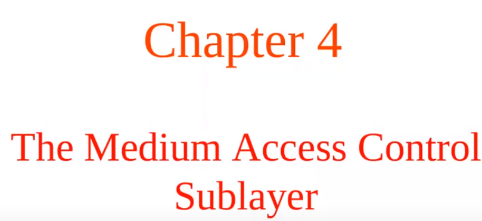
*-Clase del 24-08-2021. “Sub capa MAC”*

Como vimos antes la capa de enlace, tenía que ver con: como no sabíamos el largo de los mensajes los partía en tramas para poder procesarlos, hacer control de flujo y gestión de errores. Para entramarlos tenía que poner una bandera, etc.

Ahora vamos a ver algunas funcionalidades que podría o no, tener una capa de enlace. No siempre las vamos a encontrar.

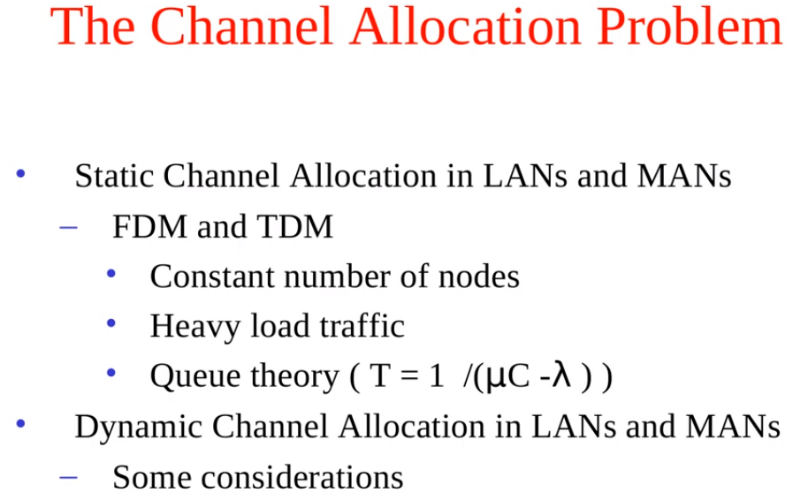
**¿Por qué una sub capa?**

Cuando tengo redes Punto a Punto estos temas no interesan, porque básicamente tengo un canal que cuando transmito hay solo 2 máquinas o extremos.

La problemática que vamos a ver, se plantea cuando tengo redes de difusión o Broadcast. O dicho de otra manera cuando tengo un canal compartido, ya sea un cable, una frec inalámbrica, etc.

El problema se presenta porque no tengo 2 nodos que van a ocupar el canal, sino varios nodos y si tengo un solo canal van a tener que competir o decidir de alguna manera como hago para asignar el canal para que todos puedan interactuar sin conflictos.

Define como acceder al canal.

Una forma fácil es hacer una asignación estática. TDM o FDM.

Esto tiene varias limitaciones. Generalmente no se usa.

-Nº fijo de nodos.

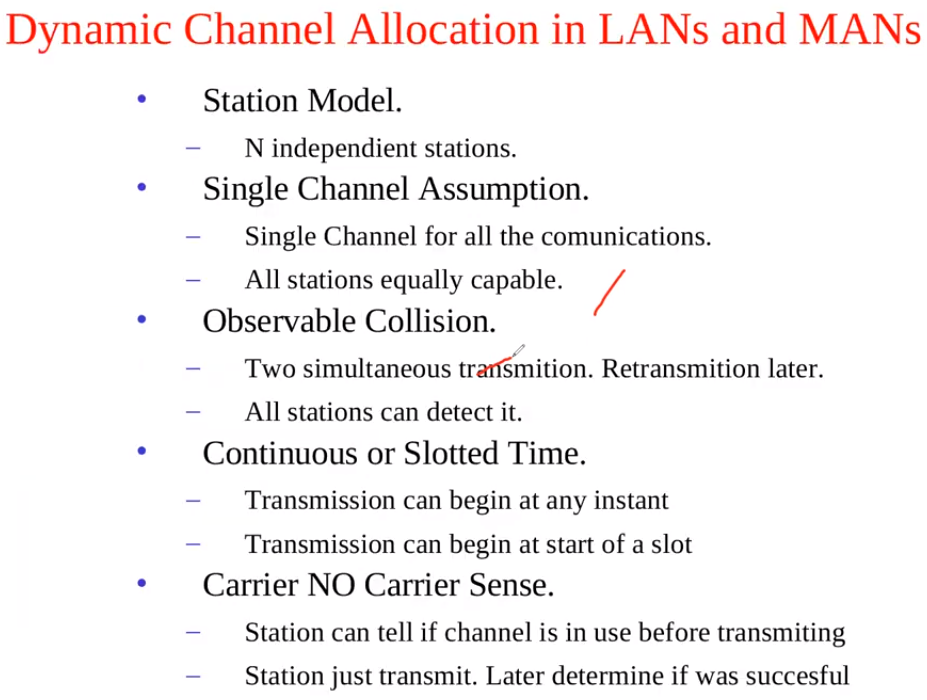
-Los nodos deberían transmitir todo el tiempo para aprovecharlo mejor, sino es ineficiente. Pero, de hecho, la mala noticia es que, en las redes el tráfico normalmente es por ráfagas, no están transmitiendo todo el tiempo. No tienen un comportamiento constante por decirlo de alguna manera, sino tiempos largos sin transmitir, y momentos cortos donde transmiten un montón.

-Teoría de colas: Se refiere al delay que tenemos en un canal. Está demostrado que, si se disminuye el BW del canal y tengo varios canales, aumenta exponencialmente el delay de todo el sistema.

Contras de la asignación estática:

Trafico por ráfagas, numero de nodos fijo, delay que crece exponencialmente si asigno canales con TDM o FDM

Por lo cual la mayoría de las asignaciones de los canales en redes se realiza de manera dinámica.

Antes de ver los mecanismos de Protocolos MAC, el autor hace algunas consideraciones respecto a los nodos y la manera de comunicarse.

1-menciona que todos los nodos son independientes. Ósea cada uno transmite cunado tenga datos y no depende de otro.

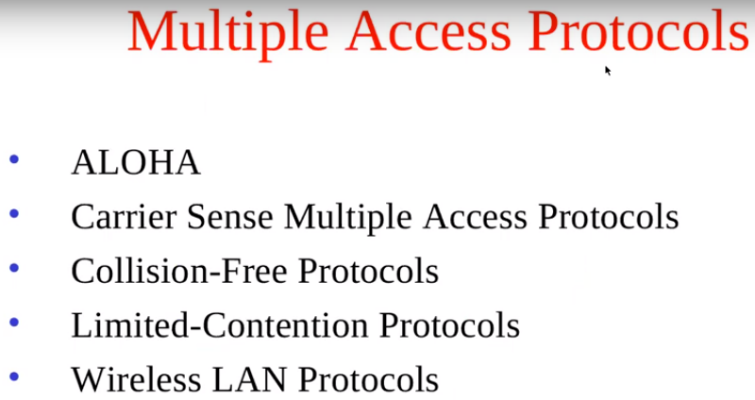
2-Partimos de que hay un solo canal compartido por todos los nodos y que todos tienen la misma capacidad de transmisión.

