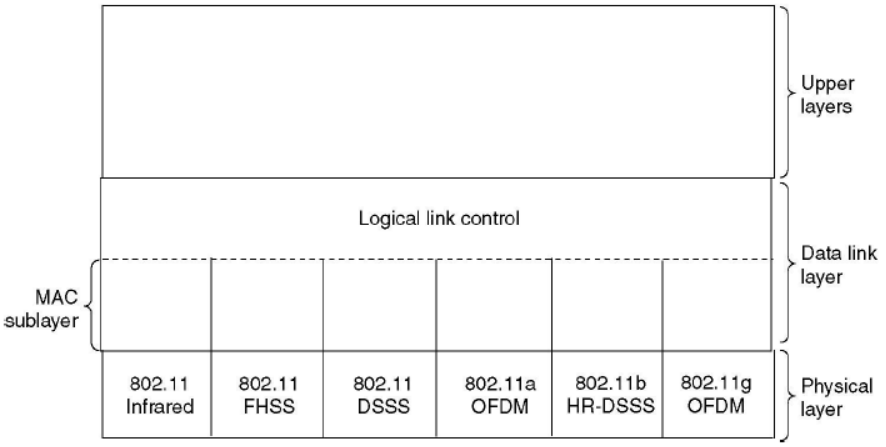
El uso típico es el siguiente:

- La capa de red de la máquina emisora pasa un paquete al LLC.
- La subcapa LLC agrega un encabezado LLC que contiene los números se secuencia y confirmación de recepción.
- La estructura resultante se introduce en el campo de carga útil de una trama 802 y se transmite.

En el receptor ocurre el proceso inverso.
LLC proporciona tres tipos de servicio: servicio no confiable de datagramas, servicio de datagramas sin confirmación de recepción y servicio confiable orientado a la conexión.
El encabezado de LLC contiene tres campos: un punto de acceso de destino, un punto de acceso de origen y un campo de control. Los puntos de acceso indican de cuál proceso proviene la trama y en dónde se va a enviar (reemplazan el campo Tipo de DIX). El campo de control contiene números de secuencia de y de confirmación de recepción. Estos campos se utilizan principalmente cuando se necesita una conexión confiable en el nivel de enlace de datos. Para internet, los intentos de mejor esfuerzo para enviar los paquetes IP son suficientes, por lo que no se requieren confirmaciones de recepción en el nivel LLC.

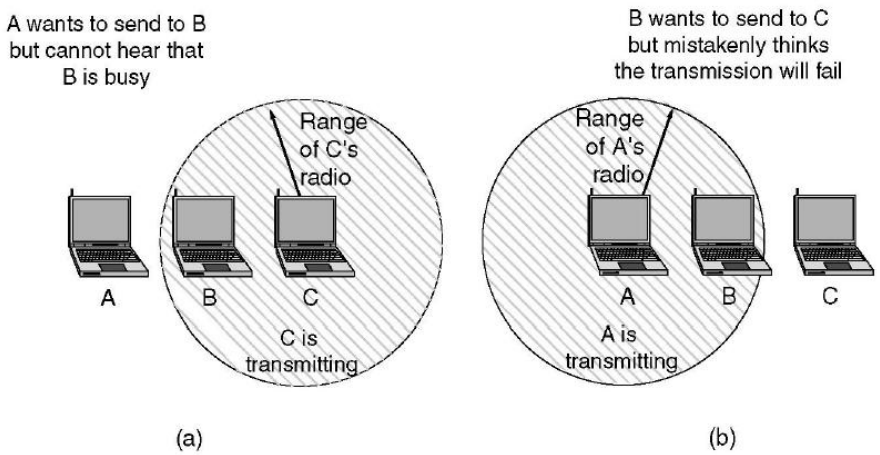
LANS INALAMBRICAS
Las LANs inalámbricas pueden funcionar en una de dos configuraciones: con una estación base y sin ninguna estación base.

