**Filmina 4 REDES DE AREA LOCAL – LAN**

**APLICACIONES DE LAS REDES LAN**

1-REDES LAN de computadores personales

Una configuración de red LAN que consta de computadores personales. En particular, el coste de la conexión a la red debe ser significativamente menor que el del dispositivo conectado. Esto sugiere que la velocidad de la red puede estar limitada, ya que, en general, el coste es superior cuanto mayor sea la velocidad.

2-REDES DE RESPALDO Y ALMACENAMIENTO

Las redes de respaldo se utilizan para interconectar grandes sistemas como computadoras centrales y dispositivos de almacenamiento masivo. El requisito principal en este caso es la transferencia elevada de datos entre un número limitado de dispositivos en un área reducida, siendo también necesaria generalmente una alta fiabilidad. Entre sus características típicas se encuentran las siguientes:

**Alta velocidad:** se precisan velocidades de 100 Mbps o más.

**Interfaz de alta velocidad:** el enlace físico entre la estación y la red debe ser de alta velocidad.

**Acceso distribuido:** se necesita una técnica de control distribuido de acceso al medio (MAC, *Medium Access Control*) para permitir que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.

**Distancia limitada:** generalmente las redes de respaldo se emplean en salas de computadores.

**Número limitado de dispositivos.**

3- RED DE ALMACENAMIENTO (SAN)

Es una red independiente para gestionar las necesidades de almacenamiento. La SAN desliga las tareas de almacenamiento de servidores específicos y crea un servicio de almacenamiento compartido a través de una red de alta velocidad. Entre los dispositivos de almacenamiento puede tener discos duros, cd, etc. Si un cliente necesita acceder a un dispositivo de almacenamiento particular, el acceso debe hacerse a través del servidor que lo controla. En una SAN, por el contrario, no hay servidor alguno entre los dispositivos de almacenamiento y la red, sino que aquellos y los servidores se encuentran directamente conectados a la red. La estructura SAN mejora la eficiencia de acceso de los clientes al almacenamiento, así como las comunicaciones directas de un dispositivo de almacenamiento a otro con la finalidad de realizar copias de respaldo y replicación.

4-REDES LAN TRONCALES

El soporte de las comunicaciones de datos entre oficinas precisa de un servicio de red capaz de cubrir las distancias involucradas y de interconectar equipos situados en un mismo edificio (quizá grande) o en un conjunto de ellos. Inconvenientes si se usa solo una LAN:

* Fiabilidad.
* Costo.
* Capacidad.

**TOPOLOGÍAS Y MEDIOS DE TRANSMISIÓN**

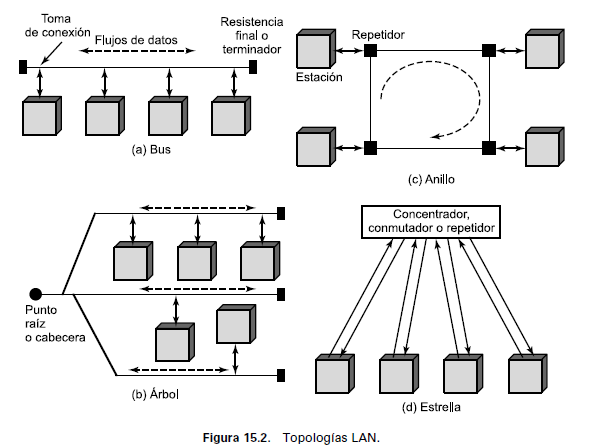
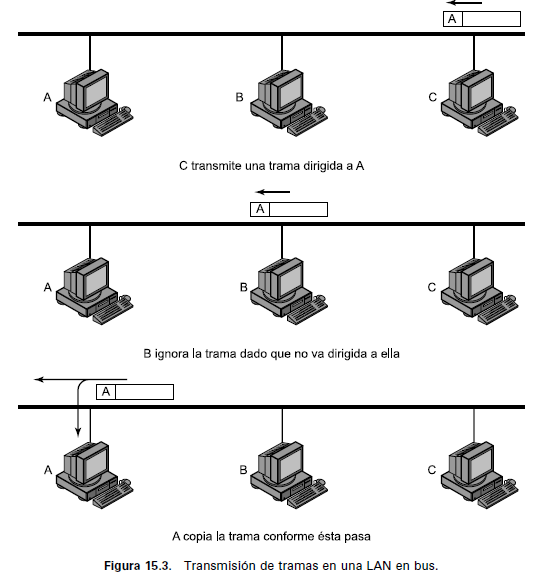
Los principales elementos de una red LAN son los siguientes:

* Topología.
* Medio de transmisión.
* Disposición.
* Técnica de control de acceso al medio.

No solo determinan el costo y capacidad de una LAN sino también los tipos de datos que pueden transmitirse, velocidad, etc.

**TOPOLOGÍAS**

Topologíase refiere a la forma según la cual se interconectan entre sí los puntos finales, o estaciones, conectados a la red. Las topologías usuales en redes LAN son bus, árbol, anillo y estrella. El bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas.



**Topologías en bus y en árbol**

Ambas topologías usan un medio multipunto.

**BUS**

Todas las estaciones se encuentran directamente conectadas al bus, cada estación tiene una única dirección. El funcionamiento *full-duplex* entre la estación y la toma de conexión permite la transmisión y la recepción de datos a través del bus. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de estaciones. En cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.

**ARBOL**

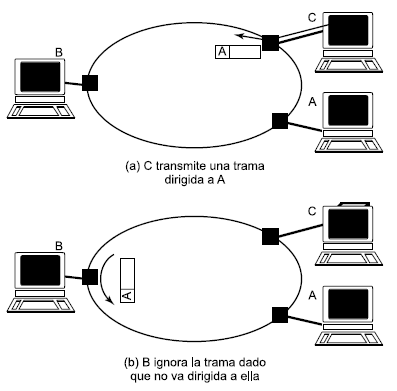
Es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados que comienza en un punto conocido como raíz o cabecera. Uno o más cables comienzan en el punto raíz y cada uno de ellos puede presentar ramificaciones. La transmisión desde una estación se propaga a través del medio y puede alcanzar al resto de estaciones.

Existen dos problemas:

* la transmisión desde una estación se puede recibir en las demás estaciones, es necesario algún método para indicar a quién va dirigida la transmisión.
* se precisa un mecanismo para regular la transmisión. Ya que si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas; también se puede considerar la situación en que una estación decide transmitir continuamente durante un largo periodo de tiempo.

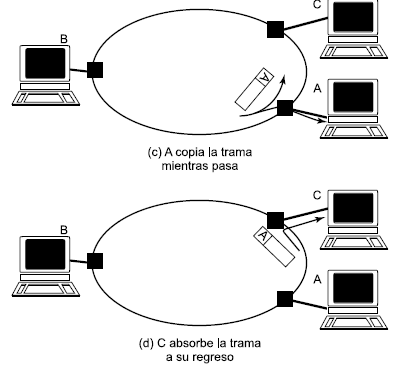
Para solucionar estos problemas, las estaciones transmiten datos en bloques pequeños llamados tramas. Cada trama consta de una porción de los datos que una estación desea transmitir además de una cabecera de trama que contiene información de control. A cada estación en el bus se le asigna una dirección, o identificador, única, incluyéndose en la cabecera la dirección destino de la trama.

Las estaciones transmiten por turnos de acuerdo con alguna forma cooperativa, no son acciones especiales para eliminar tramas del medio, cuando llega al final del bus es absorbida.

**TOPOLOGIA EN ANILLO**

La red consta de un conjunto de *repetidores* unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo, capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos. Los enlaces son unidireccionales; es decir, los datos se transmiten sólo en un sentido, de modo que éstos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario.

Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él, los datos se transmiten en tramas, Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama. La trama continúa circulando hasta que alcanza de nuevo la estación origen, donde es eliminada del medio. Dado que el anillo es compartido por varias estaciones, se necesita una técnica de control de acceso al medio para determinar cuándo puede insertar tramas cada estación.

Puede ser usada para proporcionar enlaces de muy alta velocidad sobre distancias largas. Un anillo puede proporcionar, mejor rendimiento que otra topología. Una desventaja, es que un fallo de un solo enlace o de un repetidor puede inutilizar la red entera.

**ESTRELLA**

Cada estación está directamente conectada a un nodo central común, generalmente a través de dos enlaces punto a punto, uno para transmisión y otro para recepción. Existen dos alternativas para el **funcionamiento del nodo central.** Una es el funcionamiento en modo de difusión, en el que la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central. En este caso, aunque la disposición física es una estrella, lógicamente funciona como un bus: una transmisión desde cualquier estación es recibida por el resto de estaciones, y sólo puede transmitir una estación en un instante de tiempo dado. En tal caso, al dispositivo central se le conoce como **concentrador** (*hub*). Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena temporalmente en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.

La topología en estrella se aprovecha de la disposición natural del cableado de los edificios. Generalmente, es mejor para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.

**ELECCIÓN DE LA TOPOLOGÍA**

La elección de la topología depende de varios factores entre los que se cuentan la fiabilidad de la misma, la capacidad de expansión y el rendimiento, elección del medio de transmisión, la disposición del cableado y la técnica de control de acceso. **Existen cuatro alternativas para el medio de transmisión que pueden ser utilizadas en una LAN en bus:**

**Par trenzado:** como el UTP o STP.

**Cable coaxial en banda base:** hace uso de señalización digital. El esquema original de Ethernet hacía uso de él.

**Cable coaxial en banda ancha:** utilizado en los sistemas de televisión por cable. Usa señalización analógica. Este tipo de sistema es más caro y más difícil de instalar y mantener que el cable coaxial en banda base.

**Fibra óptica:** la electrónica es costosa, es la mejor alternativa en cuanto a fiabilidad y velocidad, pero no tiene el uso masivo de UTP o STP.

**ELECCIÓN DEL MEDIO DE TRANSMISIÓN**

La elección del medio de transmisión viene determinada por una serie de factores:

* **restringida por la topología de la LAN.**
* **Capacidad:** debe soportar el tráfico de red esperado.
* **Fiabilidad:** debe satisfacer los requisitos de disponibilidad.
* **Tipos de datos soportados:** ajustados a la aplicación.
* **Alcance del entorno:** debe proporcionar servicio a la gama de entornos requeridos.

Medios de transmisión disponibles:

● UTP de alta performance

– Cat. 5 y siguientes

– Velocidades de transmisión altas para un pequeño número de dispositivos

– Estrella conmutada para redes grandes

● Fibra óptica

– Aislado de la interferencia electromagnética

– Mayor capacidad de transmisión

– Tamaño pequeño

– Costos altos de los componentes

– Mano de obra calificada para la instalación y mantenimiento

● Los precios están comenzando a bajar a medida que los productos soportan esta tecnología

**ARQUITECTURA DE PROTOCOLOS DE REDES LAN**

La arquitectura de una LAN se describe en términos de una jerarquía de protocolos que organizan las funciones básicas de la misma. La arquitectura de protocolos estandarizada para redes LAN, incluye **las capas: física, de control de acceso al medio (MAC) y de control de enlace lógico (LLC, *Logical Link Control*).** La capa física comprende la topología y el medio de transmisión, ya se vio.

**MODELO DE REFERENCIA IEEE 802**

Los protocolos definidos específicamente para la transmisión en redes LAN y MAN tratan cuestiones relacionadas con la transmisión de bloques de datos a través de la red. Según OSI, los protocolos de capas superiores (capa 3 o 4 y superiores) son independientes de la arquitectura de red y son aplicables a redes LAN, MAN y WAN. Así pues, el estudio de protocolos LAN está relacionado con las capas inferiores del modelo OSI.

Esta arquitectura fue desarrollada por el comité IEEE 802 y ha sido adoptada por todas las organizaciones que trabajan en la especificación de los estándares LAN; es la referida como el modelo de referencia IEEE 802.

La capa inferior del modelo de referencia IEEE 802 es la **capa física** del modelo OSI, e incluye funciones como:

* Codificación/decodificación de señales.
* Transmisión/recepción de bits.

Por encima de la capa física se encuentran las funciones asociadas a los servicios ofrecidos a los usuarios LAN:

**Capa de control de acceso al medio (MAC).**

* En transmisión, ensamblado de datos en tramas con campos de dirección y de detección de errores.
* En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
* Control de acceso al medio de transmisión LAN.

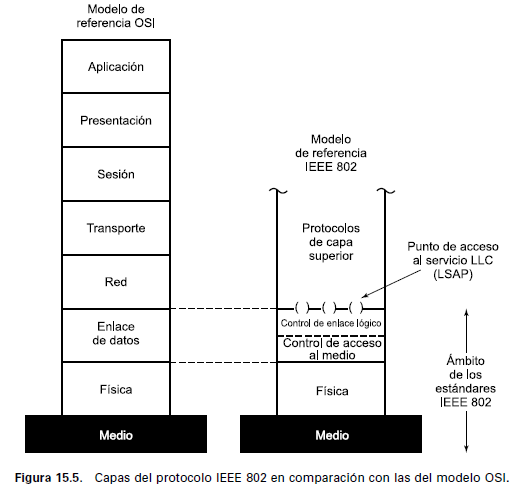
Capa de **control de enlace lógico (LLC):**

* Interfaz con las capas superiores y control de errores y de flujo.

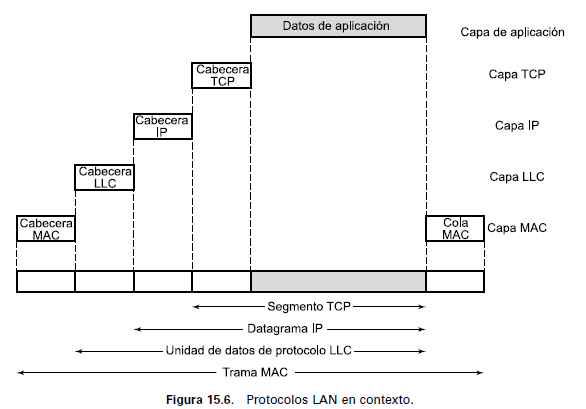
Estas funciones se asocian generalmente a la capa 2 de OSI, pero aquí se tratan en dos capas separadas.

Esta separación de funciones en la capa de enlace en MAC y LLC se debe a:

* La lógica para la gestión del acceso a un medio compartido no se encuentra en la capa 2 de control de enlace de datos tradicional.
* Se pueden ofrecer varias opciones MAC para el mismo LLC.