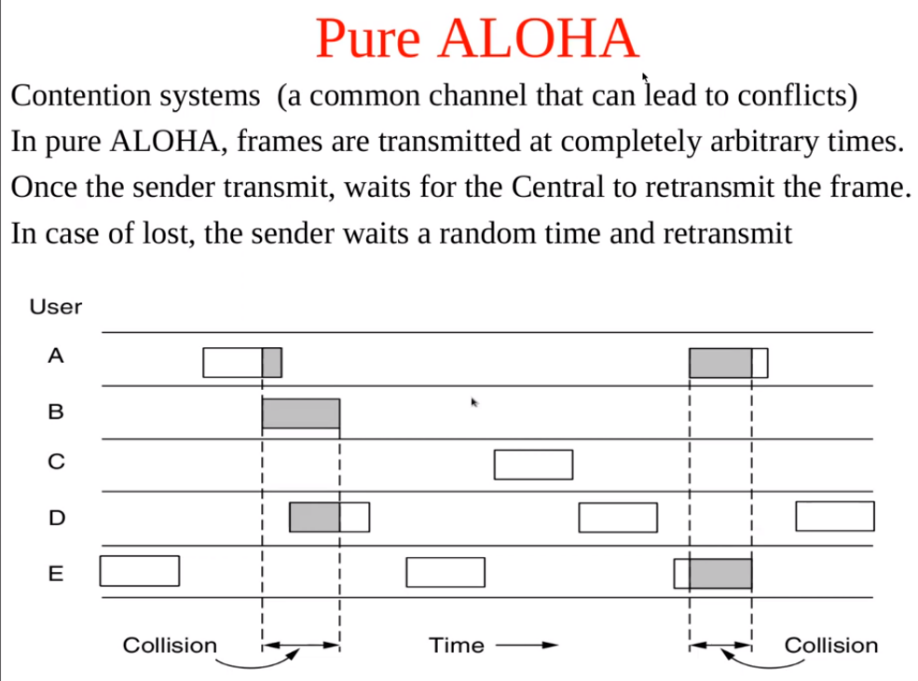
3-Se pueden observar las colisiones. Si 2 transmiten al mismo tiempo. básicamente si son niveles de tención u ondas electromagnéticas se superponen, y lo que termina pasando es que la información se destruye. Por lo que de alguna manera hay que verificar si hubo colisión y si hubo, hay que retransmitir los datos porque se perdieron.

4-Podría ser Tiempo continuo o ranurado: Lo cual implica un reloj que marca el inicio de las ranuras. Si es continuo los datos se pueden mandar cuando están disponibles, si es ranurado los datos se pueden mandar al iniciar la ranura.

5-Censado de portadora o no. Si censan portadora los nodos podrían saber si hay actividad en el canal. Podría pasar que no pueda censar portadora según el tipo de canal.

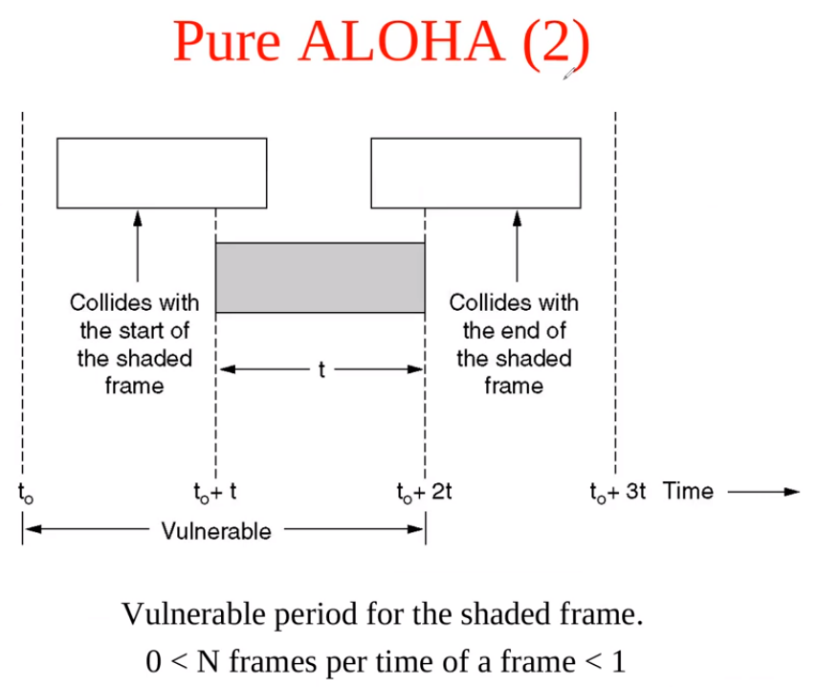
**PROTOCOLOS:**

1. ALOHA (Inalámbrico) - 2 alternativas
2. CSMA (Alámbrico – Cableado) – 3 alternativas
3. Libre de colisión – 3 alternativas
4. Contención Limitada (Concepto y un ejemplo)
5. Inalámbricos (Concepto y un ejemplo)

**1.1) – ALOHA PURO:** Se origino en Hawai, en los 70s, no había posibilidad de mandar cable submarino. El objetivo era interconectar con “Datos” varias islas del archipiélago.

La aproximación fue transmitir los datos con equipos de radio, todos a la misma frecuencia. Había un nodo central que cuando recibe un dato lo retransmite, la condición es que todos los nodos tengan visibilidad o capacidad de escuchar al nodo central, entre ellos no era necesaria, por eso no censa portadora. Este mecanismo tenía transmisión continua.

El tema era si otro transmitía en el mismo momento, había colisión. ¿pero cómo se enteraban lo nodos? Porque escuchaba si la central retransmitió lo que el mando. Si después de un tiempo aleatorio no recibió o escucho su eco, vuelve a mandarlo.

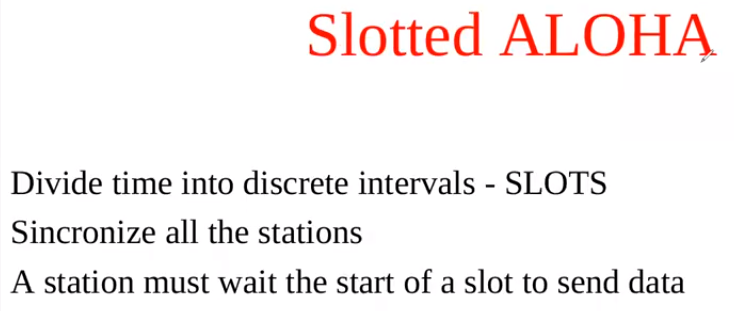
Puede haber colisión en cualquier instante de la transmisión, al principio, al medio, al fin de la transmisión. Por más que solo arruiné 2 o 3 bits de la trama, tanto el que estaba transmitiendo y el que interrumpió, ambos van a tener que retransmitir todo el mensaje nuevamente luego de un tiempo aleatorio.

La eficiencia de uso del canal no es muy buena. Pero funciona, es sencillo.

El tiempo de espera para retransmisión es aleatorio para que haya menos probabilidad de volver a colisionar.

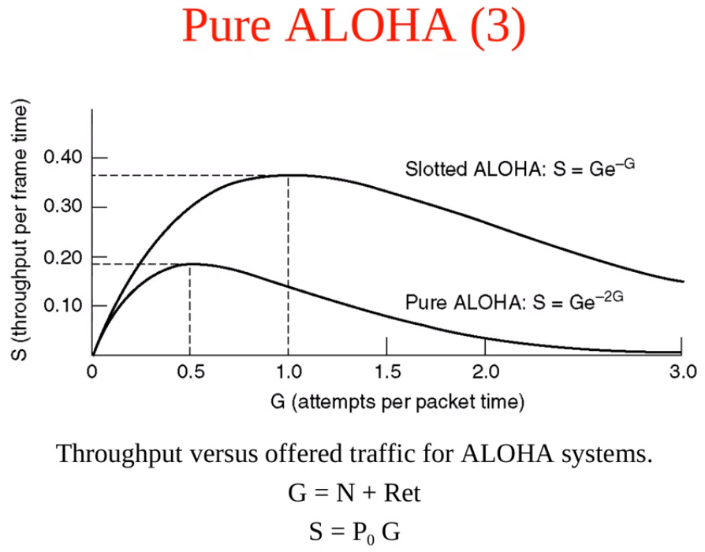
**1.2)- ALOHA RANURADO:**  básicamente pone ranuras de tiempo, y ahora los nodos en vez de transmitir cuando tengan los datos, tienen que esperar que inicie una ranura de tiempo y recién ahí transmitir.

¿Cómo sincronizo los nodos? ¿Mejora o no las cosas?