La pila de protocolos del 802.11
La capa física corresponde muy bien con la capa física OSI, pero la capa de enlace de datos de todos los protocolos 802 se divide en dos o más subcapas. En el estándar 802.11, la subcapa MAC determina la forma en la que se asigna el canal. Arriba de dicha capa se encuentra la subcapa LLC, cuyo trabajo es ocultar las diferencias entre las variantes 802 con el propósito de que sean imperceptibles para la capa de red.
El estándar 802.11 especifica tres técnicas de transmisión permitidas en la capa física. El método de infrarrojos utiliza en su mayor parte la misma tecnología que os controles remotos de televisión. Los otros dos métodos utilizan el radio de corto alcance mediante técnicas conocidas como FHSS (Espectro Disperso con Salto de Frecuencia) y DSSS (Espectro Disperso de Secuencia Directa).



Parte de la pila de protocolos del 802.11

El protocolo de la subcapa MAC del 802.11
Puesto que no todas las estaciones están dentro del alcance de radio de cada una, las transmisiones que van en un lado de la celda podrían no recibirse en el otro lado de la misma celda. Por lo tanto existe el problema de la estación oculta.
Además, existe el problema inverso, el de la estación expuesta. La mayoría de los radios son semidúplex, lo que significa que no pueden transmitir y escuchar ráfagas de ruido al mismo tiempo en una sola frecuencia.
802.11 soporta dos modos de funcionamiento: **DFC (Función de Coordinación Distribuida)** que no utiliza ningún tipo de control central, y **PCF (Función de Coordinación Puntual)** que utiliza la estación base para controlar toda la actividad en su celda. Todas las implementaciones soportan DCF pero PCF es opcional.



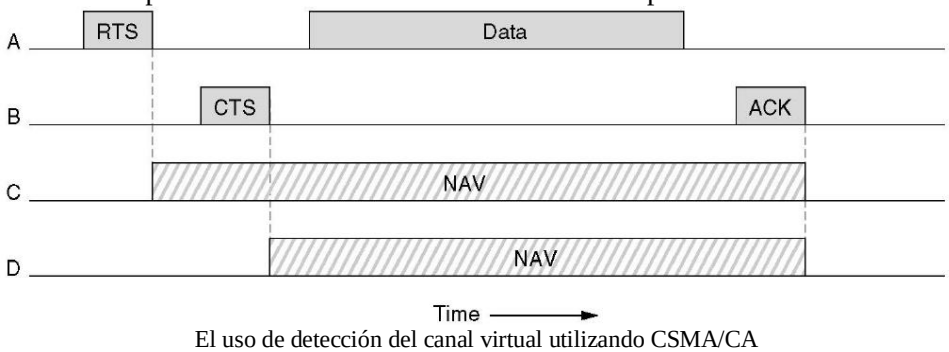
(a) El problema de la estación oculta. (b) El problema de la estación expuesta.

Cuando se emplea DFC, 802.11 utiliza un protocolo llamado CSMA/CA (CSMA con Evitación de Colisiones). Los dos métodos de funcionamiento son soportados por CSMA/CA, En el primer método, cuando una estación desea transmitir, detecta el canal. S está inactivo, comienza a transmitir. No detecta el canal mientras transmite pero emite su trama completa, la cual podría ser destruida en el receptor debido a interferencia. Si el canal está ocupado, el emisor espera hasta que esté inactivo para comenzar a transmitir. Si ocurre una colisión, las estaciones involucradas en ella esperan un tiempo aleatorio, mediante el algoritmo de retroceso exponencial binario de Ethernet, y vuelve a intentarlo más tarde.

El otro modo de la operación CSMA/CA se basa en MACAW y utiliza la detección del canal virtual. Por ejemplo: A desea enviar a B, C es una estación que está dentro del alcance de A (posiblemente también dentro del alcance de B) y D es una estación dentro del alcance de B pero no del de A.

El protocolo inicia cuando A decide enviar datos a B. A inicia enviándole una trama RTS a B en la que le solicita el permiso para enviarle una trama. Cuando B recibe esta solicitud, si decide otorgarle el permiso le regresa una trama CTS. Al recibir la CTS, A ahora envía su trama y comienza su temporizador de ACK. Al recibir correctamente la trama de datos, B responde con una trama de ACK, con lo que termina el intercambio. Si el temporizador de ACK de A termina antes de que el ACK regrese, todo el protocolo se ejecuta de nuevo.