Los datos de nivel superior se pasan hacia abajo al nivel LLC, que añade una cabecera de información de control dando lugar a una *unidad de datos de protocolo* (PDU) *LLC*. Esta información de control se utiliza para el funcionamiento del protocolo LLC. La PDU LLC se pasa a la capa MAC, que añade información de control al principio y al final del paquete creando una *trama MAC*. Una vez más, es necesaria la información de control en la trama para el funcionamiento del protocolo MAC.



**CONTROL DEL ENLACE LÓGICO - LLC**

La capa LLC en redes LAN se encarga de la transmisión de una unidad de datos de protocolo del nivel de enlace (PDU) entre dos estaciones, sin necesitar un nodo de conmutación intermedio. LLC presenta dos características no compartidas por la mayor parte de otros protocolos de control de enlace:

**1.** Debe admitir el acceso múltiple, consecuencia de la naturaleza de medio compartido del enlace.

**2.** Delega en la capa MAC algunos detalles del acceso al enlace.

El direccionamiento en LLC implica la especificación de los usuarios LLC origen y destino. En terminología OSI, estas direcciones de usuario LLC se denominan puntos de acceso al servicio (SAP, *Ser*v*ice* *Access Point*) de las capas de nivel superior.

**Servicios LLC**

LLC especifica los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios, están basados en HDLC. Existen tres posibles servicios para dispositivos conectados que usan LLC:

**Servicio no orientado a conexión sin confirmación:** es de tipo datagrama, no incluye mecanismos de control de flujo ni de errores, por lo que no está garantizada la recepción de los datos. En cualquier caso, en la mayoría de los dispositivos existe alguna capa superior de software encargada de gestionar las cuestiones de fiabilidad.

**Servicio en modo conexión:** similar al ofrecido por HDLC. Se establece una conexión lógica entre dos usuarios que intercambian datos, existiendo control de flujo y de errores.

**Servicio no orientado a conexión con confirmación:** es una mezcla de los dos anteriores. Los datagramas son confirmados, pero no se establece conexión lógica previa.

**CONTROL DE ACCESO AL MEDIO**

Todas las LAN y MAN constan de un conjunto de dispositivos que deben compartir la capacidad de transmisión de la red, de manera que se requiere algún método de control de acceso al medio con objeto de hacer un uso eficiente de esta capacidad. Ésta es la función del protocolo de control de acceso al medio (MAC).

Los parámetros clave en una técnica de control de acceso al medio son **dónde y cómo.** ***Dónde***se refiere a si el control se realiza de forma centralizada o distribuida. En un esquema **centralizado** se diseña un controlador para conceder el acceso a la red, de modo que una estación que desee transmitir debe esperar hasta que se le conceda permiso por parte del controlador.

En una red **descentralizada,** las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán.

Ventajas de un sistema centralizado:

* Puede mejorar el control de acceso proporcionando prioridades, rechazos y capacidad garantizada.
* Genera un punto de falla; es decir, existe un punto en la red tal que si se produce un fallo en él, fallará toda la red.
* Puede actuar como un cuello de botella, reduciendo las prestaciones.

Los pro y contras de los esquemas distribuidos son los contrarios a los puntos anteriores.

El segundo parámetro, ***cómo*,** viene impuesto por la topología y factores como el coste, las prestaciones y la complejidad. Se puede clasificar las técnicas de control de acceso como **síncronas o asíncronas.**

Con las técnicas síncronas:

* se dedica una capacidad dada a una conexión. (aproximación usada en conmutación de circuitos)
* Estas técnicas no son óptimas en redes LAN y MAN dado que las necesidades de las estaciones son impredecibles.

Técnicas asíncronas:

* posibilidad de reservar capacidad de forma asíncrona (dinámica), es decir, en respuesta a las demandas de cada conexión.
* La aproximación asíncrona se puede subdividir en tres categorías: rotación circular, reserva y contención.

**Rotación circular**

Se le da a cada estación la oportunidad de transmitir, ante lo que la estación puede declinar la proposición o puede transmitir sujeta a un límite superior, especificado generalmente en términos de cantidad de datos a transmitir o tiempo para ello. En cualquier caso, cuando la estación termina debe ceder el turno de transmisión a la siguiente estación en la secuencia lógica. El control de secuencia puede ser centralizado o distribuido. Cuando varias estaciones disponen de datos a transmitir durante un largo periodo de tiempo, las técnicas de rotación circular pueden resultar muy eficientes.

En cambio, pueden ser preferibles otras técnicas dependientes de si el tráfico de datos es a ráfagas o continúo. El tráfico continuo se caracteriza por transmisiones largas y razonablemente continuas; algunos ejemplos son la comunicación de voz. Por su parte, el tráfico a ráfagas se caracteriza por transmisiones cortas y esporádicas, como en el caso de tráfico interactivo terminal-estación.

**Reserva**

Son adecuadas para tráfico continuo. En estas técnicas se divide el tiempo en ranuras, una estación que desea transmitir reserva futuras ranuras para un largo, incluso indefinido, periodo de tiempo. Una vez más, las reservas se pueden llevar a cabo de forma centralizada o distribuida.

**Contención**

Apropiadas para tráfico a ráfagas. En estas técnicas no se realiza control para determinar de quién es el turno, sino que todas las estaciones compiten. Estas técnicas son distribuidas, radicando su principal ventaja en el hecho de que son sencillas de implementar y eficientes en condiciones de carga baja o moderada.

**Formato de trama MAC**

La capa MAC recibe un bloque de datos de la capa LLC y debe realizar funciones relacionadas con el acceso al medio y la transmisión de datos. MAC implementa estas funciones haciendo uso de una unidad de datos de protocolo (PDU) a la que se denomina trama MAC. Los campos de esta trama son:

**Control MAC:** información de control de protocolo necesaria para el funcionamiento del protocolo MAC.

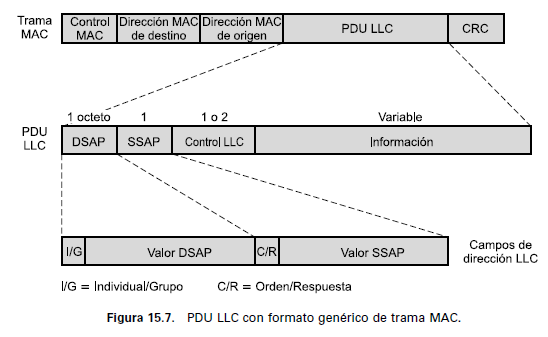
**Dirección MAC de destino:** punto de conexión física MAC en la LAN del destino de la trama.

**Dirección MAC de origen:** punto de conexión física MAC en la LAN del origen de la trama.

**LLC:** datos LLC de la capa inmediatamente superior.

**CRC:** campo de comprobación de redundancia cíclica, es un código de detección de errores.

Las dos funciones típicas de una capa de enlace se dividen entre las capas MAC y LLC:

* La capa MAC es responsable de la detección de errores y del rechazo de tramas erróneas.
* La capa LLC opcionalmente controla qué tramas han sido recibidas correctamente y retransmite las erróneas.

DSAP= SAP destino.

SSAP= SAP fuente o emisor

Estos son campos de 7 bits.

**Formato de la MAC address**

* 6 octetos únicos
* Expresada en hexadecimal
* Distribución de las direcciones octetos bajo la ieee
* Grabada físicamente en la placa

**INTERCONEXION DE REDES LAN**

Para poder **expandir los límites de una red LAN** y poder interconectar con otras LAN, se tiene 2 opciones: **puentes (bridges) o dispositivos de encaminamiento (router).**

**PUENTES o BRIDGES**

* Expanden o interconectan redes LAN.
* Su uso es sencillo.
* Permite interconexión de LANs similares
  + Diseñados para LANs con protocolos idénticos en las capas físicas y de enlace.
  + Volumen de procesamiento mínimo.

**Dispositivo de encaminamiento o ROUTER**

* Propósito general.
* Permiten interconexión de redes LAN y WAN.

**FUNCIONES DE LOS PUENTES**

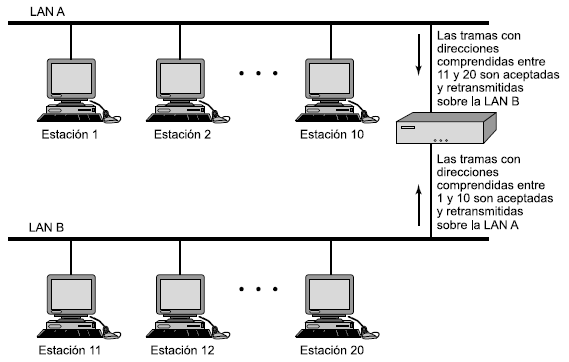
Se ilustra el funcionamiento de un puente que conecta dos redes LAN, A y B, que utilizan el mismo protocolo MAC. Las funciones del puente son pocas y sencillas:

* Lectura de todas las tramas transmitidas en una LAN y aceptación de aquellas dirigidas a estaciones en otra LAN.
* Retransmisión hacia otra LAN de cada una de las tramas, haciendo uso del protocolo de control de acceso al medio de esta LAN.
* Utilizando la dirección MAC retransmite cada trama.

Merece la pena resaltar varios aspectos del diseño de los puentes:

* El puente no modifica el contenido o formato de las tramas que recibe ni las encapsula con una cabecera adicional. Cada trama es copiada de una LAN a la otra dado que las dos LAN usan los mismos protocolos.
* El puente debe disponer de suficiente memoria para demandas pico.
* El puente debe presentar capacidad de direccionamiento y de encaminamiento. Como mínimo, debe conocer las direcciones de cada red para determinar qué tramas debe pasar. Además, pueden existir más de dos redes LAN interconectadas por varios puentes, en cuyo caso puede ser necesario encaminar una trama a través de varios puentes.
* Un puente puede conectar más de dos LAN.

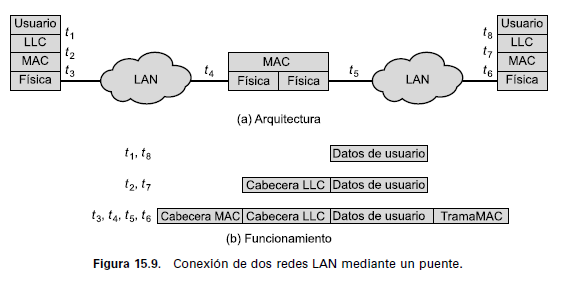
El puente permite ampliar las LAN sin modificar el software de las estaciones conectadas a ellas. Desde el punto de vista de cada una de las estaciones en las dos (o más) LAN, **parece como si sólo existiese una única red LAN en la que cada estación tiene una dirección única.** Las estaciones utilizan esa dirección única y no necesitan discriminar explícitamente entre estaciones en la misma o en diferentes LAN; el puente se encarga de ello.



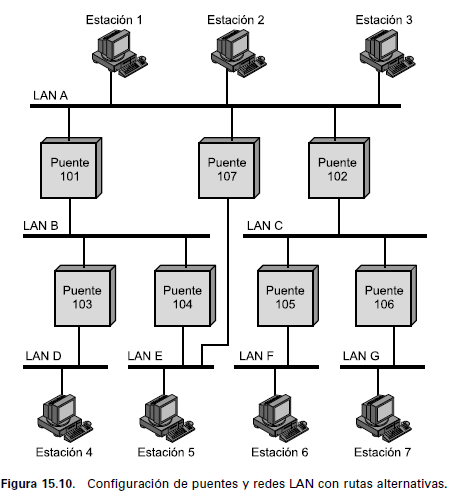
**ARQUITECTURA DE PROTOCOLOS DE LOS PUENTES**

IEEE 802.1D define la arquitectura de protocolos para puentes MAC. La dirección final o de estación se establece en el nivel MAC, de modo que es a este nivel al que puede funcionar un puente. Poe Ej, en dos LAN conectadas con los mismos protocolos MAC y LLC por un único puente. El puente captura las tramas MAC cuyo destino no se encuentra en la LAN de origen, las almacena temporalmente y las transmite sobre la otra LAN. La capa LLC no contiene el puente ya que su función es la retransmisión de las tramas MAC.

En la Figura se indica la forma en que se encapsulan los datos en un puente. Éstos se ofrecen al protocolo LLC por parte de algún usuario. La entidad LLC añade una cabecera y pasa la unidad de datos resultante a la entidad MAC, que añade una cabecera y una cola para dar lugar a una trama MAC. El puente captura la trama de acuerdo con la dirección MAC de destino especificada en ella y, dado que su función es retransmitirla intacta a la LAN destino, no elimina los campos MAC. De esta forma, la trama se deposita en la LAN destino y es capturada por la estación destino.



**ENCAMINAMIENTO ESTÁTICO**

Existe una tendencia en muchas organizaciones hacia un aumento del número de redes LAN interconectadas mediante puentes. Cuanto mayor es este número, más importante resulta proporcionar rutas alternativas entre LAN a través de puentes.

El puente debe disponer de capacidad de encaminamiento, de modo que cuando un puente recibe una trama debe decidir si llevar a cabo o no su retransmisión. Si el puente se encuentra conectado a dos o más redes, debe decidir si retransmitir la trama o no y, en su caso, sobre qué LAN hacerlo.

La capacidad de encaminamiento debe tener en consideración la topología de la configuración de interconexión entre redes y puede requerir ser alterada dinámicamente

Se han propuesto varias técnicas de encaminamiento. La más sencilla es la de **encaminamiento estático**. Esta estrategia resulta adecuada para un número pequeño de redes LAN e interconexiones estables. IEEE 802 han desarrollado especificaciones para estrategias de encaminamiento. El grupo IEEE 802.1 ha propuesto una normalización de encaminamiento basada en el uso del algoritmo del **árbol de expansión** (*spanning tree*),

En el **encaminamiento estático** se selecciona una ruta para cada pareja de LAN origen-destino en la configuración. Si se dispone de rutas alternativas entre dos LAN, generalmente se selecciona aquella con menor número de saltos. Las rutas son fijas, o al menos sólo cambian cuando se produce un cambio en la topología de la interconexión.

La estrategia es similar a la empleada en una red de conmutación de paquetes. Se crea una matriz de encaminamiento central, que indica, para cada pareja de LAN origen-destino, la identidad del primer puente en la ruta. Luego se consultando de nuevo la matriz, para obtener el siguiente salto hasta finalmente, obtener la ruta directa al destino.

Las tablas de encaminamiento se pueden obtener a partir de esta matriz y se guardan en cada puente. Cada puente precisa una tabla para cada una de las LAN a las que está conectado. La información de cada tabla se obtiene a partir de una sola fila de la matriz. Por ejemplo, el puente 105 tiene dos tablas, una para las tramas recibidas de la LAN C y otra para las de la LAN F. La tabla muestra, para cada dirección MAC destino posible, la identidad de la LAN a la que el puente debería enviar la trama.