Al ser ranura debería marcar un inicio de ranura o intervalo. La central envía periódicamente una trama muy chiquita que se llama Bit COM que se traduce como “Faro”, va avisando cuando arranca la ranura.

802.11 WIFI se basó en esta característica. Entonces todos los nodos que ven a la central, cuando tienen datos no lo mandan hasta que reciben el BitCOM.

Puede pasar que haya colisión.

Mejora porque la trama antes era vulnerable durante todo el tiempo de transmisión. Ahora como esperan la ranura de tiempo, no pueden empezar a la mitad ni al final. Entonces la trama solo es vulnerable al principio, después no va a ocurrir la colisión.

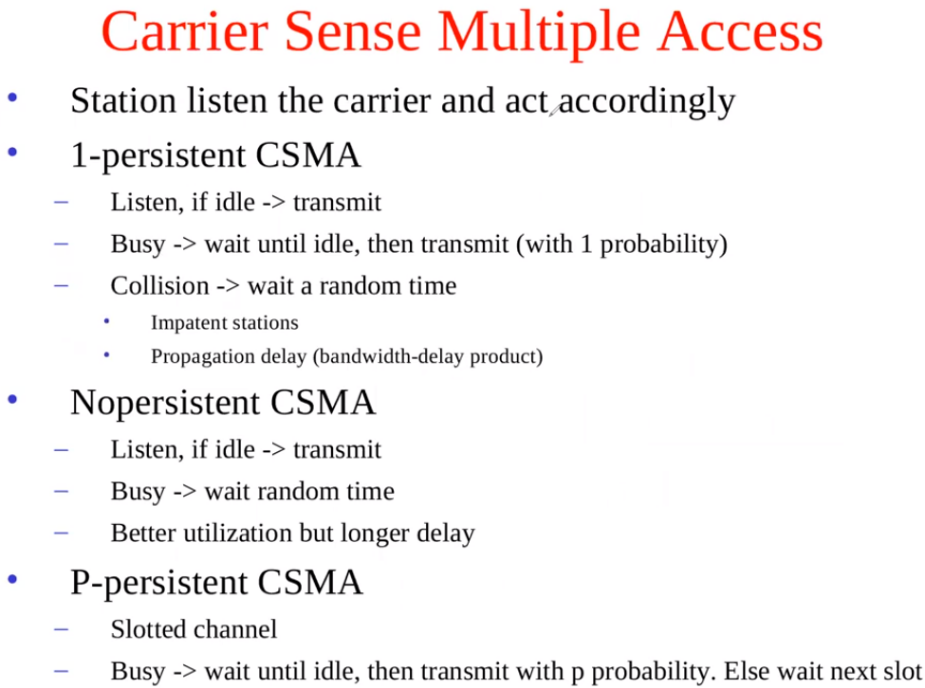
Agrega Delay, pero hay menos probabilidad de colisiones.

El libro menciona una distribución probabilística de Puason de datos a transmitir.

Eje Vertical: La tasa de salida. (Mala, varios nodos pelean por el canal.)

Eje Horizontal: Cantidad de tramas que tiene que trasmitir más las que tiene que retransmitir.

A medida que tengo más tramas para transmitir baja la eficiencia.

**2- CSMA Acceso Múltiple y Censado de Portadora. (Cableados) Hay varios dentro de esta familia.**

Antes de transmitir me fijo hay alguien transmitiendo. Si el canal está ocupado.

No se puede aplicar de manera inalámbrica. Porque no todos los nodos se perciben entre ellos.

**2.1) Persistente-1 CSMA**

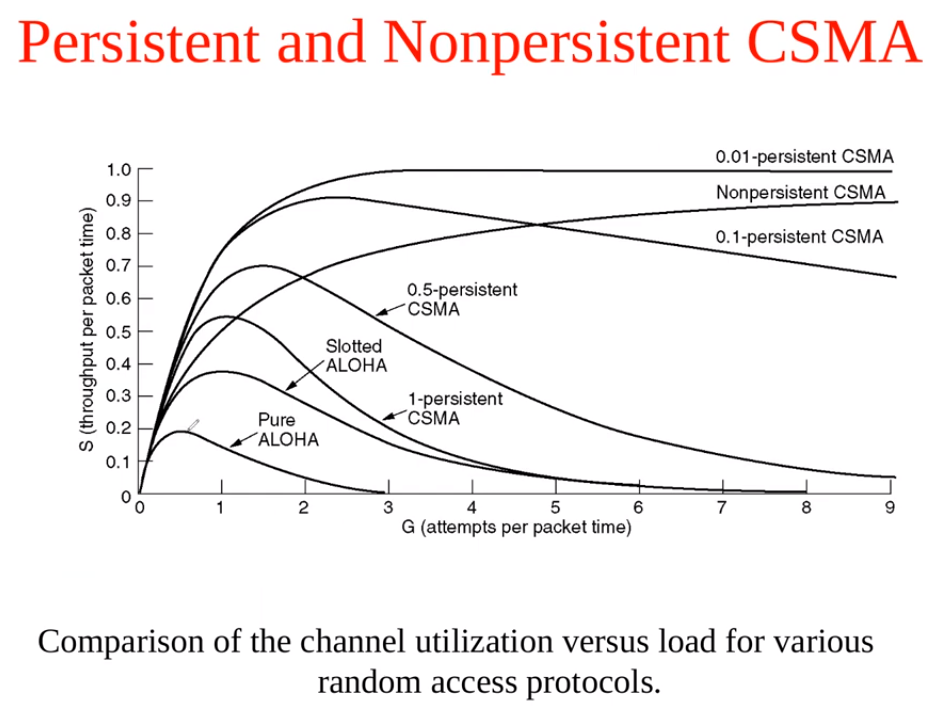
Censa si hay actividad en el cabe, antes de mandar los datos. Si no hay actividad transmite, si hay actividad se queda censando hasta que dejen de transmitir, cuando no escucha nada ahí no más transmite sus datos.

Parece bueno, tengo poco delay y ocupo mucho el canal, pero podría pasar que 2 nodos estaban esperando y colisionan. Son Nodos impacientes.

Los 2 arrancan a transmitir porque debido al delay de propagación piensan que el canal esta libre.

**2.2) NO Persistente CSMA**

Parecido al anterior, pero si el canal está ocupado, espero un tiempo aleatorio y me vuelvo a fijar. Se reducen las colisiones, pero se aumenta el Delay.



**2.3) Persistente – P …. CSMA**

Este se aplica a canales ranurados, donde tenemos algo que nos marca el inicio de trama o ranura. Si el nodo tiene dato, espera el inicio de trama, y transmiten o no en esa ranura de acuerdo a una probabilidad p, si deciden no transmitir esperan la siguiente trama y así otra vez transmiten o no con probabilidad p, Y así hasta que en algún momento transmiten. Usualmente p = 0,5, donde si tiene dato, tiene 50% de probabilidades de transmitir en cada inicio de trama.

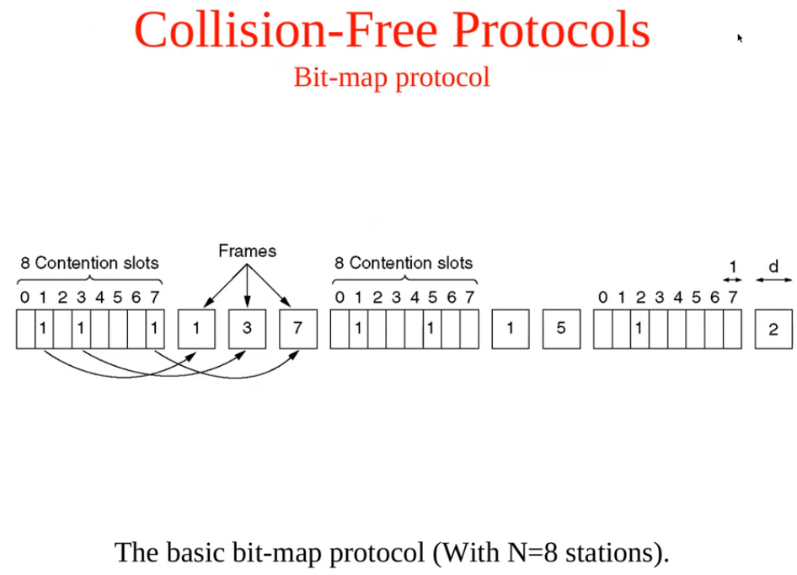
**Gráfico comparativo.**

Mejora la tasa de salida = Throughput

Horizontal: 1 es la cantidad de paquetes a transmitir por unidad de tiempo. A medida que aumenta la cantidad que tenemos para transmitir, disminuye el Throughput porque se incrementan las colisiones.