Ahora consideremos este intercambio desde el punto de vista de C y D. C está dentro del alcance de A, por lo que podría recibir la trama RTS. Si pasa esto, se da cuenta de que alguien va a enviar datos pronto, así que desiste de transmitir hasta que el intercambio esté completo. A partir de la información proporcionada en RTS, C puede estimar cuánto tardará la secuencia, incluyendo el ACK final, por lo que impone para sí misma un tipo de canal virtual ocupado (NAV, Vector de Asignación de Red). D no escucha el RTS, pero sí el CTS, por lo que también impone una señal NAV para sí misma. Las señales NAV no se transmiten, simplemente son recordatorios internos para mantenerse en silencio durante cierto periodo.



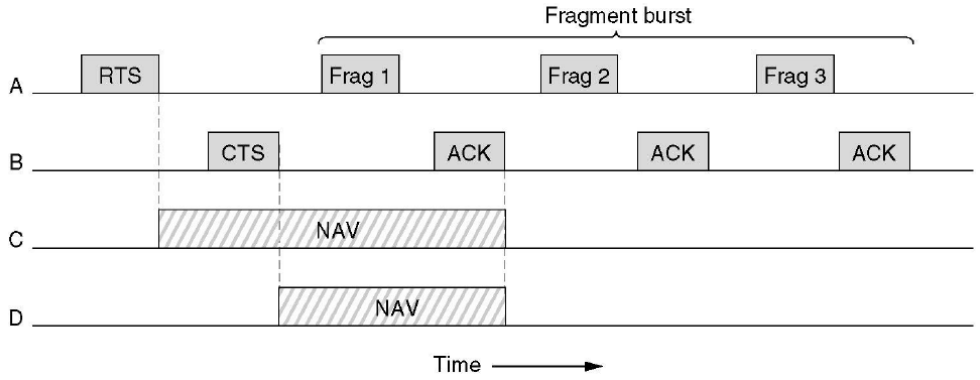
El uso de detección del canal virtual utilizando CSMA/CA

Las redes inalámbricas son ruidosas e inestables. La probabilidad de que una trama llegue a su destino se decrementa con la longitud de la trama. Si la probabilidad de que cualquier bit sea erróneo es p, entonces la probabilidad de que una trama de n bits se reciba por completo y correctamente es $(1 - p)^n$. Si una trama es demasiado grande, tiene muy pocas probabilidades de pasar sin daño y probablemente tenga que retransmitirse.

Para solucionar el problema de los canales ruidosos, 802.11 permite dividir las tramas en fragmentos, cada uno con su propia suma de verificación. Cada fragmento se numera de manera individual y su recepción se confirma utilizando un protocolo de parada y espera.

Una vez que e ha adquirido el canal mediante RTS y CTS, pueden enviarse múltiples fragmentos en una fila.

La secuencia de fragmentos se conoce como ráfaga de fragmentos.



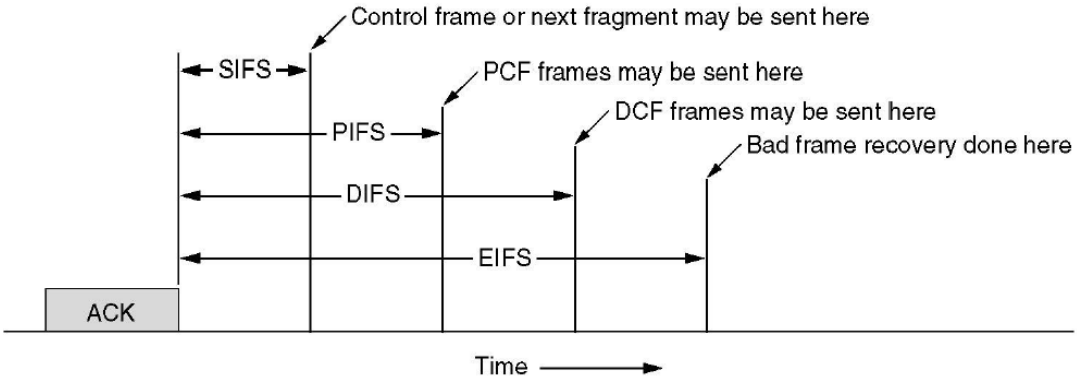
Una ráfaga de fragmentos

La fragmentación incrementa la velocidad real de transporte restringiendo las retransmisiones a los fragmentos erróneos en lugar de la trama completa. El mecanismo NAV mantiene otras estaciones en silencio sólo hasta la siguiente confirmación de recepción, pero se utiliza otro mecanismo para permitir que otra ráfaga de fragmentos completa se envíe sin interferencia.