Una vez establecidas las tablas, el encaminamiento es una tarea sencilla. Un puente copia las tramas procedentes de cada una de sus LAN. Si la dirección MAC de destino corresponde con una entrada de su tabla de encaminamiento, la trama se retransmite a través de la LAN apropiada. La estrategia de encaminamiento estático necesita la carga manual de las tablas de encaminamiento.

**TÉCNICA DEL ÁRBOL DE EXPANSIÓN (ENCAMINAMIENTO DINAMICO)**

Mecanismo en el que los puentes desarrollan automáticamente una tabla de encaminamiento y la actualizan en respuesta a cambios en la topología. El algoritmo consta de tres mecanismos: retransmisión de tramas, aprendizaje de direcciones y mecanismo para evitar bucles.

**Retransmisión de tramas**

Un puente mantiene una **base de datos de retransmisión** para cada puerto de conexión a una LAN, que indica las direcciones de estación para las que las tramas deben transmitirse sobre un puerto dado. Es decir, para cada puerto se mantiene una lista de estaciones situadas en el «mismo lado» del puente que el puerto.

Cuando se recibe una trama por uno de los puertos, el puente debe decidir si la trama se enviará a través suyo y sobre cuál de los otros puertos se realizará la retransmisión. Suponiendo que un puente recibe una trama MAC a través del puerto *x*, se aplican las siguientes reglas:

**1.** Búsqueda en la base de datos de para determinar si la dirección MAC se asocia a un puerto distinto de ***x***.

**2.** Si no se encuentra la dirección MAC destino, la trama se envía a través de todos los puertos excepto por el que llegó.

**3.** Si la dirección de destino se encuentra en la base de datos para algún puerto ***y***, se determina si ese puerto se encuentra en estado de bloqueo o de envío.

**4.** Si el puerto ***y***no está bloqueado, se transmite la trama a través de ese puerto sobre la LAN a la que se encuentra conectado.

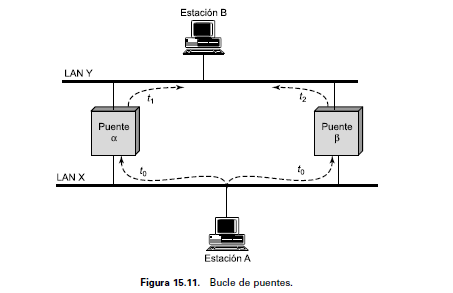
**Aprendizaje de direcciones**

El esquema se basa en la existencia en los puentes de una base de datos de retransmisión que indica la dirección de cada estación destino desde el puente en cuestión. Esta información puede cargarse en el puente. Sería deseable un mecanismo automático para aprender las direcciones de cada estación. Un esquema sencillo para conseguir esta información se basa en el empleo del campo de dirección origen presente en las tramas MAC.

Cuando se recibe una trama por un puerto dado. El campo de dirección origen de la trama indica la estación emisora, de modo que un puente puede actualizar su base de datos de retransmisión a partir de esa dirección MAC. Con el fin de permitir cambios en la topología, cada entrada en la base de datos dispone de un temporizador. Cuando se añade una nueva entrada a la base de datos, se activa el temporizador asociado. Si éste expira, se elimina la entrada de la base de datos dado que la información de dirección correspondiente puede no ser válida por más tiempo. Cada vez que se recibe una trama se comprueba su dirección origen en la base de datos. Si se encuentra como entrada ya en ésta, se actualiza (la dirección puede haber cambiado) y se reinicia el temporizador. Si la entrada, por el contrario, no está en la base de datos, se crea una nueva con su propio temporizador.

**Algoritmo del árbol de expansión**

El mecanismo de aprendizaje de direcciones descrito es efectivo si la topología de la interconexión de redes es un árbol; es decir, si no existen rutas alternativas en la red. La existencia de rutas alternativas implica la aparición de bucles cerrados.



Para solucionar este problema se usa la teoría de grafos:

* Para cualquier grafo conectado, compuesto de nodos y de terminales que conectan cada par de nodos, existe un árbol de expansión de terminales que mantiene la conectividad del grafo pero no contiene bucles cerrados.
* cada red LAN se corresponde con un nodo del grafo y cada puente con una arista.
* Es deseable un algoritmo mediante el que los puentes de la interconexión puedan intercambiar información suficiente para obtener el árbol de expansión.
* El algoritmo debe ser dinámico; es decir, los puentes deben ser capaces de percatarse ante un cambio en la topología y obtener automáticamente un nuevo árbol de expansión.

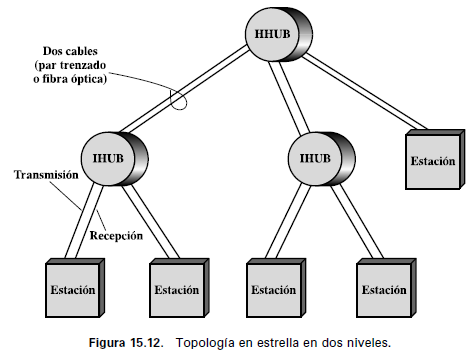
Características del algoritmo:

* El algoritmo del árbol de expansión puede desarrollar dicho árbol de expansión.
* Cada uno de los puentes tenga asignado un identificador único y se asocien costes a cada uno de los puertos de los puentes.
* El algoritmo implica el intercambio de un número reducido de mensajes entre todos los puentes para obtener el árbol de expansión de mínimo coste.
* Cuando se produzca un cambio en la topología, los puentes recalcularán automáticamente el árbol de expansión.

**CONMUTADORES DE LA CAPA 2 Y LA CAPA 3**

Existen diversos tipos de dispositivos utilizados para la interconexión de redes LAN además de los puentes. Estos dispositivos pueden ser clasificados en dos categorías: conmutadores de la capa 2 y conmutadores de la capa 3 (**switch de la capa 2 y 3**).

**CONCENTRADORES o HUB**

En una LAN con topología en estrella. El concentrador es un elemento activo que actúa como elemento central de la estrella. Cada estación se conecta al concentrador mediante dos enlaces (transmitir y recibir). El concentrador actúa como un repetidor: cuando transmite una única estación, el concentrador replica la señal hacia cada estación. El enlace consiste en dos pares trenzados no apantallados. La longitud de un enlace está limitada a en torno a 100 m. Como alternativa, se puede usar un enlace de fibra óptica, en cuyo caso la longitud máxima es del orden de 500 m.

Aunque es físicamente una estrella, funciona lógicamente como un bus: una transmisión por parte de una estación se recibe en el resto de estaciones y se produce colisión si dos estaciones transmiten al mismo tiempo.

Varios niveles de concentradores se pueden poner en cascada formando una configuración jerárquica.

Existe un **concentrador raíz** y uno o más **concentradores intermedios.**

Cada concentrador puede ser una mezcla de estaciones y otros concentradores conectados a él.

Esta estructura se adecúa bien a edificios cableados, donde, generalmente, existe un armario de interconexiones en cada planta del edificio, pudiendo colocarse un concentrador en cada una de ellas.

**CONMUTADORES DE LA CAPA 2 o SWITCH DE CAPA 2**

Los conmutadores de capa 2, desplazaron a los concentradores en el contexto de las redes LAN de alta velocidad.

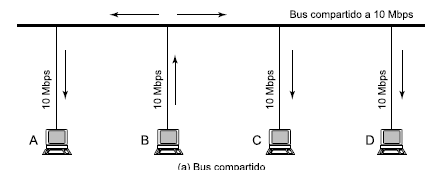
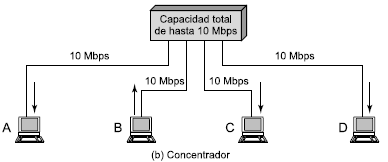
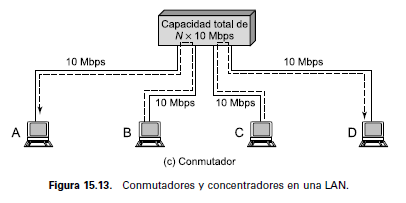
Para aclarar la distinción entre concentradores y conmutadores:

Configuración BUS:

1. todas las estaciones deben compartir la capacidad total del bus, que es de 10 Mbps.
2. Solo una estación puede transmitir a la vez.

Configuración estrella con HUB:

1. Todas las estaciones se conectan al HUB.
2. La transmisión de una estación se recibe en el concentrador y se retransmite sobre todas las líneas de salida.
3. Para evitar la ocurrencia de colisión, sólo una estación puede transmitir en un momento dado.
4. la capacidad total de la LAN es de 10 Mbps.



Se pueden mejorar las prestaciones mediante el uso de un conmutador de la capa 2:

* el hub actúa como un conmutador, de forma análoga a un conmutador de paquetes o de circuitos.
* Una trama que ingresa desde una estación dada es conmutada hacia la correspondiente línea de salida.
* Las líneas desocupadas se pueden usar para otras conexiones vivas.
* Puede transmitir más de una estaciona la vez.
* Multiplica la capacidad de la LAN.

Beneficios de **SWITCH de capa 2:**

**1.** No se necesita cambiar el software ni el hardware de los dispositivos conectados para convertir una LAN en bus o una LAN con un concentrador en una LAN con un conmutador.

**2.** se asume que el switch tiene la capacidad suficiente para atender a todos los dispositivos conectados.

* cada uno de ellos tiene una capacidad dedicada igual a la de la LAN original completa. Si el conmutador puede dar un rendimiento de 20 Mbps, parece como si cada dispositivo conectado tuviese una capacidad dedicada de entrada o salida de 10 Mbps.

**3.** El conmutador de la capa 2 permite escalar de forma Simple, se pueden conectar dispositivos adicionales a él mediante el incremento correspondiente de su capacidad.

Existen dos tipos de CONMUTADORES O SWITCH:

**Conmutador de almacenamiento y envío (*store-and-forward switch*):** el conmutador acepta una trama sobre una línea de entrada, la almacena temporalmente y después la rutea sobre la línea de salida correspondiente.

**Conmutador rápido (*cut-through switch*):** el conmutador aprovecha que la dirección de destino se encuentra al comienzo de la trama MAC, tan pronto como reconozca la dirección de destino empieza a transmitir sobre la linea de salida adecuada.

El conmutador de tipo rápido permite el mayor rendimiento posible, aunque a riesgo de propagar tramas erróneas dado que no es capaz de comprobar el campo CRC.

Un conmutador de la capa 2 puede ser visto como una versión *full-duplex* de un concentrador, pudiendo incorporar además la lógica necesaria para funcionar como un puente multipunto. Se enumeran las siguientes diferencias entre puentes y conmutadores de la capa 2:

* La gestión de las tramas en un puente se hace por software, mientras que un conmutador de la capa 2 lleva a cabo el reconocimiento de direcciones y el reenvío de tramas por hardware.
* Por lo general, un puente sólo puede analizar y retransmitir las tramas de una en una, mientras que un conmutador de la capa 2 tiene varias rutas de datos que actúan en paralelo, pudiendo así manejar múltiples tramas simultáneamente.
* Un puente utiliza siempre un mecanismo de almacenamiento y envío, mientras que un conmutador de la capa 2 puede funcionar en modo rápido (*cut-through*).

En las LANs es común encontrar configuraciones con un conmutador de capa 2 que efectúa las funciones de un puente, en lugar de un puente.

**CONMUTADORES DE LA CAPA 3**

**Problemas de los switch de capa 2:**

A medida que el número de dispositivos crece, los conmutadores de capa 2 muestran deficiencias. Presentan dos problemas fundamentales: sobrecarga de difusión (broadcast) y falta de enlaces múltiples.

Un conjunto de dispositivos y redes LAN conectados por un conmutador de capa 2 **tienen el mismo espacio de direccionamiento plano.** El término ***plano***hace referencia a que todos los usuarios comparten una dirección de difusión común (dirección de broadcast MAC). De esta forma, si un dispositivo emite una trama MAC con una dirección de difusión, la trama será entregada a todos los dispositivos conectados a la red interconectados por switch capa 2 o puentes. En una red grande, una tasa de tramas de difusión elevada puede crear una sobrecarga tremenda. Se puede dar un caso aún peor, conocido como *tormenta de difusión*: un dispositivo defectuoso que inserte continuamente tramas de difusión llega a congestionar completamente la red.

El segundo problema de rendimiento concerniente al uso de puentes o switch de capa 2 las normativas en vigor prohíben la existencia de bucles cerrados en la red. Dicho de otro modo, sólo puede existir un único camino entre cualesquiera dos dispositivos. Esto impide que cualquier implementación que se adecue a los estándares proporcione múltiples caminos entre dispositivos, limitando así tanto el rendimiento como la fiabilidad de la red.

Una es dividir una red local grande en una serie de **subredes** conectadas entre mediante *routers*. Así, una trama MAC de difusión queda restringida únicamente a aquellos dispositivos y switch que pertenecen a la misma subred. Además, los routers basados en IP emplean algoritmos de encaminamiento sofisticados que toleran la existencia de varios caminos entre subredes a través de diferentes dispositivos de encaminamiento.

**Problemas de los routers**

El uso de routers presenta problemas de rendimiento:

* realizan todo el procesamiento IP relacionado con la retransmisión por software. Las redes LAN de alta velocidad y los switch de altas prestaciones pueden transmitir millones de paquetes por segundo, mientras que un router basado en software maneja por debajo de un millón de paquetes por segundo.

**La solución son los switch de capa 3 o dispositivos de encaminamiento** que implementan la lógica de retransmisión de paquetes en hardware.

Existen 2 categorías de conmutadores de capa 3:

* paquete a paquete
* basados en flujos.

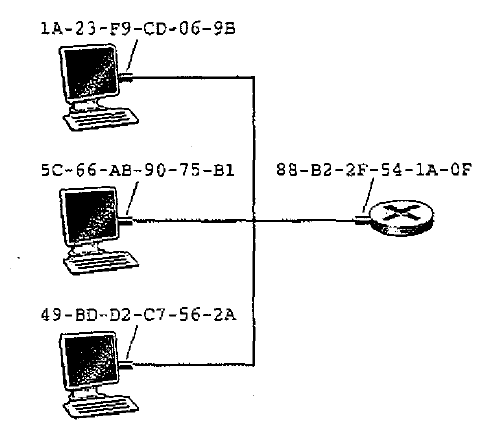
**Un conmutador tipo paquete a paquete** opera de la misma forma que los routers tradicionales. Como la lógica de retransmisión está en el hardware, el conmutador puede incrementar el rendimiento, en comparación con un router que lo haga por software.