Observar cómo sería el Delay

**3) Protocolos Libre de colisión.**

En los casos anteriores podían ocurrir colisiones, en este grupo de mecanismos o protocolos no van a generarse colisiones nunca.

**3.1) Mapa de bits:**

Supongamos que tenemos 8 estaciones que quieren usar “el mismo medio, cableado o inalámbrico”, si es inalámbrico todos deben estar al alcance de todos, no como en ALOHA.

El tema es que, hay un inicio de trama, o de ranura… acá se llama Slot de contención, donde cada nodo si tiene datos a transmitir pone en alto a la ranura que le corresponde a él de esta trama.

Entonces después de esta trama de contención, lo que pasa es que hay una ranura de tiempo para cada nodo que, por decirlo de alguna manera, notifico que tenía datos para transmitir. Cuando se acaban todas las ranuras de datos a transmitir, vuelve a ver una ranura de contención.

Parecido a TDM, pero no se le asigna ranuras fijas de tiempo a los nodos, si a quien necesite.

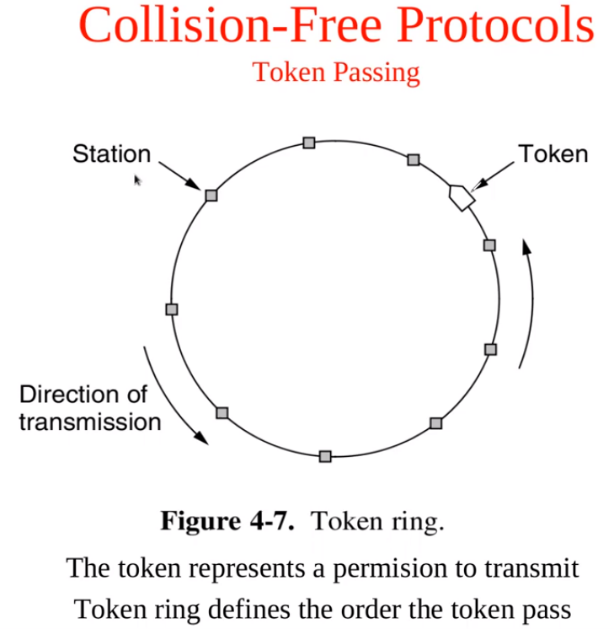
Todos los nodos deberían estar sincronizados en el tiempo, el protocolo no especifica como. Los slot de contención son pequeños en comparación con las ranuras de transmisión de datos.

Los nodos pueden informar de alguna manera en el slot de contención la duración de la trama de datos, si estas fueran de tamaño variable y no fijo.

¿Qué pasa si tengo muchos nodos? ¿o poco tráfico?

El slot de contención se hace muy grande y desaprovecho el uso del canal. Lo utilizo más para slot de control que para datos.

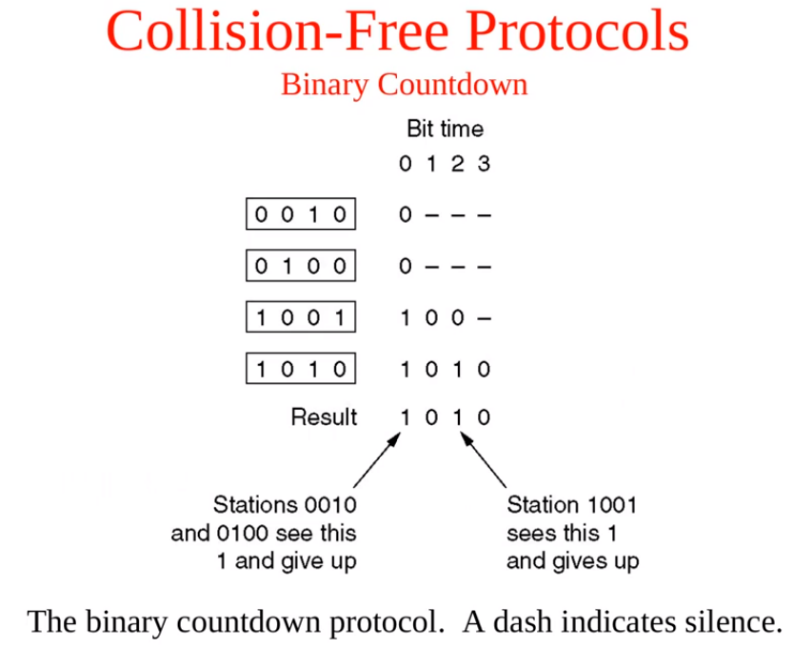
Ósea NO ESCALA, no sirve para muchos nodos.



**3.2) Token Passing – Pasar la ficha o el token:** Token Ring es una red que usaba este mecanismo. Esto funciona básicamente así, el token es un patrón o secuencia de bits, una trama pre establecida chiquita con un valor determinado. Los nodos están interconectados y se pasan el token uno a otro dentro de una red cerrada.

El nodo no puede enviar datos hasta que le llega el token. Cuando llega, lo saca, envía todos sus datos, cuando los mismos son reenviados por todos los nodos, dan la vuelta a toda la red y vuelven al origen, el Emisor los saca por decirlo de alguna manera y re inyecta el token.

No hay colisiones, pero si hay muchos nodos, demora mucho en recorrerlos todos. NO Escala.

Con mucha carga de datos puede funcionar, pero si son pocos se desperdicia el canal.

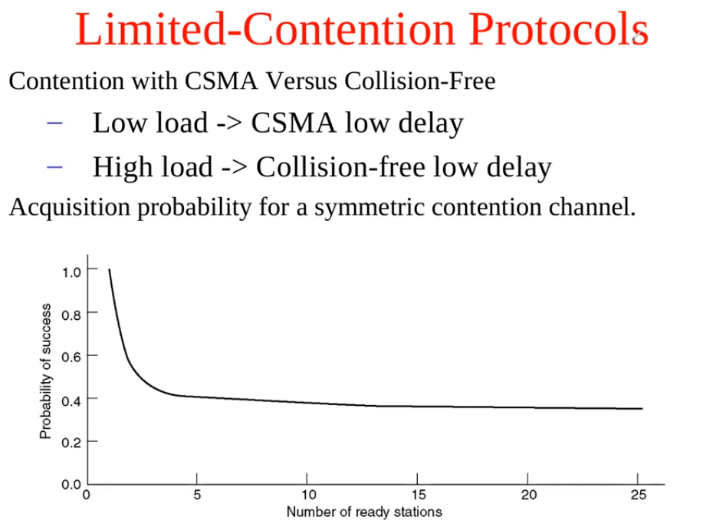
**3.3) Conteo descendente Binario:** A cada nodo se le asigna una dirección. En el ejemplo tenemos 16 nodos, de los cuales 4 quieren escribir en un momento determinado.

Esto es ranurado, entonces al inicio de cada ranura, el nodo que quiere escribir coloca su dirección. Van completando las ranuras de bit y comparando. El Canal realiza una “OR” entre ellos.

Verifica las columnas, si hay 0 y 1, continua en carrera los 1, si son iguales continúan la comparación en la siguiente columna. Y se llega al resultado del número de nodo que va a transmitir en ese momento.

Parece sencillo, tiene la ventaja que establece prioridades entre los nodos, según la cantidad de 1 o la dirección de más peso.

No es equitativo. Ventaja o desventaja según la aplicación.