Todo el análisis anterior se aplica al modo DFC 802.11. No hay control central y la estación compite por tiempo aire. El otro mecanismo permitido es PCF, en el que la estación base sondea las demás estaciones, preguntándoles si tienen tramas que enviar. Puesto que el orden de transmisión se controla por completo por la estación base en el modo PCF, no ocurren colisiones.

El mecanismo básico consiste en que la estación base difunda una **trama de beacon** (trama guía o faro) de manera periódica. Esta trama contiene parámetros de sistema, como secuencias de salto y tiempos de permanencia (para FHSS), sincronización de reloj, etc. También invita a las nuevas estaciones a suscribirse al servicio de sondeo. Una vez que una estación se inscribe para el servicio de sondeo a cierta tasa, se le garantiza de manera efectiva cierta fracción de ancho de banda, y se hace posible proporcionar garantías de calidad de servicio.

PCF y DCF pueden coexistir dentro de una celda. Se define cuidadosamente el intervalo de tiempo entre tramas. Después de que se ha enviado una trama, se necesita cierta cantidad de tiempo muerto antes de que cualquier estación pueda enviar una trama. Se definen cuatro intervalos diferentes, cada uno con un propósito específico.



Espaciado entre tramas 802.11

El intervalo más corto es SIFS (Espaciado Corto Entre Tramas). Se utiliza para permitir que las distintas partes de un diálogo transmitan primero.

Siempre hay una sola estación que debe responder después de un intervalo SIFS. Si falla al utilizar su oportunidad y transcurre un tiempo PIFS (Espaciado Entre Tramas PCF), la estación base podría enviar una trama de beacon o una trama de sondeo.

Si la estación base no tiene nada que decir y transcurre un tiempo DIFS (Espaciado Entre Tramas DCF), cualquier estación podría intentar adquirir el canal para enviar una nueva trama.

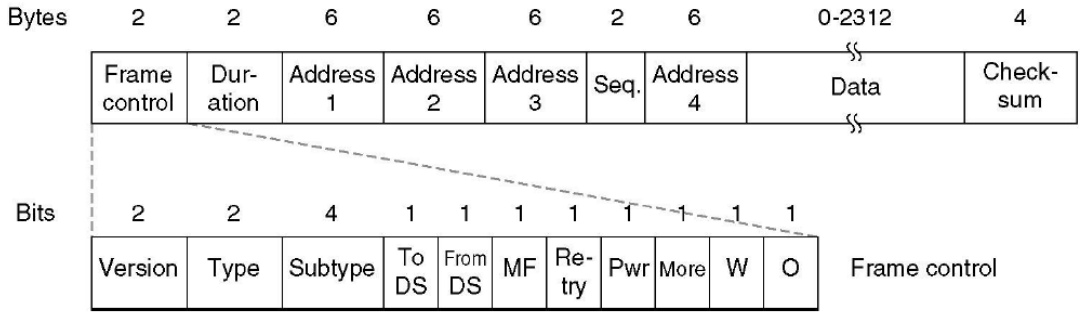
Sólo una estación que acaba de recibir una trama errónea o desconocida utiliza el último intervalo de tiempo, EIFS (Espaciado Entre Tramas Extendido), para reportar la trama errónea.

La estructura de la trama 802.11

Se definen tres clases de tramas en el cable: de datos, de control y de administración.

