

Capa de enlace

Los canales de comunicación (capa física) tienen problemas y suelen ocurrir errores. El objetivo de la capa de enlace es poder resolver esos errores. Y generar una comunicación confiable entre dos Hosts.

Los protocolos de Capa de enlace para poder generar conexiones confiables entre 2 hosts se encargan de:

- Control de flujo: evitar que emisor rápido sature receptor lento
 - .Protocolos de tubería estudiados en capa de transporte
- Entramado:
 - En el canal solo hay un stream de bits, el protocolo se encarga de diferenciar donde comienzan y terminan cada entramado y así definir los paquetes.
- Detección y corrección de errores:
- Manejo de colisiones:
 - .Dos máquinas quieren enviar tramas al mismo tiempo por el mismo canal

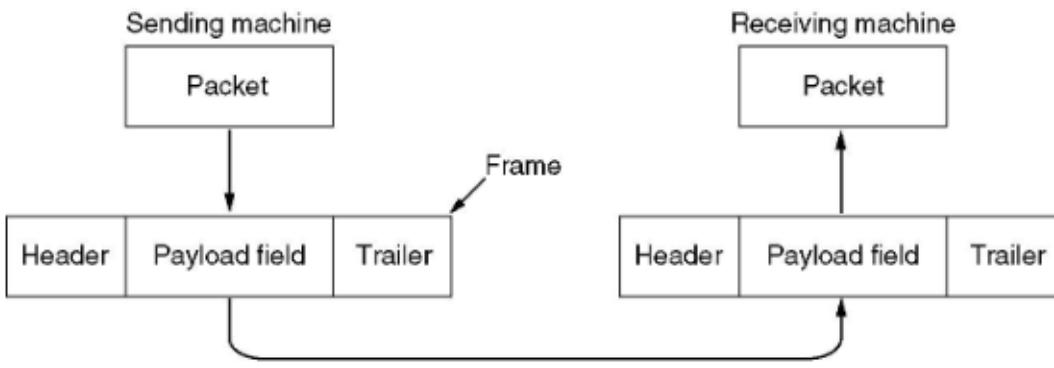
Qué suele contener una trama luego de pasar por la capa de enlace de datos.

- encabezado: suele contener: direcciones del origen y de destino; a veces la longitud de la trama, etc.
- campo de carga útil (el contenido que se quiere enviar).
- un terminador final (para control de errores)

Bytes	8	6	6	2	0-1500	0-46	4	
(a)	Preamble	Destination address	Source address	Type	Data »»	Pad	Check-sum	
(b)	Preamble	S o F	Destination address	Source address	Length »»	Data »»	Pad	Check-sum

La comunicación entre CEDs de diferentes máquinas utiliza los mismos conceptos que la capa de transporte.

- Confirmaciones de recepción de tramas
- Temporización de reenvío
- Retransmisiones de tramas (perdidas o dañadas)
- Uso de números de secuencia en las tramas (para identificar tramas duplicadas).
- Llevar a caballito (piggybacking) – para aprovechar mejor el canal de comunicaciones.
- Uso de protocolos como parada y espera o de tubería (go back N, repetición selectiva).



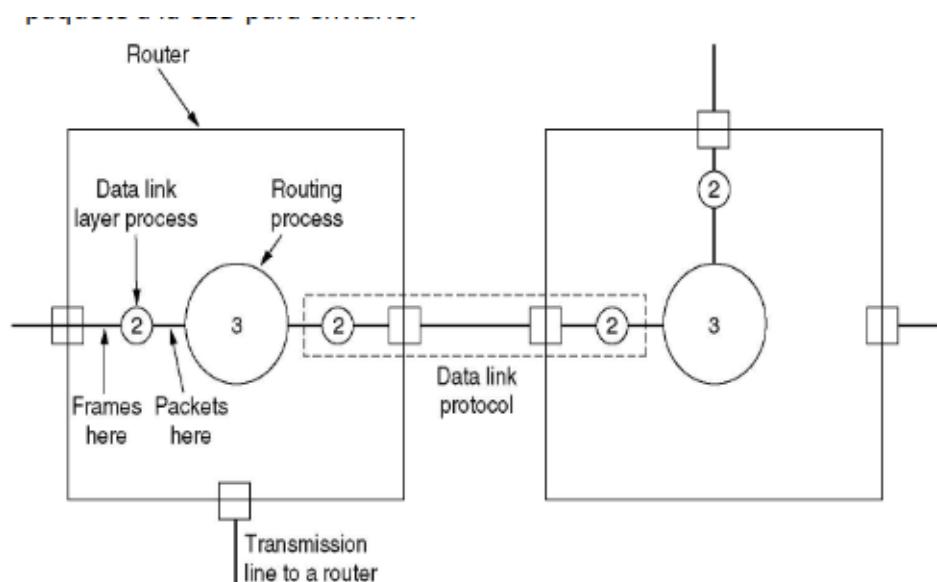
- La CED toma de la CR paquetes y los encapsula en **tramas**.
- Las tramas tienen una **longitud máxima** impuesta.
- Cada paquete de la CR se divide en tramas.
- En la CR de la máquina de origen hay un proceso que entrega bits a la CED para transmitirlos a la máquina de destino.
- El trabajo de la CED es transmitir los bits a la máquina de destino para que puedan ser entregados a su CR.