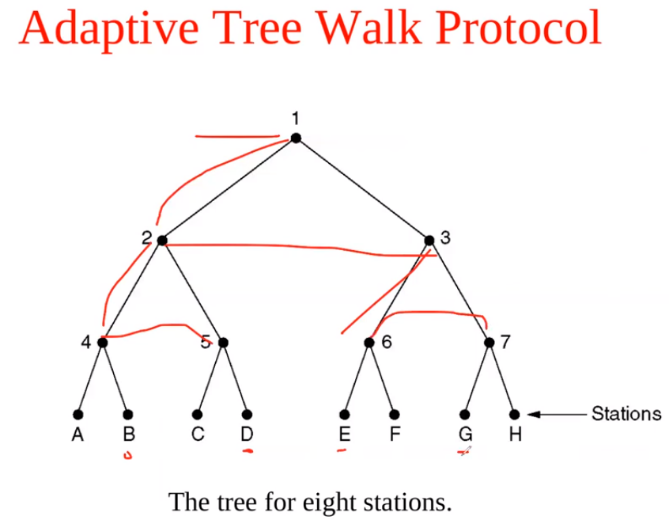
Si comparamos los protocolos libres de colisión con los CSMA, Carrier sense multiple accese. Resulta que los CSMA son mejores cuando hay poca carga, tienen menos delay y más tasa de transferencia.

Cuando hay mucha carga, los CSMA tienen muchas colisiones entonces los “libre de colisiones” funcionan mejor.

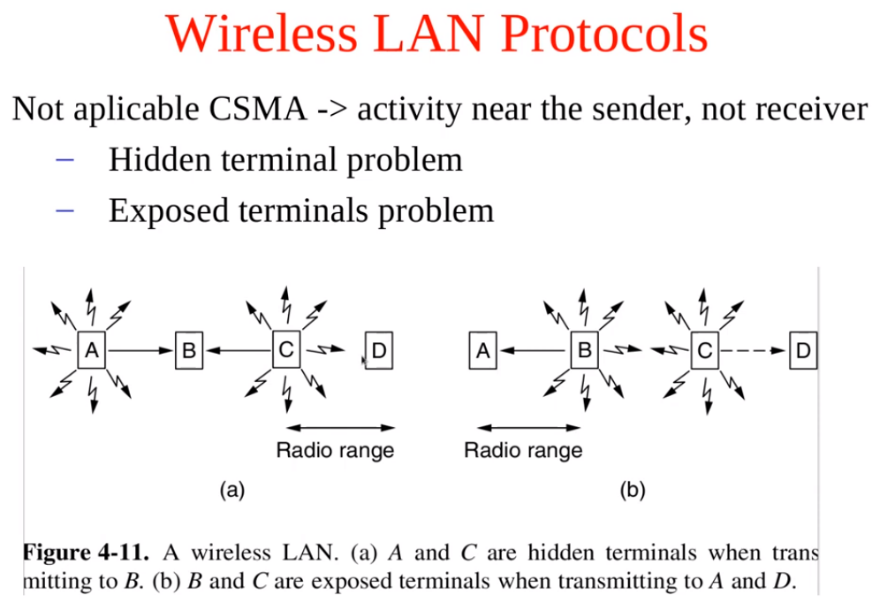
Entonces se plantea usar un protocolo adaptativo, libre de colisión con mucha carga y comportamiento CSMA con poca carga.

**4) Protocolo Árbol de Camino Adaptativo. (CONTENCIÓN LIMITADA)**

Básicamente esto funciona, si tengo 8 nodos, tengo un árbol invertido.

****Entonces en un momento determinado, se fija si hay nodos listos para transmitir. Si hay uno transmite directamente, si hay más de uno, hay competencia por usar el canal. Entonces lo que hace es achicar el dominio de colisión por decirlo de alguna manera.

Lo que hace es verificar los niveles de las ramas, y que compitan los que están solo debajo del 2, como hay mas de 1 nodo que quiere competir, otra vez chequea un nivel de rama mas abajo, 4 por ejemplo, y como hay uno solo que quiere transmitir, ese envía sus datos, luego sigue verificando los demás niveles de ramas.

Ósea, si hay mucho para transmitir, primero transmite el nodo A, luego el B, después CDEFGH, se comporta como los libre de colisión. Mientras que cuando hay pocos nodos listos, deja que transmitan al verificar algunos de los niveles superiores de las ramas, no necesita bajar.

El profe no lo ha visto aplicado nunca.

**5) Protocolos inalámbricos:** Vemos los principios básicos, no lo vemos con detalle, porque si no deberíamos ver el protocolo 802.11 WIFI que es muy usado y conocido. Solo vamos a ver un protocolo llamado MACA que es sencillo.

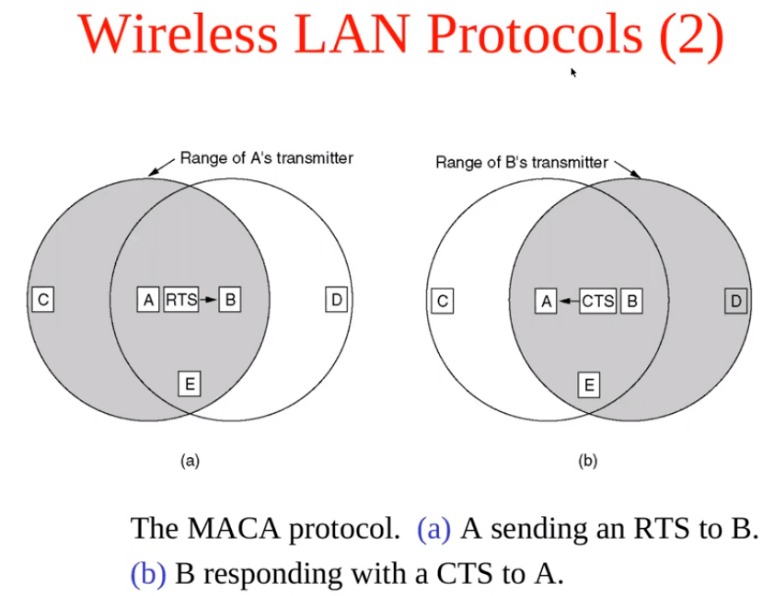
Con respecto las Redes inalámbricas, como mencionamos, no podemos aplicar CSMA, censado de portadora, porque los nodos no se ven siempre entre ellos, pueden estar fuera de mi alcance.

El problema acá es cuando censo, censo la actividad en el Emisor, no en el receptor.

**-Terminal oculto:** B recibe de ambos, porque A y C, censan y piensan que nadie transmite, porque entre ellos no hay alcance. En B hay colisiones, pero ni A ni C se enteran.

**-Terminal Expuesta:**

En transmisión inalámbrica no se censa portadora, por estos 2 problemas.

¿Cómo lo solucionan? 802.11 usa algo parecido.

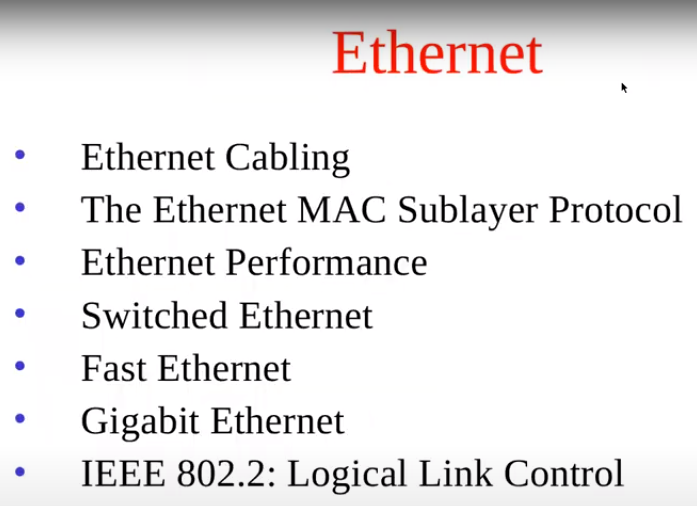
**MACA:** Si A tiene que mandar un mensaje a B, antes de mandar el mensaje le manda una trama muy chiquita con un patrón especial que indica que quiere enviar información a B. RTS: Request to send.