Trama de datos: primero está el campo de *Control de trama*, que contiene 11 subcampos:

- Versión del protocolo: permite que dos versiones del protocolo funcionen al mismo tiempo en la misma celda.
- Campo de Tipo (de Datos, de Control o de Administración).
- Campo de Subtipo (por ejemplo CTS o RTS).
- A DS y De DS: indican que la trama va hacia o viene del sistema de distribución entre celdas.
- MF: indica que siguen más fragmentos.
- Retrans.: marca una retransmisión de una trama que se envió anteriormente.
- Administración de energía: es utilizado por la estación base para poner al receptor en estado de hibernación o sacarlo de tal estado.
- Más: indica que el emisor tiene tramas adicionales para el receptor.
- W: especifica que el cuerpo de la trama se ha codificado utilizando el algoritmo WEP (Privacidad Inalámbrica Equivalente).
- O: indica al receptor que una secuencia de tramas que tenga este bit encendido debe procesarse en orden estricto.



La trama de datos 802.11

El segundo campo de la trama de Datos, *Duración*, indica cuánto tiempo ocuparán el canal la trama y su confirmación de recepción.

El encabezado de la trama contiene cuatro direcciones: origen y destino, las otras dos direcciones se utilizan para las estaciones base de origen y destino para el tráfico entre celdas.

El campo de *Secuencia* permite que se numeren los fragmentos. De los 16 bits disponibles, 12 identifican la trama y 4 el fragmento.

El campo *Datos* contiene la carga útil y le sigue el campo común de *Suma de verificación*.

Trama de administración: formato similar al de las tramas de datos, excepto que no tienen una de las direcciones de la estación base, debido a que las tramas de administración se restringen a una sola celda.

Tramas de control: son más cortas; tienen una o dos direcciones, y ni tienen campo de *Datos* ni de *Secuencia*. La información clave se encuentra en el campo de *Subtipo*, que por lo general es RTS, CTS o ACK.

Servicios

Cada LAN inalámbrica que se apegue al estándar 802.11 debe proporcionar nueve servicios: cinco de distribución y cuatro de estación.

Los **servicios de distribución** se relacionan con la administración de membresías dentro de la celda y con la interacción con estaciones que están fuera de la celda. Son proporcionados por las estaciones base y tienen que ver con la movilidad de la estación conforme entran y salen de las celdas, conectándose ellos mismos a las estaciones base y separándose ellos mismos de dichas estaciones. Estos servicios son:

1. *Asociación*: utilizado por las estaciones móviles para conectarse ellas mismas a las estaciones base. Se utiliza después de que una estación se mueve dentro del alcance de radio de la estación base. Una vez que llega, anuncia su identidad y sus capacidades. La estación base podría aceptar o rechazar la estación móvil. Si se acepta, dicha estación debe autenticarse.
2. *Disociación*: es posible que la estación o la estación base se disocie, con lo que se rompería la relación.
3. *Reasociación*: una estación podría cambiar su estación base preferida mediante este servicio. Si se utiliza correctamente no se perderán datos como consecuencia del cambio de estación base (handover).
4. *Distribución*: determina cómo enrutar las tramas enviadas a la estación base.
5. *Integración*: si una trama necesita enviarse a través de una red no 802.11 con un esquema de direccionamiento o formato de trama diferentes, este servicio maneja la traducción del formato

802.11 al requerido por la red destino.

Los **servicios de estación** se relacionan con la actividad dentro de una sola celda. Se utilizan después de que ha ocurrido la asociación y son los siguientes:

1. *Autenticación*: una estación debe autenticarse antes de que se le permita enviar datos. Una vez que la estación base asocia una estación móvil, le envía una trama especial de destino para ver si dicha estación móvil sabe la clave secreta (contraseña) que se le ha asignado. La estación móvil prueba que sabe la clave secreta codificando la trama de desafío y regresándola a la estación base. Si el resultado es correcto, la estación móvil se vuelve miembro de la celda.
2. *Desautenticación*: cuando una estación previamente autenticada desea abandonar la red, se desautentica.
3. *Privacidad*: para que la información que se envíe a través de una LAN inalámbrica se mantenga confidencial, debe codificarse. Este servicio maneja la codificación y la decodificación.
4. *Entrega de datos*: la transmisión de datos es la parte esencial. No se garantiza la transmisión confiable. Las capas superiores deben tratar con la detección y la corrección de errores.