**Un conmutador basado en flujos** trata de mejorar el rendimiento mediante la identificación de flujos de paquetes IP que poseen las mismas direcciones de origen y de destino. Esta tarea se realiza observando el tráfico de salida, o bien mediante una etiqueta de flujo en la cabecera de cada paquete (existente en IPv6). Una vez que un flujo es identificado, es posible establecer una ruta predefinida a través de la red para acelerar el proceso de retransmisión. De esta forma se consigue un incremento en el rendimiento con respecto a un dispositivo de encaminamiento puramente basado en software.

**Direccionamiento de la capa de enlace**

Los nodos (hosts y routers) tienen direcciones de la capa de enlace (MAC), los nodos tienen también direcciones de la capa de red (IP). El Protocolo de resolución de direcciones (ARP*),* que proporciona un mecanismo para traducir las direcciones IP en direcciones de la capa de enlace (MAC).

**Direcciones MAC**

* Las direcciones de la capa de enlace (denominada MAC) se asignan a los adaptadores instalados en cada nodo.
* La dirección MAC tiene **6** bytes de longitud, lo que nos da 2^(**48)** posibles direcciones MAC.
* estas direcciones de **6** bytes suelen expresarse en notación hexadecimal, indicándose cada byte de la dirección mediante una pareja de números hexadecimales.
* Aunque las direcciones MAC se diseñaron para ser permanentes, hoy día es posible modificar la dirección MAC de un adaptador mediante un software apropiado.

Una propiedad de las direcciones MAC es que nunca puede haber dos adaptadores con la misma dirección. El IEEE se encarga de gestionar el espacio de direcciones MAC. Cuando una empresa quiere fabricar adaptadores, compra por un precio fijado una parte del espacio de direcciones compuesto por 2^(**24)** direcciones. IEEE asigna el fragmento de 2**24** direcciones fijando los primeros 24 bits de una dirección MAC y dejando que la empresa diseñe combinaciones únicas de los últimos 24 bits para cada adaptador.

La dirección MAC de un adaptador nunca varia independientemente de a donde se lleve el adaptador, tiene **PORTABILIDAD**.

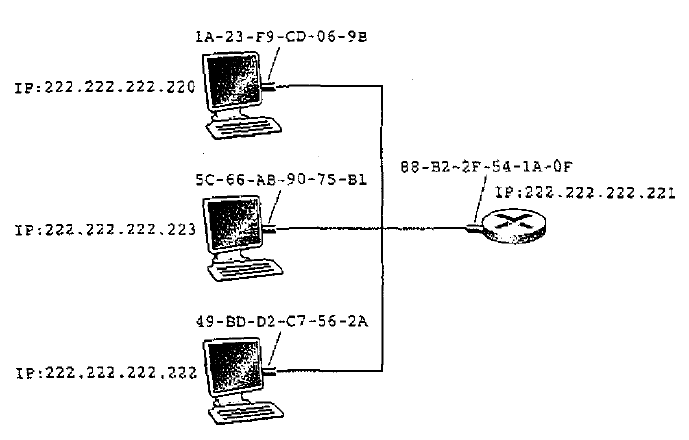
Las direcciones IP tienen una estructura jerárquica (es decir, una parte de red y una parte de host) y que es necesario modificar la dirección IP de un nodo cuando el host se mueve, es decir, cuando cambia la red a la que el host está conectado, no tiene portabilidad.

Cuando un adaptador de un emisor quiere enviar una trama a otro adaptador de destino, inserta la dirección MAC del destino en la trama y luego la envía a través de la red LAN. Si la red LAN es de difusión, la trama será recibida y procesada por todos los adaptadores de la LAN. Cada adaptador que reciba la trama comprobara si la dirección MAC de destino contenida en la trama corresponde con su dirección MAC. Si existe una correspondencia, el adaptador extraerá el datagrama incluido en la trama y lo pasara hacia arriba por la pila de protocolos para entregárselo a su nodo padre. Si no hay una correspondencia entre ambas direcciones, el adaptador descarta la trama, sin pasar el datagrama de la capa de red hacia arriba por la pila de protocolos. De este modo, solo el nodo de destino será interrumpido cuando se reciba la trama.

Si un adaptador de un emisor quiere que todos los demás adaptadores de la LAN reciban y *procesen* la trama que va a enviar. El adaptador emisor inserta una dirección de difusión MAC especial en el campo de la dirección de destino de la trama. Para las redes LAN que utilizan direcciones de **6** bytes, la dirección de difusión es una cadena compuesta por 48 unos (1) consecutivos (es decir, FF-FF-FF-FF-FF-FF en notación hexadecimal).

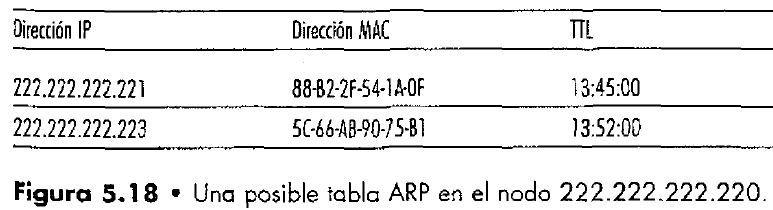
**Protocolo de resolución de direcciones (ARP)**

Como existen tanto direcciones de la capa de red (IP) como direcciones de la capa de enlace (MAC), surge la necesidad de una traducción entre ellas. En Internet, esta tarea la lleva a cabo el **Protocolo de resolución de direcciones (ARP).**

Una red donde cada nodo tiene una dirección IP única y el adaptador de cada nodo tiene una dirección MAC única, si un nodo desea enviar un datagrama IP a otro nodo. Si tanto el nodo de origen como el destino se encuentran en la misma red (LAN). Para enviar un datagrama, el nodo de origen tiene que proporcionar a su adaptador no solo el datagrama IP sino también la dirección MAC del nodo de destino. El adaptador del nodo emisor construirá entonces una trama de la capa de enlace que contendrá la dirección MAC del nodo destino y enviara la trama a la red LAN.

El nodo de origen para determinar la dirección MAC del nodo de destino, usa el protocolo ARP. **Un módulo ARP en el nodo emisor toma como entrada cualquier dirección IP de la misma LAN y devuelve la dirección MAC correspondiente.**

**ARP resuelve direcciones IP solo para los nodos de una misma subred.**

Cada nodo (host o router) tiene en su memoria una tabla ARP, que contiene las correspondencias entre las direcciones IP y las direcciones MAC. La tabla ARP también contiene un valor de tiempo de vida (TTL), que indica cuando se eliminara cada correspondencia de la tabla. La tabla no necesariamente contiene una entrada para cada nodo de la subred; algunos nodos pueden haber tenido entradas que han caducado, mientras que otros puede que nunca hayan tenido una entrada en la tabla.

Ejemplo de funcionamiento de ARP

Si el nodo 222.222.222,220 quiere enviar un datagrama con direccionamiento IP a otro nodo de dicha subred. El nodo emisor necesita obtener la dirección MAC del nodo de destino a partir de la dirección IP de dicho nodo. Esto es fácil si la tabla ARP del nodo emisor tiene una entrada para nodo de destino. Pero, si la tabla ARP no contiene una entrada para el nodo de destino, el nodo 222.222.222.220 desea enviar un datagrama al nodo 222.222.222. 222. En este caso, el nodo emisor utiliza el protocolo ARP para resolver la dirección.

Primero, el nodo emisor construye un paquete **ARP query o consulta.** **Un paquete ARP contiene las direcciones MAC e IP del emisor y el receptor.** Los paquetes de consulta y de respuesta ARP tienen el mismo formato. El propósito del paquete de consulta ARP es consultar a todos los demás nodos de la subred para determinar la dirección MAC de la dirección IP que está resolviendo.

El nodo 222.222.222.220 pasa un paquete de consulta ARP al adaptador con la indicación de que envié el paquete a la dirección de difusión MAC, FF-FF-FF-FF-FF-FF. El adaptador encapsula el paquete ARP en una trama de la capa de enlace, utiliza la dirección de difusión para la dirección de destino de la trama y la transmite a la subred.

La trama que contiene la consulta ARP es recibida por todos los demás adaptadores existentes en la subred y cada adaptador pasa la consulta ARP contenida en la trama al módulo ARP de dicho nodo. Cada nodo realiza una comprobación para ver si su dirección IP se corresponde con la dirección IP de destino del paquete ARP. El único nodo en el que se produzca la coincidencia devolverá al nodo que ha realizado la consulta una respuesta ARP con la correspondencia deseada.

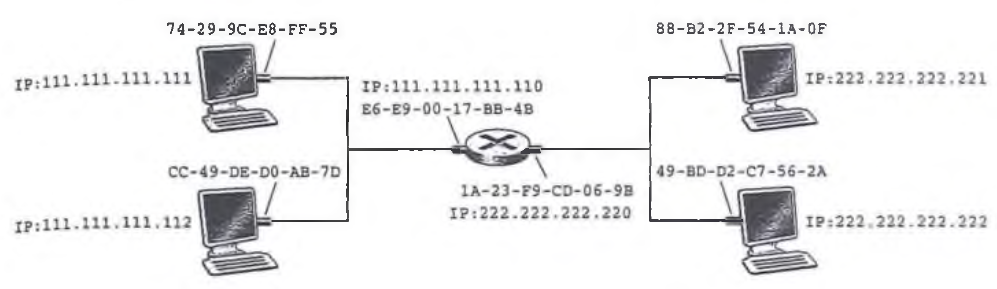
El nodo que ha realizado la consulta podrá entonces actualizar su tabla ARP y enviar su datagrama IP, encapsulado dentro de una trama de la capa de enlace cuya dirección de destino MAC es la del nodo que ha contestado a la anterior consulta ARP.

Características de ARP:

* el mensaje ARP de consulta se envía en una trama de difusión, mientras que el mensaje ARP de respuesta se envía en una trama estándar.
* ARP es un protocolo plug-and-play; es decir, la tabla ARP de un nodo se construye automáticamente. Y si un nodo esta desconectado de la subred, su entrada finalmente se elimina de las tablas de los restantes nodos de la subred.

Se preguntan si ARP es un protocolo de la capa de enlace o un protocolo de la capa de red. Un paquete ARP se encapsula dentro de una trama de la capa de enlace y así se sitúa, encima de la capa de enlace. Sin embargo, un paquete ARP dispone de campos que contienen direcciones de la capa de enlace, por lo que se podría decir que es un protocolo de la capa de enlace, pero también contiene direcciones de la capa de red y, por tanto, podría también argumentarse que es un protocolo de la capa de red. En último término, probablemente ARP sea considerado un protocolo que se encuentra a caballo entre las capas de enlace y de red. (Solo leer este párrafo).

**Envió de un datagrama a un nodo fuera de la subred**

Si un nodo de una subred desea enviar un datagrama de la capa de red a un nodo que de otra subred(a través de un router a otra subred). 2 subredes conectadas por un router.

Existen dos tipos de nodos: hosts y routers. Cada host tiene una dirección IP y un adaptador. Un router tiene una dirección IP para *cada* unade sus interfaces. Para cada interfaz de router existe también un módulo ARP (en el router) y un adaptador. Dado que el router de la Figura 5.19 tiene dos interfaces, tendrá dos direcciones IP, dos módulos ARP y dos adaptadores, cada adaptador de la red tiene su propia dirección MAC.

Si un nodo de la subred 1 (ej 111.111.111.111) desea enviar un datagrama IP a un nodo de la 2 (host 222.222.222.222). El host emisor pasa el datagrama a su adaptador, el host emisor debe indicar a su adaptador una dirección MAC de destino.

Para que el datagrama vaya desde el nodo de la subred 1 a un nodo de la Subred 2, el datagrama tiene en primer lugar que ser enviado a la interfaz de router (111.111.111.110, que es la dirección IP del router del primer salto en el camino hacia su destino final). Por tanto, la dirección MAC apropiada para la trama es la dirección del adaptador de la interfaz de router (111.111.111.110, es decir, E**6** - E9-00-17-BB-4B).

El host de emisor obtiene la dirección MAC para la dirección de la interfaz del router (111.111.111.110) usando ARP. Una vez que el adaptador del emisor tiene esta dirección MAC, crea una trama (que contiene el datagrama direccionado a 222.222.22.22) y envía la trama hacia la Subred 1. El adaptador del router de la Subred 1 ve que la trama de la capa de enlace se dirige hacia él y, por tanto, pasa la trama a la capa de red del router.

El diagrama IP se ha transmitido desde el host de origen al router. El datagrama debe ir ahora desde el router al destino. El router tiene que determinar la interfaz correcta a la que el datagrama será reenviado. Esto se hace consultando la tabla de reenvió del router. La tabla de reenvió indica al router que el datagrama es reenviado a través de la interfaz de router 222.222.222.220. Esta interfaz entonces pasa el datagrama a su adaptador, que encapsula el datagrama en una nueva trama y la envía a la subred 2. Esta vez, la dirección MAC de destino de la trama es la dirección MAC del destino final. El router obtiene esta dirección MAC de destino a través de ARP.

**Filmina 5 LANs de alta velocidad**

**Protocolos de acceso múltiple**

Existen 2 tipos de enlace, **punto a punto** formado por un emisor y un receptor en cada extremo, un enlace de difusión, puede tener múltiples nodos emisores y receptores, todos conectados al mismo y único canal de difusión compartido; cuando un nodo transmite una trama, el canal se encarga de difundir esa trama y cada uno de los demás nodos recibe una copia.

Un problema en la capa de enlace es como coordinar el acceso de múltiples nodos emisores y receptores a un canal de difusión compartido, lo que se conoce con el nombre de **problema de acceso múltiple.**

El problema crucial es determinar quién es el que tiene derecho a transmitir hacia el canal y cuando lo tiene.

Las redes de computadoras tienen protocolos **denominados protocolos de acceso múltiple** mediante los cuales los nodos se encargan de regular sus transmisiones al canal de difusión compartido.

Puesto que todos los nodos son capaces de transmitir tramas, podría darse el caso de que más de dos nodos transmitieran tramas al mismo tiempo. Cuando esto sucede, todos los nodos reciben varias tramas simultáneamente; es decir, las tramas transmitidas colisionan en todos los receptores. Normalmente, cuando se produce una colisión ninguno de los nodos receptores puede interpretar ninguna de las tramas transmitidas;

Para poder garantizar que el canal de difusión realice un trabajo útil aun cuando haya múltiples nodos activos, es necesario **coordinar** de alguna manera las **transmisiones** de esos nodos activos. Este trabajo de coordinación es responsabilidad del protocolo de acceso múltiple.