Entonces que pasa, lo recibe B y todos los que estén dentro del alcance de A, y saben que A va a mandar datos, entonces ellos se quedan callados. Y B responde con un CTS, clear to send, un “estoy listo para recibir los datos”.

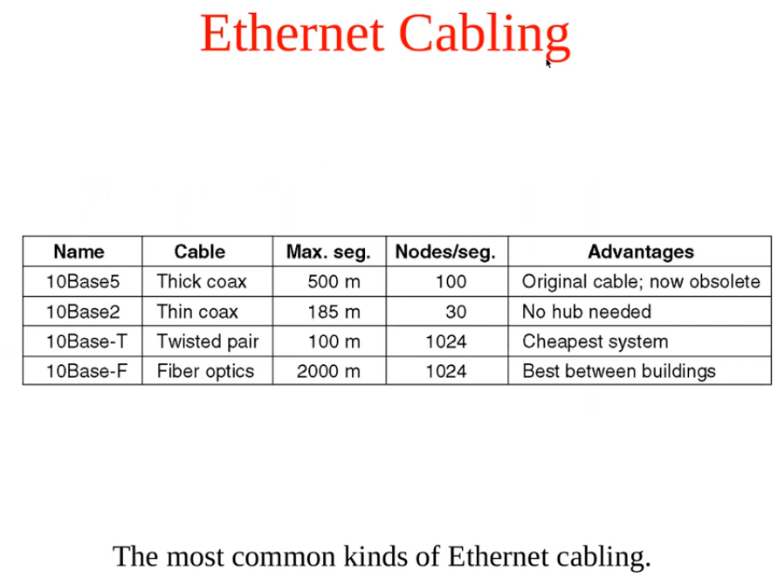
Lo recibe D en el ejemplo, y sabe que no tiene que transmitir para no interrumpir.

Es como un aviso para todos que se callen y no molesten.

Acá terminan los protocolos MAC. Ahora viene un ejemplo.

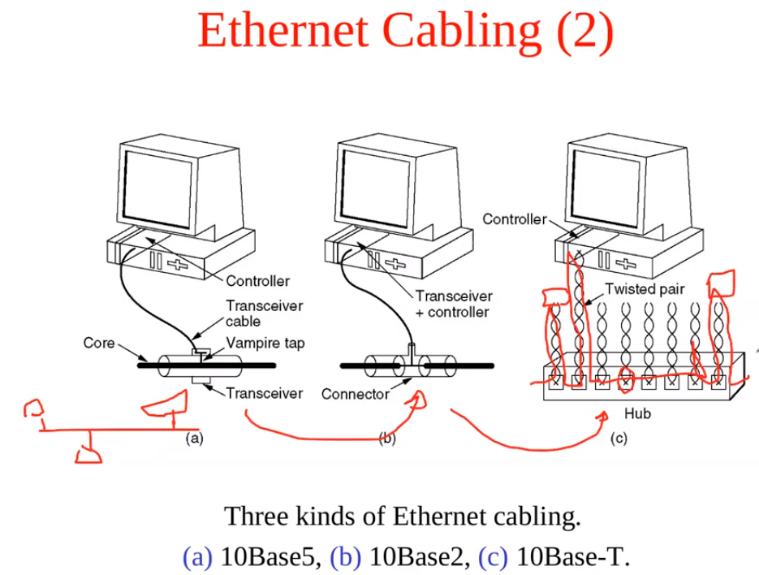
**ETHERNET:** Caso de uso de las Sub capa MAC

-Como es la trama y un par de cosas más.

No importa mucho, habla un poco de las normas.

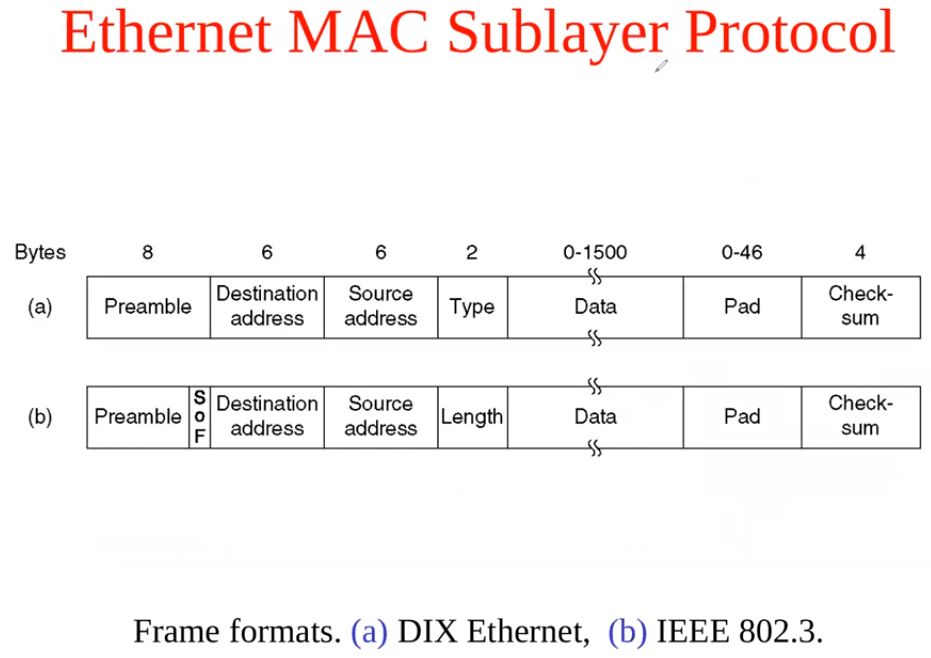
Originalmente cable coaxial gruesito, medio duro, complicada la instalación. Todos los nodos se conectaban mediante un conector tipo vampiro que tocaba el vivo

Como era medio complicada la instalación se pasó a un cable coaxial más fino y flexible, y con conectores en vez del vampiro. Era más fácil de instalar RG-58 era el cable creo.

Pero el tema era que los conectores eran bastante débiles en cuanto a su conexión, entonces si se abría el circuito ya no tenía una guía de onda y ya no tenía ninguna maquina conectada a la red. Había que tener mucho cuidado con los conectores.

La 3er versión ya tenía un concentrador llamado HUB, y cada maquina se conectaba en una topología de estrella con el concentrador. Usaban Par trenzado.

En este caso no se visualiza claramente el medio compartido. Pero internamente el HUB lo puentea las bocas que no están conectadas. Físicamente es una estrella, pero lógicamente sigue siendo un bus. Cada maquina estaba conectada por 2 pares trenzados.

**Formato de TRAMA Ethernet:**

Cada vez que alguien manda información, en un cable coaxial o UTP, lo que manda es una trama de este tipo.

Preámbulo: Combinación de 0 y 1, 8 Bytes, es una Honda cuadrada que sirve de portadora para sincronizar las maquinas.

Dirección destino y origen. 6 Bytes cada una.

Tipo:2 Bytes. A que capa de Red le mando los datos. Ej: IPv4 o IPv6.

Datos: Es un capo de tamaño variable de hasta 1500 Bytes.

PAD: Relleno, significa que entre datos y el PAD debería haber mínimo 46 Bytes. Ósea de 46 a 1500 es la suma.