Los protocolos de acceso múltiple se clasifican en:

* Protocolos de particionamiento del canal.
* Protocolos de acceso aleatorio.
* Protocolos de toma de recursos o turnos.

Un protocolo de acceso múltiple para un canal de difusión con una velocidad de R bps, características deseables:

1. Cuando sólo haya un nodo que tenga datos para enviar se le asignará los R bps.

2. Cuando haya M nodos para transmitir, cada uno tendrá una tasa de transferencia de R/M bps (tasa media de trasmisión).

3. El protocolo será descentralizado; es decir, no habrá ningún nodo maestro.

4. el protocolo será simple.

**Protocolos de particionamiento del canal**

Multiplexación por división en el tiempo (TDM)

El canal da soporte a *N* nodos y la tasa de transmisión del canal es igual a *R* bps. TDM divide el tiempo en marcos temporales y *luego* subdivide cada marco temporal en *N* particiones de tiempo. Cada partición de tiempo se asigna entonces a uno de los *N* nodos. Cada vez que un nodo tenga un paquete para enviar, transmite los bits del paquete durante su partición de tiempo asignada, dentro del marco TDM que se repite de forma cíclica.

TDM elimina las colisiones y es divide equitativamente el ancho de banda. Dos inconvenientes: cada nodo está limitado a una tasa promedio de *R/N* bps, aunque sea el único nodo que tiene paquetes para transmitir. El segundo es que un nodo siempre tiene que esperar a que le llegue el tumo dentro de la secuencia de transmisión; es obligatorio aun cuando sea el único nodo que tenga una trama que enviar.

La multiplexación por división de frecuencia (FDM)

FDM divide el canal de *R* bps en diferentes frecuencias (cada una con un ancho de banda de *R/N)* y asigna cada frecuencia a cada uno de los *N* nodos. FDM comparte con TDM tanto las ventajas como los inconvenientes. Cada nodo está limitado a un ancho de banda de *R/N,* incluso cuando sea el único nodo que tienen paquetes para enviar.

**Protocolos de acceso aleatorio**

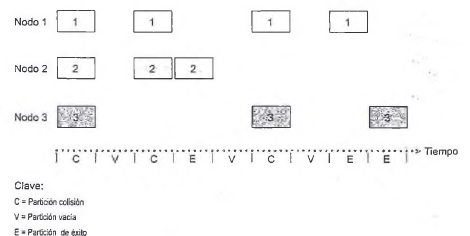
En estos, cada nodo transmite siempre a la máxima velocidad del canal. Cuando se produce una colisión, cada nodo implicado retransmite repetidamente su trama hasta que la trama consiga pasar sin sufrir colisiones. Cuando un nodo experimenta una colisión tal vez no retransmite la trama de forma inmediata. En lugar de ello, espera durante un tiempo aleatorio antes de retransmitir la trama.Cada nodo implicado en una colisión selecciona un retardo aleatorio independientemente. Puesto que los retardos aleatorios son elegidos de forma independiente, es posible que uno de los nodos seleccione un retardo que sea suficientemente menor que los retardos de los otros nodos que han intervenido en la colisión, pudiendo así ser capaz de conseguir que su trama pase a través del canal sin experimentar una nueva colisión. Entre ellos ALOHA, CSMA, CSMA/CD.

**ALOHA**

Una estación transmite una trama siempre que lo necesite.

Luego, la estación pasa a escuchar el medio durante un tiempo igual al máximo retardo de propagación posible de ida y vuelta a través de la red más un pequeño incremento fijo de tiempo. La trama se envió con éxito si durante este intervalo de escucha la estación escucha una confirmación; en caso contrario, retransmitirá la trama.

La estación desistirá si no recibe una confirmación después de varias retransmisiones. Si la trama es válida y la dirección de destino en la cabecera de la trama coincide con la de la receptora, la estación devuelve inmediatamente una confirmación. La trama puede ser incorrecta debido a la presencia de ruido en el canal o debido a que otra estación transmitiera una trama casi al mismo tiempo. En este último caso, las dos tramas pueden interferir entre sí en el receptor, de modo que no se acepte ninguna; esto se conoce como **colisión**.

**ALOHA ranurado:** El tiempo del canal se hace discreto, considerando ranuras uniformes de duración igual al tiempo de transmisión de una trama. Es necesario el uso de un reloj central u técnica que permita sincronizar todas las estaciones. La transmisión sólo se permite en los instantes de tiempo que coincidan con el comienzo de una ranura. Así, las tramas que se solapen lo harán completamente, lo que incrementa la utilización máxima del sistema.

El funcionamiento del protocolo ALOHA con particiones en cada nodo es simple:

• Cuando el nodo tiene una nueva trama que enviar, espera hasta el comienzo de la siguiente partición y transmite la trama completa dentro de la partición.

• SI no se produce una colisión, el nodo habrá transmitido correctamente su trama.

• Si se produce una colisión, el nodo detecta la colisión antes de que la partición termine. El nodo intentara retransmitir su trama en cada partición posterior hasta conseguir que la trama sea transmitida sin experimentar colisiones. En cada partición el nodo determina si va a intentar retransmitir la trama o no, en caso de no repite lo mismo para la siguiente partición.

**CSMA- ACCESO MULTIPLE CON DETECCION DE PORTADORA**

Si el tiempo de propagación es pequeño comparado con el de transmisión, cuando una estación transmita una trama, el resto de estaciones lo sabrá casi inmediatamente. De esta manera, no intentarán transmitir hasta que lo haya hecho la primera. Las colisiones no serán habituales, ya que sólo ocurrirán cuando dos estaciones comiencen a transmitir casi simultáneamente.

CSMA se desarrolló en base a esto. Una estación que desee transmitir escucha el medio para determinar si existe alguna otra transmisión en curso. Si el medio está siendo usado, la estación deberá esperar. En cambio, si éste se encuentra libre, la estación podrá transmitir. Si dos o más estaciones intentan transmitir casi al mismo tiempo, se producirá colisión. Para solucionar esto, las estaciones esperan una cantidad de tiempo después de transmitir en espera de una confirmación, teniendo en consideración el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión y retransmite.

Efectiva para redes en las que el tiempo de transmisión de trama es mucho mayor que el de propagación.

Para tramas largas o tiempo de propagación cortos se mejora la utilización del canal.

**CSMA/CD**

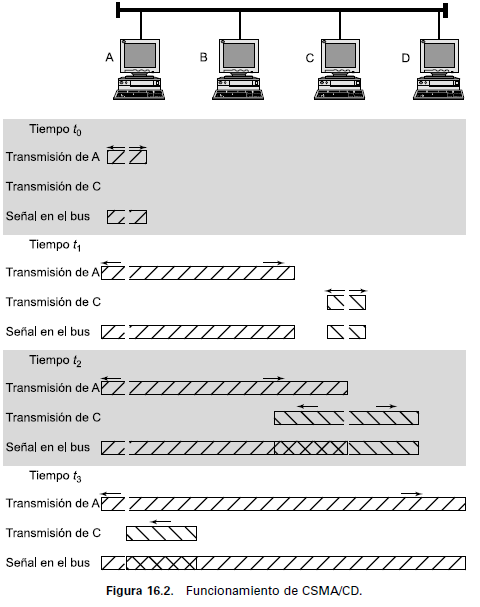
CSMA tiene un problema, cuando dos tramas colisionan, el medio permanece inutilizable mientras dure la transmisión de ambas tramas dañadas, la cantidad de tiempo desaprovechado puede ser considerable.

Este desaprovechamiento de la capacidad puede reducirse si una estación continúa escuchando el medio mientras dure la transmisión. La inclusión de esta característica conduce a las siguientes reglas para CSMA/CD:

**1.** Si el medio está libre, transmite; sino paso 2.

**2.** Si el medio está ocupado, escucha hasta que se desocupe, luego transmite.

**3.** Si se detecta una colisión durante la transmisión, se transmite una señal de interferencia para las estaciones detecten la colisión. Luego, se deja de transmitir.

**4.** luego de la colisión, la estación espera una cantidad de tiempo aleatoria conocida como **espera** (*backoff)*, intentando transmitir de nuevo a continuación (volviendo al paso 1).

La cantidad de tiempo desaprovechado se reduce al tiempo que se necesita para detectar una colisión.

Una regla importante, consiste en que la trama debe ser lo suficientemente larga como para permitir la detección de la colisión antes de que finalice la transmisión. Si se usan tramas más cortas, no se produce la detección de la colisión.

Para asegurar que la espera mantenga la estabilidad, se usa la **espera exponencial binaria,** enesta técnica, la estación intentará transmitir cada vez que colisione:

* Durante los primeros 10 intentos de retransmisión, el valor medio del tiempo de espera se dobla cada vez.
* A partir de ahí, este valor permanece igual durante 6 intentos adicionales.
* Después de 16 intentos sin éxito, la estación abandona e informa de un error.

De esta forma, a medida que la congestión crece, las estaciones esperan para transmitir periodos de tiempo cada vez más largos, reduciendo así la probabilidad de una colisión. En condiciones de baja carga, garantiza que una estación puede usar el canal tan pronto como éste se libere. Pero provoca un efecto de último-en-llegar, primero-en-salir: las estaciones sin colisiones o con muy pocas tendrán una oportunidad de transmitir antes de aquellas que llevan esperando más tiempo.

**Protocolos de toma de turnos**

**ANILLO CON PASO DE TESTIGO (Token Ring)**

El estándar IEEE 802.5 de anillo con paso de testigo fue creado por IBM.

Un anillo tiene repetidores, cada uno conectado a otros dos formando así un único camino cerrado. Los datos se transmiten alrededor del anillo desde un repetidor hasta el siguiente. Cada repetidor regenera cada bit y lo retransmite.

Para que un anillo funcione como una red de comunicaciones son necesarias tres funciones que son llevadas a cabo por los repetidores: inserción de datos, recepción de datos y eliminación de datos.

Un paquete puede ser eliminado por el repetidor destino o por el repetidor que lo emitió después de que haya dado una vuelta completa en el anillo. Existen dos estados en los que se puede encontrar un repetidor: estado de escucha y estado de transmisión.

En el estado de escucha cada bit recibido se retransmite con un pequeño retardo, necesario para permitir al repetidor realizar las funciones básicas como búsqueda de patrones de bits, copia de cada bit entrante y su envió a la estación, modificación de un bit mientras circula.

Cuando la estación dispone de datos a transmitir y el repetidor al que se encuentra conectada tiene permiso para hacerlo, este último entra en estado de transmisión. En este estado el repetidor recibe bits de la estación y los retransmite por la línea de salida.

Un tercer estado, estado de cortocircuito (*bypass*), resulta útil. En este estado se puede activar un cortocircuito, de manera que las señales propagadas atraviesan el repetidor sin más retardo que el de propagación en el medio. Ventajas: solución al problema de fiabilidad, y mejora las prestaciones al eliminar los retardos del repetidor para aquellas estaciones del medio que no se encuentren activas.

**La técnica de anillo con paso de testigo,** se basa en el uso de una trama pequeña, denominada testigo (*token*), que circula cuando todas las estaciones están libres. Cuando una estación desea transmitir debe esperar a que le llegue el testigo. En este caso, toma el testigo cambiando uno de sus bits, lo que lo convierte en la secuencia de comienzo de las tramas de datos. Posteriormente, la estación añade y transmite el resto de campos requeridos en la construcción de la trama.

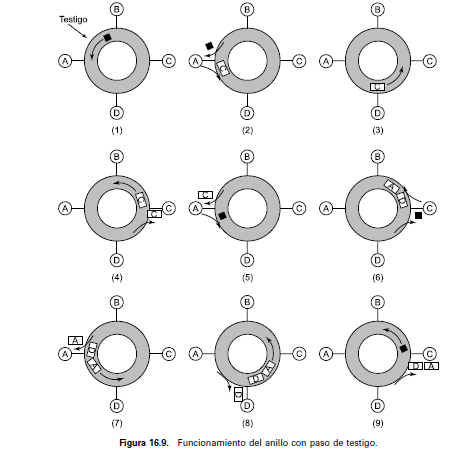
Cuando una estación toma el testigo y comienza a transmitir, el testigo deja de estar presente en el anillo, de manera que el resto de estaciones que deseen transmitir deben esperar. La trama en el anillo realiza una vuelta completa y se absorbe en la estación transmisora, que insertará un nuevo testigo en el anillo cuando se cumplan las dos condiciones siguientes:

* La estación ha terminado la transmisión de su trama.
* Los bits iniciales de la trama transmitida hayan vuelto a la estación (después de una vuelta completa al anillo).

Una vez que se ha insertado un nuevo testigo en el anillo, la siguiente estación en la secuencia que disponga de datos a transmitir podrá tomar el testigo y llevar a cabo la transmisión. Este método es ineficiente para poca carga.

Ventajas:

* Control de acceso flexible.
* Puede proporcionar prioridades y servicio con ancho de banda garantizado.

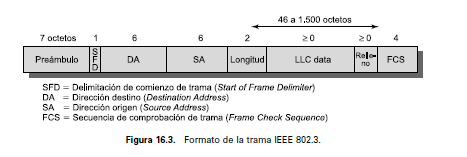


**ETHERNET IEEE 802.3**

Las redes LAN de altas velocidades utilizadas en la actualidad son las basadas en Ethernet, desarrolladas por el comité de estándares IEEE 802.3. Existe una capa de control de acceso al medio y una capa física.

**FORMATO DE LA TRAMA IEEE 802.3 Estructura de la trama de Ethernet**

Para el envió de un datagrama IP desde un host a otro host, estando ambos hosts en la misma red LAN Ethernet, el adaptador del emisor encapsula el datagrama IP dentro de una trama Ethernet y pasa dicha trama a la capa física, que la envía a la red LAN. El adaptador del receptor recibe la trama de la capa física, extrae el datagrama IP y lo pasa a la capa de red. No se establece un acuerdo previo entre los adaptadores de los hosts. Campos de la trama:



* **Campo de datos (46 a 1.500 bytes).**Este campo transporta el datagrama IP. Si se tiene menos de 46 bytes, se rellena hasta 46 bytes y se usa el **campo de longitud** por parte de la capa de red para eliminar el relleno.
* **Dirección de destino (6 bytes).**Este campo contiene la dirección MAC del adaptador de destino.
* **Dirección de origen (6 bytes).** Este campo contiene la dirección MAC del adaptador que transmite la trama hacia la LAN.
* **Campo de tipo (2 bytes).** El campo de tipo permite a Ethernet multiplexar los protocolos de la capa de red.
* **Comprobación de. redundancia cíclica (CRC) (4 bytes).** permite que el adaptador del receptor detecte los errores de bit de la trama.
* **Preámbulo (8 bytes).** La trama Ethernet comienza con el campo preámbulo de 8 bytes. Cada uno de los siete primeros bytes tiene el valor 10101010 y el último byte tiene el valor 10101011. Los siete primeros bytes sirven para “despertar” a los adaptadores de recepción y sincronizar sus relojes con el reloj del emisor. Los últimos 2 bits del octavo byte del preámbulo alertan al adaptador B de que va a llegar “información importante”.

Específicamente, cuando el adaptador B recibe una trama procedente del adaptador A ejecuta una comprobación CRC de la trama, pero ni envía un mensaje de reconocimiento cuando la trama pasa la comprobación CRC, ni envía un mensaje de reconocimiento negativo cuando la comprobación CRC falla. Cuando una trama no pasa la comprobación CRC, el adaptador B simplemente la descarta. Por tanto, el adaptador A no sabe si la trama que ha transmitido ha llegado al adaptador B y ha superado la comprobación CRC.

**CSMA/CD: protocolo de acceso múltiple de Ethernet / ETHERNET Y CSMA/CD**

Cuando los nodos están interconectados mediante un concentrador, la LAN Ethernet es una LAN de difusión; es decir, cuando un adaptador transmite una trama, todos los adaptadores de la LAN reciben esa trama. Dado que Ethernet puede emplear la comunicación por difusión, necesita un protocolo de acceso múltiple. Ethernet utiliza CSMA/CD. CSMA/CD hace lo siguiente:

1. Un adaptador puede comenzar a transmitir en cualquier instante; es decir, no existe el concepto de partición de tiempo.

2. Un adaptador nunca transmite una trama cuando detecta que algún otro adaptador está transmitiendo; es decir, utiliza un mecanismo de sondeo de portadora.

3. Un adaptador que está transmitiendo aborta su transmisión tan pronto como detecta que otro adaptador también está transmitiendo; es decir, utiliza un mecanismo de detección de colisiones.

4. Antes de intentar llevar a cabo una retransmisión, un adaptador espera un intervalo de tiempo aleatorio que normalmente es más pequeño que el tiempo que se tarda en transmitir una trama.

**Tecnologías Ethernet**

Existen muchas versiones diferentes de Ethernet como 10BASE-T, 10BASE-2, 100BASE-T, 1000BASE-LX y 10GBASE-T, todas están formadas por un acrónimo donde, la primera parte del acrónimo es la velocidad de transmisión, en este caso, 10 Mbps, 100 Mbps, 1gbps, 10gbps. La segunda parte se refiere al método de señalización, en este caso BASE se refiere a la tecnología Ethernet en banda base. La parte final del acrónimo especifica el medio físico, Ethernet puede emplear varios medios físicos como coaxial, fibra, par, etc. La T hace referencia al par trenzado.

10BASE-2: usa cable coaxial de 50 ohm, la longitud máxima es de 500m.

10BASE-T: usa UTP no apantallado en una topología estrella, la longitud está limitada a 100 m.

**Tecnologías fast Ethernet**

Son especificaciones de la IEEE 802.3 para proporcionar una LAN de bajo costo compatible con Ethernet a 100 Mbps, alternativas:

* **100BASE-X:** emplean 2 enlaces físicos entre los nodos, uno para Tx y otro para Rx:
  + 100BASE-TX: 2 pares trenzados, STP o UTP de categoría 5.
  + 100BASE-FX: dos cables de fibra óptica.
* **10GBASE-T:** estandarizado en 2007, permite operar sobre UTP.

**Funcionamiento full-duplex de ETHERNET**

Una red Ethernet tradicional es *semi-duplex*: una estación puede transmitir o recibir tramas, pero no al mismo tiempo. En el modo de funcionamiento *full-duplex*, una estación puede transmitir y recibir al mismo tiempo, de manera que una Ethernet a 100 Mbps en *full-duplex* alcanzaría, teóricamente, una velocidad de 200 Mbps.

Son necesarios cambios para funcionar en *full-duplex*. Las estaciones deben tener adaptadores *full-duplex*. El punto central en la topología en estrella debe ser un conmutador. En este caso, cada estación constituye un dominio de colisión separado. De hecho, las colisiones no se producen y el algoritmo CSMA/CD no es necesario. Se sigue utilizando, sin embargo, el mismo formato de trama MAC 802.3 y las estaciones pueden continuar ejecutando el algoritmo CSMA/CD a pesar de que jamás se detectará una colisión.

**Redes de área local virtuales (VLAN) imágenes en filminas**

Las redes LAN modernas suelen estar configuradas de forma jerárquica, teniendo cada grupo de trabajo su propia red LAN conmutada conectada a las redes LAN conmutadas de los otros grupos a través de una jerarquía de conmutadores. Problemas:

* **Falta de aislamiento del tráfico**: Aunque la jerarquía localiza el tráfico del grupo dentro de un mismo conmutador, el tráfico de difusión tiene que atravesar toda la red institucional. Limitar el ámbito del tráfico de difusión mejoraría el rendimiento de la LAN.
* **Uso ineficiente de los conmutadores***.* Si en lugar de tres grupos la institución tiene 10 grupos, entonces se necesitarían 10 conmutadores de primer nivel. Un único conmutador de muchos puertos podría ser lo suficientemente grande como para acomodar a todo el mundo, pero este único conmutador no proporcionaría la funcionalidad de aislamiento del tráfico.
* **Gestión de los usuarios.** Si un empleado se mueve entre grupos, el cableado físico debe modificarse para conectar al empleado a un conmutador diferente.

Estas desventajas pueden ser abordadas por un conmutador compatible con redes de área local virtual (VLAN, Virtual Local Area Network). Un conmutador compatible con redes VLAN permite definir múltiples redes de área local virtuales sobre una única infraestructura de red de área local física. Los hosts de una VLAN se comunican entre sí como si sólo ellos (y ningún otro host) estuvieran conectados al conmutador. En una VLAN basada en puertos, el administrador de la red divide los puertos (interfaces) del conmutador en grupos. Cada grupo constituye una VLAN, con los puertos de cada VLAN formando un dominio de difusión (es decir, el tráfico de difusión de un puerto sólo puede llegar a los demás puertos del grupo).

El administrador de la red declara que un puerto pertenece a una determinada VLAN utilizando un software de gestión de conmutadores; en el conmutador se mantiene una tabla de correspondencias entre puertos y redes VLAN y el hardware del conmutador solo entrega tramas entre puertos que pertenecen a la misma VLAN. La pertenencia a una VLAN se define por SW.

¿Cómo puede enviarse el tráfico del departamento IE al departamento CC? seria conectando un puerto del conmutador VLAN a un router externo y configurando dicho puerto para que pertenezca tanto a la VLAN IE como a la VLAN CC. Un datagrama IP enviado desde el departamento IE al departamento CC primero atravesaría la VLAN IE para llegar al router y luego sería reenviado por el router por la VLAN CC hasta el host de CC. Hoy en día está incorporado en el mismo dispositivo el conmutador VLAN y un router.

Un método para poder interconectar 2 conmutadores que tienen las mismas VLAN, agrupar estaciones conectadas a conmutadores distintos en una VLAN, consiste en interconectar los conmutadores VLAN utilizando la técnica conocida como troncalizacion VLAN (VLAN *Trunking).* Un puerto especial de cada conmutador se configura como un puerto troncal para interconectar los dos conmutadores VLAN. El puerto troncal pertenece a todas las VLAN y las tramas enviadas a cualquier VLAN son reenviadas a través del enlace troncal hacia el otro conmutador. Para que cada conmutador identifique a que VLAN pertenece cada trama, se definió un formato de la trama ETHERNET ampliado, 802.1Q, la trama 802.1Q está formada por la trama estándar de Ethernet más una etiqueta VLAN añadida a la cabecera que contiene la identidad de la VLAN a la que pertenece la trama.

El conmutador del lado emisor de un enlace troncal VLAN añade la etiqueta VLAN a la trama, la cual es analizada y eliminada por el conmutador del lado receptor del enlace troncal. La etiqueta VLAN en si consta de un campo Identificador de protocolo de etiquetado, un campo Información de control de etiquetado, que contiene un campo identificador de VLAN y un campo de prioridad.

**Ventajas**

 Fácil mantenimiento y resolución de problemas

 Minimización de errores

 Tablas de enrutamiento reducidas

 Dominio de fallas finito

 Diseño escalable

**Razones para implementar VLAN**

 Agrupar usuarios

 Seguridad

 QoS

 Evitar enrutamiento

**Configurar una vlan**

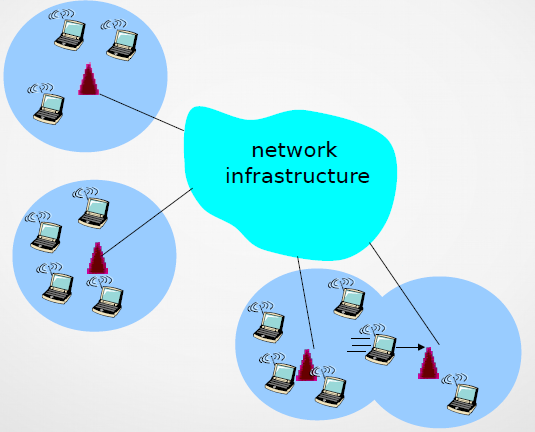
 Puerto Troncal (VLAN Trunking)

 Puerto de Acceso

**Filmina N°6 Redes LAN inalámbricas**

Dentro de una red inalámbrica podemos identificar los siguientes elementos:

**- Hosts inalámbricos***.* Son los dispositivos que actúan como sistemas terminales y que ejecutan las aplicaciones. Ej, notebooks, PDA, un teléfono o una computadora de escritorio. Los hosts en si pueden ser móviles o no.

**- Enlaces inalámbricos***.* Un host se conecta a una estación base o a otro host inalámbrico a través de un enlace de comunicaciones inalámbrico. Las diferentes tecnologías de enlace inalámbrico tienen distintas velocidades de transmisión y pueden transmitir a diferentes distancias.

**- Estación base***.* Es responsable de enviar y recibir datos hacia y desde un host inalámbrico que este asociado con esa estación base. Sera responsable de coordinar la transmisión de los múltiples hosts inalámbricos que estén asociados con ella. Un host inalámbrico esta “asociado” con una estación base, significa que el host se encuentra dentro de la distancia máxima de comunicación inalámbrica de la estación base y el host utiliza la estación base para reenviar datos hacia y desde la red de mayor tamaño. Ej, torres de telefonía celular, puntos de acceso a redes LAN. La estación base puede estar conectada a una red de mayor tamaño funcionando así como retransmisor de la capa de enlace.

Modos de operación en las redes inalámbricas:

* **Modo de infraestructura:** los hosts asociados con una estación base operan en este modo, los servicios tradicionales de red son proporcionados por la red con la que un host se conecta a través de la estación base.
* **Redes ad hoc:** Los hosts inalámbricos no tienen ninguna infraestructura a la que conectarse. En ausencia de dicha infraestructura, los propios hosts tienen que proporcionar servicios tales como el enrutamiento, la asignación de direcciones, etc.

Cuando un host móvil se desplaza fuera del alcance de una estación base y entra dentro del área de cobertura de otra, cambia su punto de conexión con la red de mayor tamaño (es decir, cambia la estación base con la que está asociado); este proceso se conoce con el nombre de transferencia (handoff). Esto plantea problemas como, averiguar la ubicación actual del host, direccionamiento, enrutamiento, etc.

**- Infraestructura de red.** Esta es la red de mayor tamaño con la que un host inalámbrico puede querer comunicarse.

Estos elementos pueden combinarse de muchas formas distintas para componer distintos tipos de redes inalámbricas. Se puede clasificar las redes inalámbricas según dos criterios: si un paquete dentro de la red inalámbrica realiza exactamente **un salto inalámbrico o varios saltos inalámbricos** y si existe una **infraestructura** o no, ej una estación base, dentro de la red:

**• Redes basadas en infraestructura y un único salto.**Estas redes tienen una estación base conectada a una red cableada de mayor tamaño. Toda la comunicación se realiza entre esta estación base y un host inalámbrico, con un único salto inalámbrico. Incluye redes 802.11, las redes de telefonía celular y las redes 802.16 WiMAX.

**• Redes sin infraestructura y un único salto.**No existe una estación base conectada a una red inalámbrica. Uno de los nodos de esta red puede coordinar las transmisiones de los restantes nodos. Incluye Bluetooth y las redes 802.11 en modo ad hoc.

• **Redes basadas en infraestructura y múltiples saltos.**Existe una estación base que esta cableada a la red de mayor tamaño. Algunos nodos inalámbricos pueden tener que retransmitir sus comunicaciones a través de otros nodos inalámbricos con el fin de comunicarse a través de la estación base. Ej sensores inalámbricos y redes de malla inalámbricas.

• **Redes sin infraestructura y múltiples saltos.** No existe una estación base y los nodos pueden tener que retransmitir sus mensajes a través de otros diversos nodos para alcanzar un cierto destino. Los nodos también pueden ser móviles, con lo que la conectividad entre los nodos ira variando, lo que constituye una clase de redes conocidas con el nombre de redes **móviles ad hoc***.*

**Características de las redes y enlaces inalámbricos**

Si se reemplaza una Ethernet cableada por una red inalámbrica no hace falta cambios en la capa de red ni en las capas superiores. Pero no así en la capa de enlace. Distinciones de importancia entre un enlace cableado y un enlace inalámbrico:

**•Intensidad decreciente de la señal***.* La señal se atenúa a medida que va atravesando la materia lo que da como resultado una intensidad de señal decreciente a medida que se incrementa la distancia entre el emisor y el receptor.

**• Interferencias de otros orígenes***.* Los orígenes que transmiten en la misma banda de frecuencia interferirán entre sí, competencia por el medio físico. Por ejemplo, los teléfonos inalámbricos a 2,4 GHz y las redes LAN inalámbricas 802.11b transmiten en la misma banda de frecuencias. El ruido presente en el entorno también puede provocar interferencias.