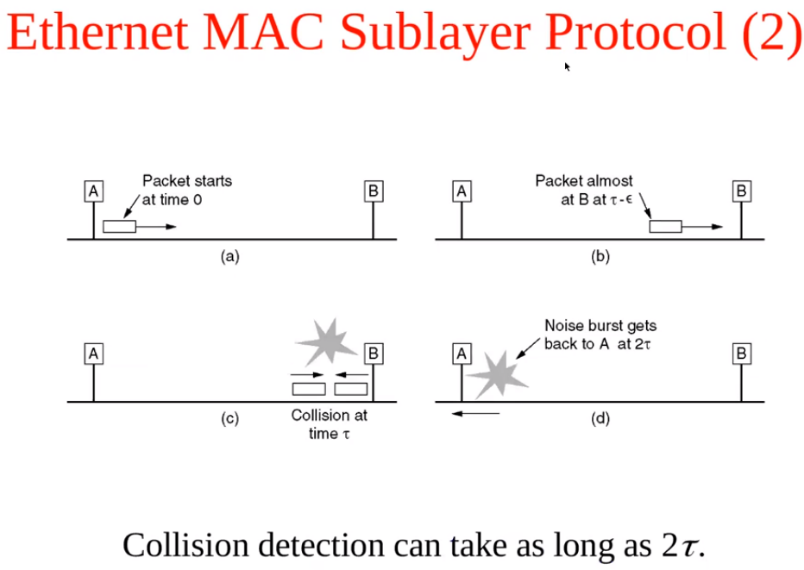
checksum: 4 Bytes.

¿Para qué mando las direcciones?

Si el medio es compartido y mando un mensaje, lo reciben todas.

Destino: Para que las maquinas que estén conectadas puedan descarar el mensaje sin procesarlo si no era para ellas. La placa de red se ahorra trabajo. Por eso está el destino al inicio de la trama.

Origen: Para que el receptor sepa a quien responder.



¿Para que el relleno/PAD?

Trama de valor mínimo. Para poder detectar colisiones debería estar todavía transmitiendo, porque la señal tiene que realizar el camino de ida y de vuelta para que el emisor se entere.

La colisión es un procedimiento “analógico” donde se compara el nivel de señal que viene del canal con los datos que yo estoy transmitiendo. Entonces no puedo saber si mi trama esta colisionando si yo ya terminé de transmitir.

Por norma la distancia máxima de la red está determinada.

B censa, y no hay portadora y transmite, la señal de A no había llegado.

De Alguna forma me tengo que asegurar que A está transmitiendo luego de que pasa el tiempo 2tau, para poder comparar la transmisión con lo que censa del canal.

Entonces con una longitud determinada y una velocidad de propagación determinada, se puede calcular el tamaño mínimo de trama para que en el peor de los casos cuando allá una colisión en la otra punta la pueda detectar.

Al tiempo la IEEE quiso normalizar y creo el protocolo 802.3 para redes de datos cableadas de área local.

Tiene 7 Bytes de preámbulo + 1 Byte más. (también con 0 y 1 le parece al profe) Aclarar con lo que dice Ana en la practica

Cambio tipo por largo. ¿Dónde iba la longitud en Ethernet? ¿Dónde está el tipo en 802.3?

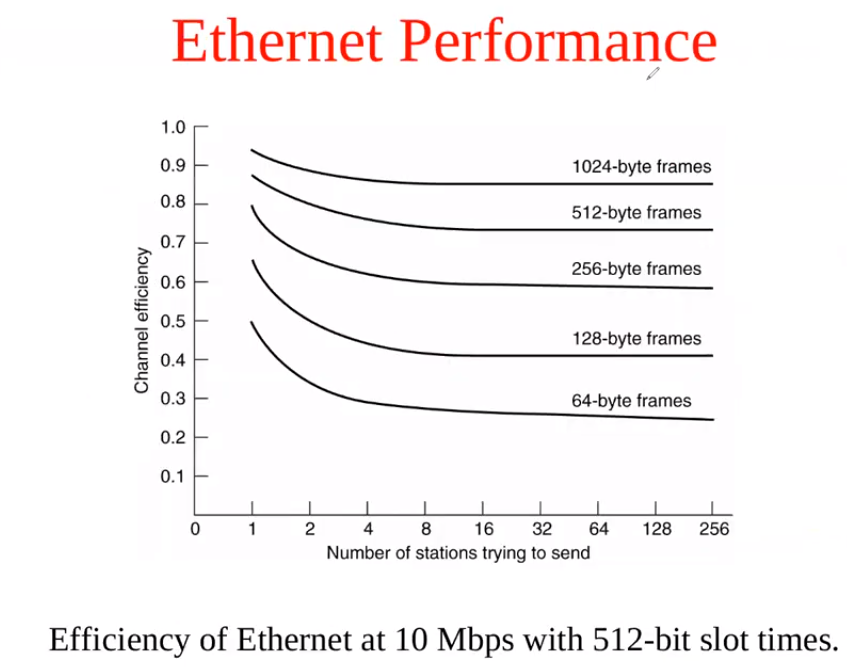
Los 2 protocolos convivían en la misma red física.

En los 802.3, en los primeros bytes de los datos generaron una sub capa, de la sub capa MAC, esta “sub sub” capa se llama LLC (Logical Link Control), y acá van 2 Byte que indican el tipo.

Según el profe: En Ethernet no está el largo, porque esto es una trama de capa de enlace, esto arranca con 0 y 1 que me generan una portadora, cuando se acaba la portadora, se acaba. No hace falta saber el largo, se acabó y listo.

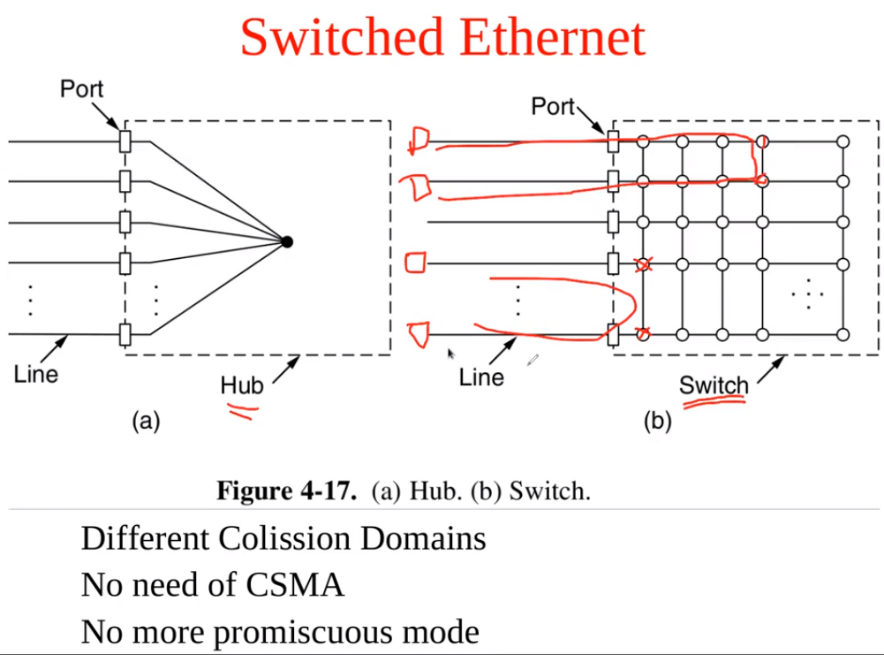
**¿Cómo hacen para que convivan ambos?**

Lo que hicieron fue poner un código para los protocolos de RED, del campo Tipo, mayor a 1500. Ósea si es mayor a 1500 estamos hablando del campo Tipo en Ethernet y si es menor de 1500, es el largo de la trama y se refiere a 802.3, y tenemos que chequear los bytes de LLC para verificar el tipo de protocolo de RED.



Esta el profe la ignoro.

Porque la dirección tiene 6 bytes, si normalmente se usan 4, esto es porque estamos en capa de Enlace. No en capa de RED, no son direcciones IP. Son direcciones MAC, donde los 3 bytes de más alto peso corresponden al fabricante, y los 3 bytes de menor peso para las subplacas. Todas en una red local deben tener una dirección única, no se pueden repetir.

**HUB:**

No importa porque puerto se transmita algo en el Hub, automáticamente se retransmite a todas las demás bocas.

Esto se llama o se dice que hay un solo dominio de colisión.

Todos se juntan en el mismo punto, entonces si 2 escriben pueden colisionar.

**Switch:**

Envía el mensaje solo al destinatario, no a todos.