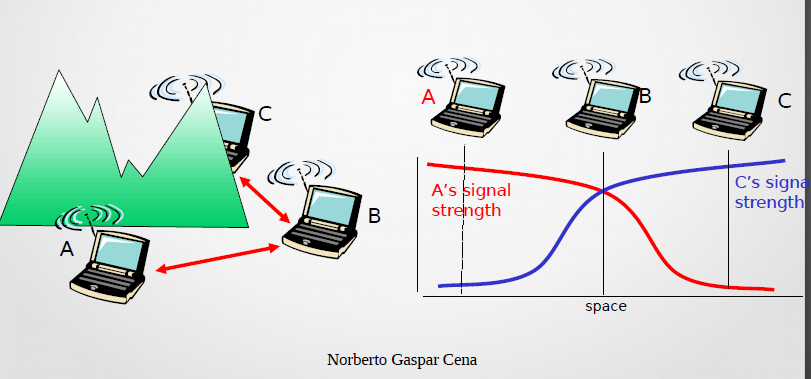
**• Propagación multicamino***:* Se da cuando partes de la onda electromagnética se reflejan en los objetos y en el suelo, tomando caminos de diferentes longitudes entre un emisor y un receptor. Esto hace que la señal recibida sea menos limpia en el receptor.

**•** Los errores de bit serán más comunes en los enlaces inalámbricos que en los enlaces cableados. Los protocolos de enlace inalámbrico empleen potentes códigos CRC para la detección de errores, y protocolos de la capa de enlace con transferencia de datos fiable que se encargan de retransmitir las tramas corrompidas.

**•** El host recibe una señal electromagnética que es una combinación de una forma degradada de la señal original transmitida por el emisor y del ruido de fondo presente en el entorno. **La relación señal-ruido (SNR)** es una medida relativa de la intensidad de la señal recibida y de este ruido. Cuanto mayor sea la SNR más fácil es para el receptor extraer la señal transmitida del ruido de fondo.

**•** En el caso de los enlaces cableados de difusión, todos los nodos reciben las transmisiones realizadas por los restantes nodos. En el caso de los enlaces inalámbricos, la estación A está transmitiendo hacia la estación B. Suponga también que la estación C está transmitiendo hacia la estación B. Con el **problema del terminal oculto**, las obstrucciones físicas presentes en el entorno (por ejemplo, una montaña o un edificio) pueden impedir que A y C escuchen las transmisiones del otro, incluso aun cuando las transmisiones de A y C estén interfiriéndose mutuamente en el destino B.

**•**Un segundo escenario que da como resultado la presencia de colisiones indetectables en el receptor es el debido al desvanecimiento de la intensidad de 2da señal a medida que esta se propaga a través del medio inalámbrico. A y C están colocadas de tal forma que sus señales no son lo suficientemente intensas como para que puedan ambas estaciones detectar las transmisiones de la otra, a pesar de lo cual esas señales *tienen* una intensidad suficiente como para interferir entre sí en la estación B.



**WiFi: redes LAN inalambricas 802.11**

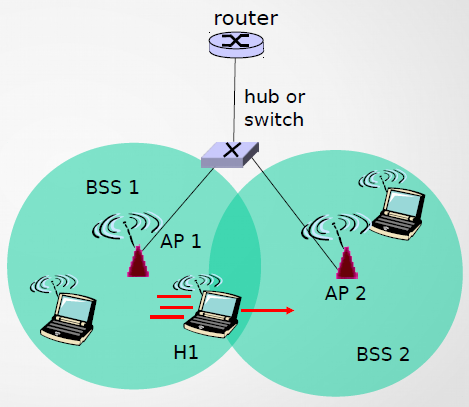
Un estándar de las redes LAN inalambricas es la IEE 802.11 conocida como red WiFi. Existen varios estándares 802.11 para la tecnología LAN inalámbrica, incluyendo:

* **802.11b:** opera a 2,4-2,485 GHz sin licencia y velocidades de hasta 11 Mbps.
* **802.11a:** Opera a 5,1-5,8 GHz licenciado - Velocidades de hasta 54Mbps. Distancia más corta y afectada por la propagación multicamino.
* **802.11g:** Opera a 2,4-2,485 GHz - Velocidades de hasta 54Mbps.
* **802.11n:** En proceso de estandarización – antenas Multiple-entrada Multiple-salida (MIMO), 2 o más antenas en el emisor y 2 o más en el receptor que están transmitiendo y recibiendo. - Velocidades de hasta 200Mbps.

Hay disponibles diversos dispositivos en modo dual (802.1 la/g) y trimodo (802.11a/b/g).

Los tres estándares 802.11 comparten características:

* emplean el mismo protocolo de acceso al medio, CSMA/CA.
* comparten la misma estructura de trama para la capa de enlace.
* Tienen la capacidad de reducir su velocidad de transmisión para poder alcanzar mayores distancias.
* permiten trabajar tanto “en modo de infraestructura” como en “modo ad hoc”.

**La arquitectura 802.11**

Componentes de la arquitectura de una red LAN inalámbrica 802.11: El componente fundamental de la arquitectura 802.11 es el **conjunto de servicio básico (BSS)**. Un BSS contiene:

* una o más estaciones inalámbricas.
* Una estación central, conocida como punto de acceso (AP, Access point).

Los puntos de acceso se interconectan a un dispositivo de interconexión (como un conmutador o un router), que a su vez lleva hacia Internet. En una red doméstica hay un punto de acceso y un router que conectaran el BSS con Internet.

Cada estación inalámbrica 802.11 tiene **una dirección MAC** en la tarjeta adaptadora de la estación. Cada punto de acceso tiene también una dirección MAC para su interfaz inalámbrica. Al igual que Ethernet, estas direcciones MAC son administradas por el IEEE y son globalmente únicas.

Las redes LAN inalambricas que incorporan puntos de acceso suelen denominarse **redes LAN inalambricas de infraestructura**, siendo la “infraestructura” los puntos de acceso junto con la infraestructura de Ethernet cableada que interconecta los puntos de acceso y un router. Las estaciones IEEE 802.11 también pueden agruparse para formar una **red ad hoc**: una red sin ningún control central y que no tiene conexiones con el “mundo exterior”, formada por dispositivos próximos entre sí y que no encuentran una red de infraestructura próxima ni un punto de acceso centralizado.

**WiFi: Canales y asociación**

* Cada estación inalámbrica necesita **asociarse** con un punto de acceso antes de poder enviar o recibir datos de la capa de red.
* Cuando un administrador de red instala un punto de acceso, asigna un **Identificador de conjunto de servicio (SSID*)***de una o dos palabras a ese punto de acceso.
* El administrador debe también asignar un número de canal a ese punto de acceso. 802.11 opera en el rango de frecuencias de 2,4 GHz a 2,485 GHz, se define 11 canales parcialmente solapados. Dados dos canales cualesquiera diremos que no se solapan si y solo si están separados por cuatro o más canales. En particular, el conjunto de canales I, 6 y 11 es el único conjunto de tres canales no solapados.
* **Jungla WiFi.**
  + Una jungla WiFi es cualquier ubicación física en la que una estación inalámbrica está recibiendo una señal suficientemente intensa desde dos o más puntos de acceso. Por ejemplo, cafeterías. Cada uno de estos puntos de acceso estará, probablemente, ubicado en una subred IP diferente y se le habrá asignado un canal de manera independiente.
  + Para poder obtener acceso a Internet, una estación inalámbrica necesita unirse a exactamente una de las subredes y, por tanto, necesitara asociarse con exactamente uno de los puntos de acceso. Solo el punto de acceso asociado enviara tramas de datos a la estación inalámbrica y nuestra estación inalámbrica enviara tramas de datos hacia internet solamente a través del punto de acceso asociado.
  + cómo se asocia una estación inalámbrica con un punto de acceso concreto? como sabe una estación que puntos de acceso hay disponibles en la jungla?

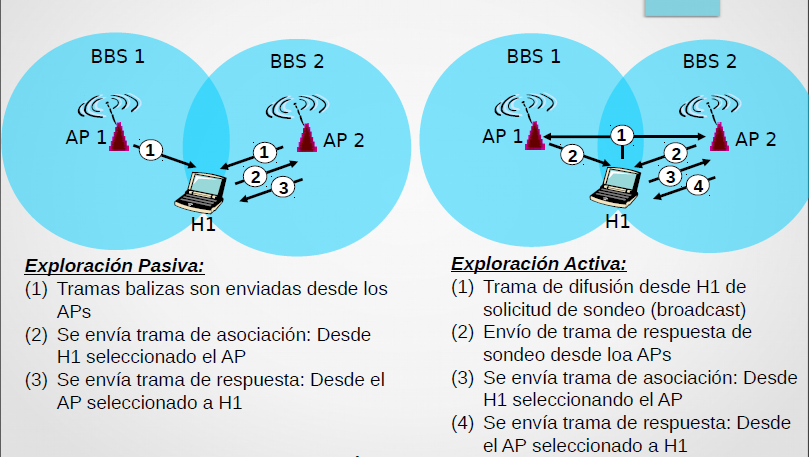
Como resolver los problemas de la jungla:

El estándar 802.11 un punto de acceso envíe de forma periódica **tramas baliza (beacon frames)**, cada una de las cuales incluye la dirección MAC y el identificador SSID del punto de acceso. La estación inalámbrica, que sabe que los puntos de acceso están enviando tramas baliza, explora los once canales buscando la tramas baliza de cualquier punto de acceso que pueda haber en las proximidades (algunos pueden estar transmitiendo a través del mismo canal). Habiendo determinado qué puntos de acceso hay disponibles a través de las tramas baliza, el host inalámbrico selecciona uno de los puntos de acceso para llevar a cabo la asociación.

El estándar 802.11 no especifica un algoritmo para seleccionar con cuál de los puntos de acceso disponibles asociarse; Normalmente, el host elige el punto de acceso cuya trama baliza se recibe con la máxima intensidad de señal. La intensidad de la señal no es lo único que influirá en el rendimiento, es posible que el punto de acceso seleccionado pueda estar sobrecargado por otra serie de hosts asociados, y se deja sin seleccionar un punto de acceso descargado, debido a la intensidad de la señal es ligeramente menor. Por esto, recientemente se han propuesto diversas formas de elección de los puntos de acceso.

El proceso de exploración de los canales y de escucha de las tramas baliza se conoce **con el nombre de exploración pasiva**.

Un host inalámbrico también puede **realizar una exploración activa**, difundiendo una trama de sondeo que será recibida por todos los puntos de acceso que caigan dentro del alcance del host inalámbrico. Los puntos de acceso responden a la trama de la solicitud de sondeo con una trama de respuesta de sondeo. EI host inalámbrico puede entonces elegir el punto de acceso con el que asociarse de entre todos aquellos que hayan respondido.

Después de seleccionar el AP con el que asociarse, el host inalámbrico envía una trama de solicitud de asociación a ese punto de acceso, el cual responde con una trama de respuesta de asociación. Una vez asociado con un punto de acceso, el host se unirá a la subred a la que pertenezca el punto de acceso. Normalmente el host enviara un mensaje de descubrimiento DHCP hacia la subred a través del punto de acceso para obtener una dirección IP de esa subred. Una vez obtenida la dirección, el resto del mundo vera entonces a dicho host simplemente como otro host cualquiera con una dirección IP perteneciente a dicha subred.

Para poder crear una asociación con un punto de acceso concreto, puede que la estación inalámbrica tenga que autenticarse ante el punto de acceso. Las redes LAN inalambricas 802.11 proporcionan diversas alternativas para la autenticación y el acceso:

* Acceso a una red inalámbrica basándose en la dirección MAC de la estación.
* nombres de usuario y contraseñas.
* En ambos casos, el punto de acceso se comunica normalmente con un servidor de autenticación, reenviando la información intercambiada entre la estación terminal inalámbrica y el servidor de autenticación utilizando un protocolo como RADIUS.

**El protocolo MAC 802.11**

Puede haber múltiples estaciones que pueden desear transmitir tramas de datos al mismo tiempo a través del mismo canal, es preciso utilizar un protocolo de acceso. Seleccionaron un protocolo de acceso aleatorio para las redes LAN inalambricas 802.11, se conoce como CSMA con evitación de colisiones CSMA/CA. Diferencias con CSMA/CD:

* No se detectan las colisiones, sino que se implementan mecanismos para evadirlas.
* Debido a las altas tasas de errores de bit en los canales inalámbricos se usa esquema de reconocimiento/retransmisión (ARQ).

El protocolo MAC 802.11 *no* implementa ningún mecanismo de detección de colisiones. Hay dos razones importantes para esto:

• La capacidad de detectar colisiones requiere la capacidad de enviar y de recibir al mismo tiempo. Como la intensidad de la señal recibida es menor a la transmitida por el adaptador 802.11, resulta muy costoso construir un hardware que pueda detectar una colisión.

• Todavía más importante es que, incluso si el adaptador pudiera transmitir y escuchar al mismo tiempo, el adaptador seguiría sin ser capaz de detectar todas las colisiones, debido a los problemas del terminal oculto y del desvanecimiento.

El esquema de **reconocimiento de la capa de enlace** en 802.11, cuando una estación en una LAN inalámbrica envía una trama, esta puede no llegar intacta al destino por diversas razones. Para resolver esta probabilidad no deseable de fallo, el protocolo MAC 802.11 utiliza reconocimientos en la capa de enlace.

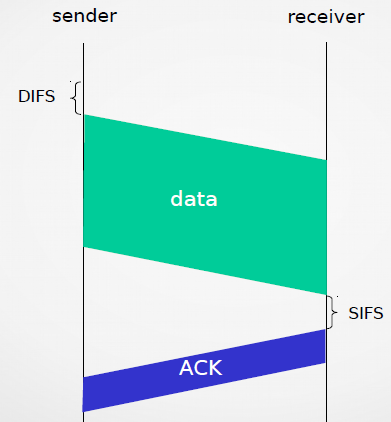
Cuando la estación de destino recibe una trama, pasa la prueba de comprobación de CRC, espera un corto periodo de tiempo conocido con el nombre de Espaciado corto entre tramas (SIFS) y luego devuelve una trama de reconocimiento (ACK). Si la estación transmisora no recibe una trama de reconocimiento dentro de un periodo de tiempo especificado, supone que se ha producido un error y retransmite la trama. Si no se recibe una trama de reconocimiento después de un número fijo de retransmisiones, la estación transmisora se da por vencida y descarta la trama.

En el protocolo **CSMA/CA 802.11** si una estación dispone de una trama para transmitir:

1. Si la estación detecta que el canal está inactivo, transmite la trama después de un corto periodo de tiempo, llamado Espacio distribuido entre tramas (DIFS).

2. En caso contrario, la estación selecciona un valor de espera (*backoff)* aleatorio y efectúa una cuenta mientras detecta que el canal está inactivo. Cuando detecta que el canal está ocupado, el valor del contador se congela.

3. Cuando el contador alcanza el valor 0, la estación transmite la trama completa y luego espera a recibir el ACK.

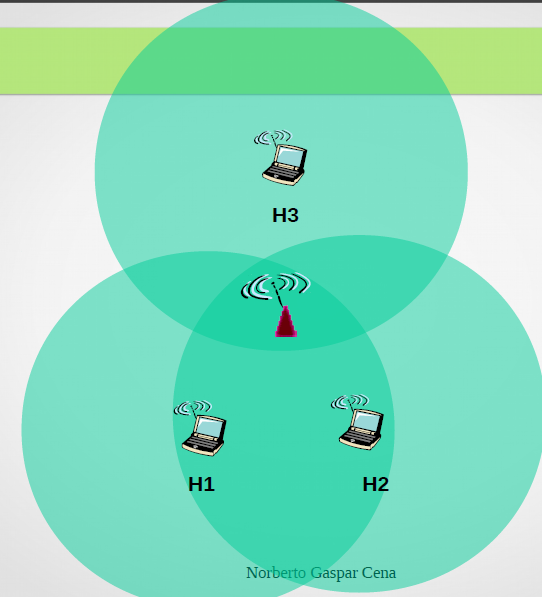
4. Si se recibe una trama de reconocimiento, la estación transmisora sabe que su trama ha sido recibida correctamente en la estación de destino. Si la estación tiene otra trama que enviar, comienza de nuevo el protocolo CSMA/CA en el paso 2. Si no se recibe una trama de reconocimiento, la estación transmisora vuelva a entrar en la fase de *backoff* del paso 2, seleccionando el valor aleatorio de un intervalo más largo.

¿Por qué CSMA/CD y CSMA/ CA adoptan enfoques tan distintos en este punto?

* CSMA/CD de Ethernet, una estación comienza a transmitir en cuanto detecta que el canal está inactivo.
* CSMA/CA la estación no transmite mientras efectúa la cuenta atrás, aun cuando detecte que no hay actividad en el canal.

Si hay dos estaciones, cada una de ellas con una trama para transmitir, pero ninguna de las estaciones transmite inmediatamente, porque ambas detectan que hay una tercera estación que ya está transmitiendo. En 802.11 la situación es distinta:

* 802.11 no detecta las colisiones y no aborta en las transmisiones.
* El objetivo de 802.11 es evitar las colisiones siempre que sea posible.
* En 802.11, si las dos estaciones detectan que el canal está ocupado, ambas entran en un estado de espera aleatoria.
* Si los valores son distintos, una vez que el canal pase a estar inactivo una de las dos estaciones empezara a transmitir antes que la otra y (si las dos estaciones no están ocultas) la “estación perdedora” escuchara la señal de la estación “ganadora”, congelara su cuenta atrás y se abstendrá de transmitir hasta que la estación ganadora haya completado su transmisión.
* Se pueden producir colisiones: las dos estaciones podrían estar ocultas a ojos una de otra o las dos estaciones podrían seleccionar valores de espera aleatorios lo suficientemente próximos como para que la transmisión procedente de la estación que comience primero pueda alcanzar a la segunda estación.

**Enfrentándose al problema de los terminales ocultos: RTS y CTS**

El protocolo MAC 802.11 ayuda a evitar las colisiones incluso en presencia de terminales ocultos. Ej, dos estaciones inalambricas y un punto de acceso. Ambas estaciones inalambricas caen dentro del alcance del AP y ambas están asociadas con el AP. Sin embargo, debido al desvanecimiento, cada una de las estaciones inalambricas esta oculta a la vista de la otra, aunque ninguna de las dos está oculta para el punto de acceso.

Para evitar este problema, el protocolo IEEE 802.11 permite a una estación utilizar una corta trama de control:

* Solicitud de transmisión (RTS, *Request to Send)*
* Preparado para enviar (CTS, *Clear to Send)* para *reservar* el acceso al canal.

Cuando un emisor quiere enviar una trama, enviar primero una trama RTS al punto de acceso, indicando el tiempo total requerido para transmitir la trama y la trama de reconocimiento (ACK). Cuando el punto de acceso recibe la trama RTS, responde difundiendo una trama CTS. Esta trama CTS sirve a dos propósitos distintos: proporciona al emisor un permiso explicito para enviar y también informa a las otras estaciones de que no deben transmitir durante ese periodo de tiempo reservado.

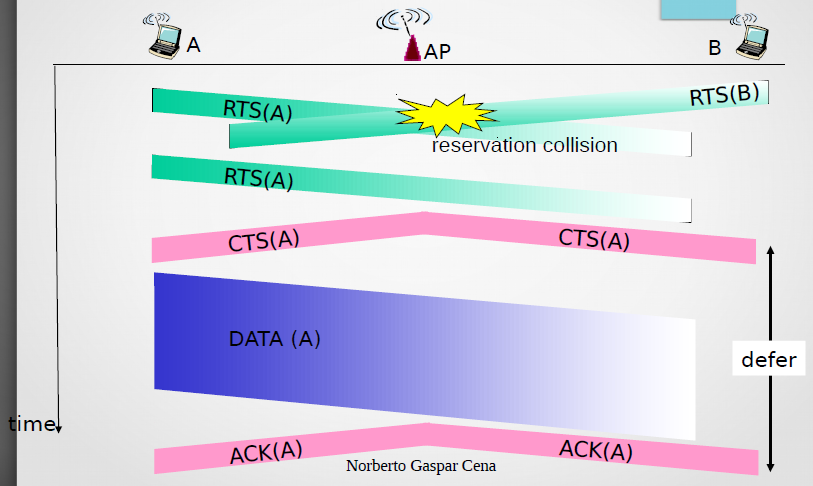
El uso de las tramas RTS y CTS puede mejorar el rendimiento de dos formas importantes:

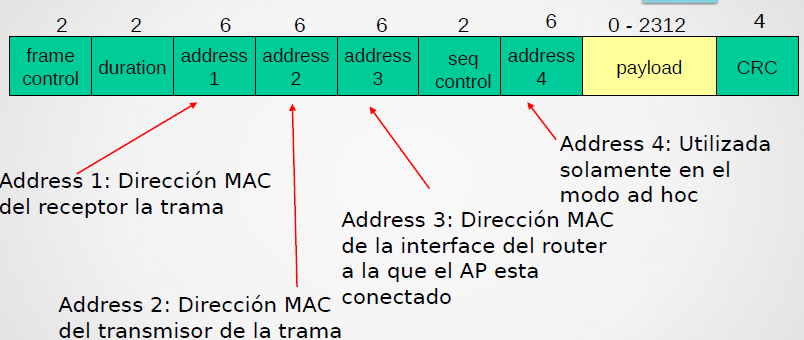
• El problema de las estaciones ocultas queda mitigado, ya que una trama DATA larga solo se transmitirá despues de haber reservado el canal.

• Puesto que las tramas RTS y CTS son cortas, una colisión solo durara mientras duren esas tramas cortas RTS o CTS.

• Una vez transmitidas las tramas RTS y CTS correctamente, las tramas DATA y ACK siguientes deberían poder transmitirse sin colisiones.

• introduce un retardo y consume recursos del canal.

Por esta razón, el intercambio RTS/CTS solamente se utiliza para reservar el canal para la transmisión de una trama DATA larga. Cada estación inalámbrica puede establecer un umbral RTS, de modo que la secuencia RTS/CTS se utilice únicamente cuando la trama que hay que transmitir sea mayor que el umbral. Si es menor la secuencia RTS/CTS se omite para todas las tramas DATA enviadas.

**La trama IEEE 802.11**

Contiene diversos campos que son específicos para su uso en enlaces inalámbricos, los campos son los siguientes:

* **Campos de carga útil y CRC:** la carga útil puede ser un datagrama IP o paquete, el CRC incluye un código de redundancia cíclica para que el receptor detecte errores en la trama recibida.
* **Campos de dirección:** tiene *cuatro* campos de dirección cada uno de los cuales puede contener una dirección MAC, tres de los campos de dirección son necesarios para propósitos de la comunicación por la red, específicamente para mover el datagrama de la capa de red de una estación inalámbrica hasta una interfaz de router a través de un punto de acceso. El cuarto campo de dirección se utiliza cuando los puntos de acceso se reenvían tramas entre sí en modo ad hoc. El estándar 802.11 define estos campos como sigue:
  + El campo Dirección 1 contiene la dirección MAC de la estación inalámbrica que tiene que recibir la trama.
  + Dirección 2 es la dirección MAC de la estación que transmite la trama.
  + El campo Dirección 3 contiene la dirección MAC de la interfaz de router a la que el AP está conectado.
* **Campos Número de secuencia, Duración y Control de trama:** números de secuencia permite al receptor distinguir entre una trama recién transmitida y la retransmisión de una trama anterior. El protocolo 802.11 permite a una estación transmisora reservar el canal durante un periodo de tiempo, que incluye el tiempo para transmitir su trama de datos y el tiempo para transmitir una trama de reconocimiento. Este valor de duración está incluido en el campo Duración de la trama. El campo de control se usa para distinguir las tramas de asociación, RTS, CTS, ACK y de datos, para definir los significados de los diferentes campos de dirección, si emplea cifrado o no.

**WiFi trama 802.11- trama 802.3 (IMAGEN EN FILMINA)**

Un ejemplo de comunicación por red hay dos puntos de acceso, cada uno de los cuales es responsable de una serie de estaciones inalambricas. Cada uno de los puntos de acceso tiene una conexión directa con un router, el cual a su vez se conecta a la red Internet global. Un punto de acceso es un dispositivo de la capa de enlace y que, por tanto, nunca “habla” IP ni comprende las direcciones IP.

El proceso de transferir un datagrama desde la interfaz del router R1 hasta la estación inalámbrica Hl. El router no es consciente de que existe un punto de acceso entre él y Hl; desde la perspectiva del router, Hl es simplemente un host en una de las subredes a la que el router está conectado.

• El router, que conoce la dirección IP de Hl, utiliza ARP para determinar la dirección MAC de Hl. Después de obtener la dirección MAC de Hl, la interfaz del router RI encapsula el datagrama dentro de una trama Ethernet. El campo de dirección de origen de esta trama contiene la dirección MAC de R1 y el campo de la dirección de destino contiene la dirección MAC de Hl.

• Cuando la trama Ethernet llega al punto de acceso, este convierte la trama Ethernet 802.3 en una trama 802.11 antes de transmitirla por el canal inalámbrico. El punto de acceso rellena los campos Dirección 1 y Dirección 2 con la dirección MAC de H1 y su propia dirección MAC. Como Dirección 3, el punto de acceso inserta la dirección MAC de Rl.

Que sucede cuando la estación inalámbrica H1 responde transfiriendo un datagrama desde H1 a Rl.

• H1 crea una trama 802.11, rellenando los campos Dirección 1 y Dirección 2 con la dirección MAC del punto de acceso y la de Hl. Como Dirección 3, Hl inserta la dirección MAC de Rl.

• Cuando el punto de acceso recibe la trama 802.11, la convierte en una trama Ethernet. El campo de dirección de origen de esta trama será la dirección MAC de Hl, mientras que el campo de dirección de destino será la dirección MAC de Rl. Por tanto, el campo Dirección 3 permite al punto de acceso determinar la dirección MAC de destino apropiado a la hora de construir la trama Ethernet.

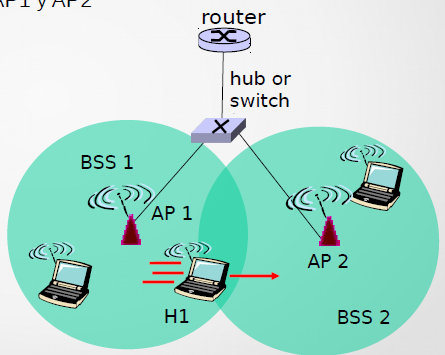
**Movilidad dentro de la misma subred IP**

Para incrementar el rango de una red LAN inalámbrica se implantan varios BSS dentro de la misma subred IP. Esto plantea el problema de la movilidad entre los distintos BSS: ¿cómo pueden moverse las estaciones de un BSS a otro sin perder las conexiones TCP activas?

* La movilidad puede gestionarse de forma sencilla cuando los BSS forman parte de una misma subred.
* Cuando las estaciones se desplazan entre subredes contiguas, hacen falta protocolos más complejos.

Un ejemplo de movilidad entre diversos BSS dentro de la misma subred. Con 2 BSS interconectados con un host, H1, que se desplaza desde BSS1 a BSS2. Si el dispositivo de interconexión que conecta a los dos BSS *no* es un router, todas las estaciones de los dos BSS, incluyendo los SP, pertenecen a la misma subred IP. Por tanto, cuando H1 se mueve desde BSS1 a BSS2 puede conservar su dirección IP y todas sus conexiones TCP activas. Si el dispositivo de interconexión fuera un router, entonces H1 tendría que obtener una nueva dirección IP en la subred hacia la cual se está moviendo. Este cambio de dirección interrumpiría cualquier conexión TCP activa en H1. Esto se ve desde dos puntos desde el host y AP, y desde el switch.

Lo que sucede específicamente cuando H1 se mueve de BSS1 a BSS2, es que, a medida que H1 se aleja de AP1, H1 detecta que la señal de AP1 comienza a debilitarse y empieza entonces a explorar en busca de una señal de mayor intensidad. H1 recibe tramas baliza de AP2 (tendrá el mismo identificador SSID que AP1). H1 se desasocia entonces de AP1 y se asocia con AP2, al mismo tiempo que mantiene su dirección IP y sus conexiones TCP activas.

Desde el punto de vista del conmutador, el host se ha desplazado de un punto de acceso a otro, los conmutadores disponen de “auto-aprendizaje”, que les permite construir automáticamente sus tablas de reenvió. Este auto-aprendizaje gestiona eficientemente desplazamientos ocasionales; sin embargo, los conmutadores no fueron diseñados para dar soporte a usuarios extremadamente móviles que deseen mantener las conexiones TCP mientras se desplazan entre varios BSS.

Antes del desplazamiento el conmutador tiene una entrada en su tabla de reenvió que relaciona la dirección MAC de H1 con la interfaz de salida del conmutador que llega a H1. Si H1 se encuentra inicialmente en BSS1, un datagrama para H1 tendrá que ser dirigido hacia H1 a través del punto de acceso AP1. Sin embargo, una vez que H1 se asocia con BSS2 sus tramas deben ser dirigidas hacia AP2. Una solución, es que AP2 envié al conmutador una trama Ethernet de difusión con la dirección de origen de H1 luego de la nueva asociación. Cuando el conmutador reciba la trama actualizara su tabla de reenvió, permitiendo alcanzar a H1 a través de AP2.