Básicamente tiene una matriz de conmutación adentro.

Tiene la ventaja de comunicación simultanea entre distintos nodos y no pasa nada. Tienen menos colisiones, pero se sigue usando CSMA cuando hay trama de difusión. Es “casi” no necesario.

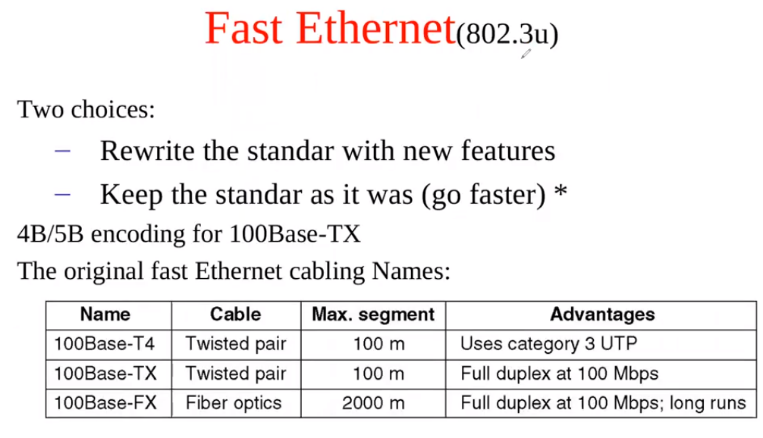
¿Cómo sabe cómo tiene que conmutar? ¿En qué puerto está conectada cada maquina?

Por las direcciones, Los Switch tienen una tabla donde tienen asociada cada puerto o boca, con una dirección MAC.

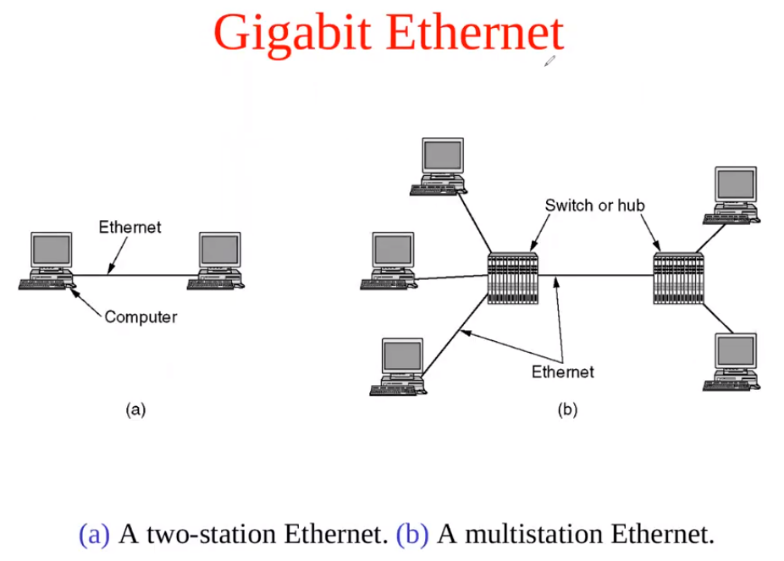
Entonces cada vez que llega una trama a un puerto, se fija en la dirección y en la tabla. Y realiza la conexión correspondiente.

Esta tablita que asocia dinámicamente puertos con direcciones MAC está en RAM. Tiene un tamaño determinado.

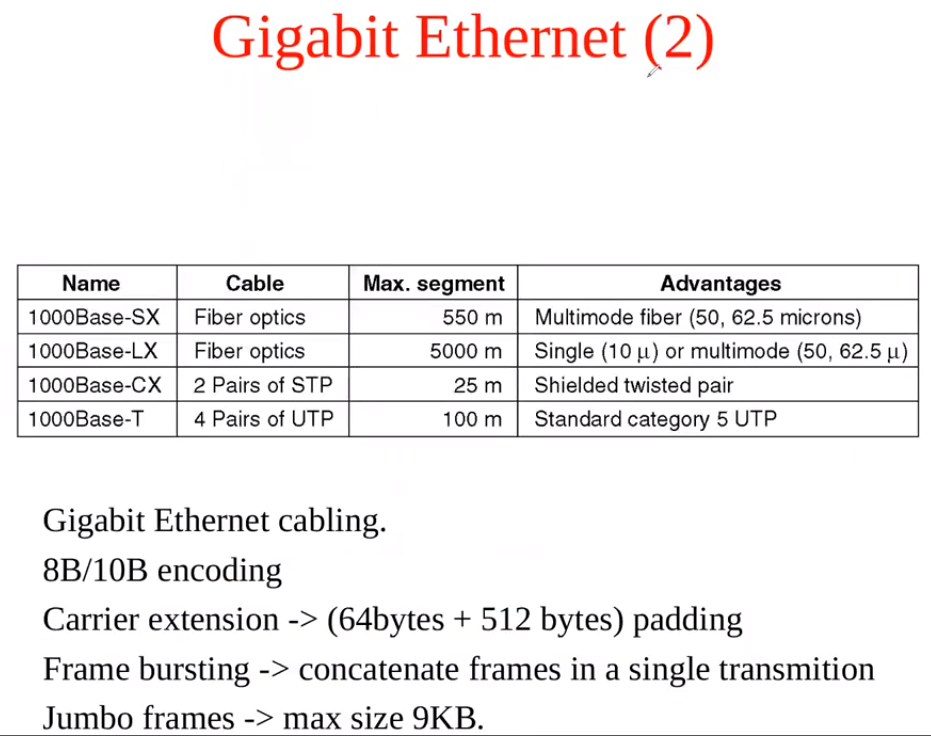
Ej: de ataque por inundación …… Cuando no sabe que MAC esta con que puerto, manda a todos y después completa la tabla. Tienen un poquito más de seguridad que los HUB si esnifean.



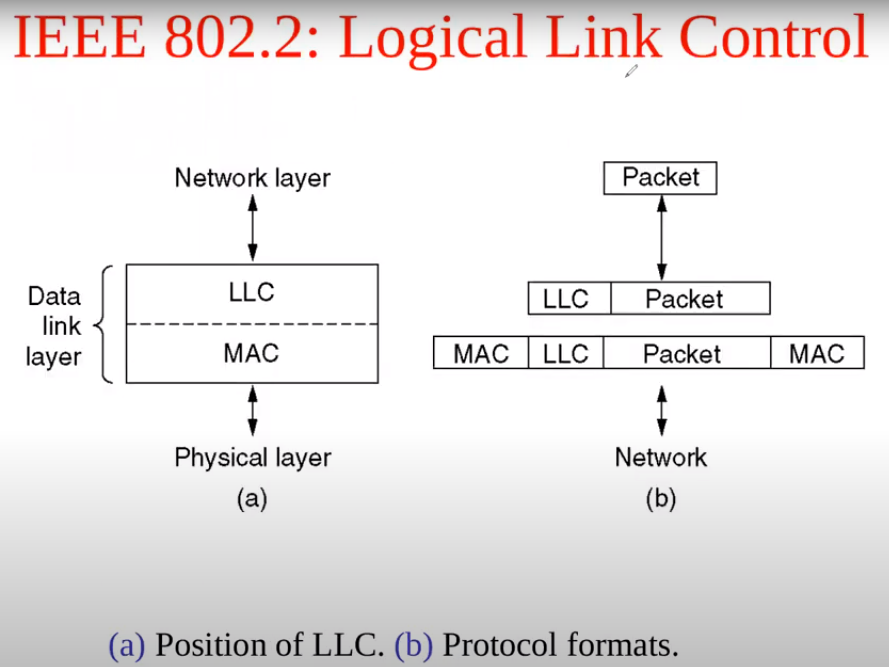
El profe lo ignora.



El profe lo ignora.



El profe lo ignora.

Acá retoma el profe. Donde se detalla un poco 802.3

Como hace con el campo que antes era Tipo.

Ósea entre la MAC y la LLC formarían lo que es la capa de enlace. Abajo la subcapa física y arriba la de red.