Control de Flujo

Al llegar una trama a un enrutador, este controla si esta libre de errores.

Si es la trama esperada, entonces se pasa esa trama al software de enrutamiento.

El software elige el lugar adecuado por donde enviar esa trama, y le devuelve el paquete a la CED para que lo envie.



Al igual que la capa de transporte, la capa de enlace utiliza algoritmos de chequeo de envío de tramas.

Si una trama se llega, se reenvia una trama de control con confirmación de recepción positivo o negativo.

Al igual que CT, se usan temporizadores de retransmisión en el emisor.

Al enviarse una trama, se inicia un **temporizador**.

Si la trama o la confirmación de recepción se pierden el temporizador expirará. Luego, se puede enviar la trama de nuevo.

Si la confirmación de recepción llega antes que el temporizador expira, entonces el temporizador se cancela.

¿Que sucede con las tramas duplicadas? Es decir, se perdió la trama de confirmación y entonces el emisor reenvió la trama.

Al igual que CT, se usan números de secuencia en las tramas que salen, y el receptor tiene una función que dado un número de secuencia de la trama que llega, decide si ella es duplicada o no.



Problema: ¿Cómo transmitir datos entre dos máquinas y en ambas direcciones eficientemente? (recordar lo que hace TCP)

Solución: Llevar a caballito (piggybacking).

- cuando llega una trama de datos, el receptor se aguanta y espera hasta que la CR le pasa el siguiente paquete P .
- La confirmación de recepción se anexa a la trama de datos de salida
 - con P - (usando el **campo ack** en el encabezado de la trama).

Cuando la capa de red no tiene ningún paquete para enviar, entonces nunca mandaríamos la confirmación. Por lo que si en x msegundos no llega un paquete a la CED, entonces se manda una trama de ACK independiente.

Canales de Difusión

Como no puede haber un cable que conecte cada máquina entre sí, se usan canales de difusión. En un canal de difusión se conectan varias máquinas, de modo que si una máquina envía un mensaje, lo reciben todas. Los canales pueden ser:

- Inalambricos
- Cableados

Debido a que varias máquinas están conectadas a un mismo canal, se debe tener un algoritmo de control de colisiones, ya que más de una vez dos o más máquinas querrán enviar mensajes simultáneamente por el mismo canal. ¿Qué es una colisión? Cuando dos tramas se traslapan en el tiempo y la señal resultante se altera. La idea es evitar que ocurran, o que ocurran la menor cantidad posible.

Control de Colisiones

Para solucionar las colisiones se crea una subcapa de capa de enlace, que se encarga únicamente de las colisiones. Se llama subcapa de control de acceso al medio SCAM

- La subcapa MAC es una subcapa inferior de la CED.

El objetivo principal de los protocolos de colisión en una red de difusión, es como determinar quien puede usar el canal cuando hay competencia sobre el mismo.

Para ello están los protocolos de acceso multiple- PAM.

Definen quien es el siguiente en usar el canal de difusión.

En las redes inalámbricas, se usan Access points que coordinan las comunicaciones entre los hosts.

Y en las redes cableadas, cuando se encuentran muchas máquinas conectadas a un Hub, o a un mismo cable coaxial. Ethernet usa el protocolo CSMA/CD.

Redes Cableadas

Vamos a suponer que en esta red hay N estaciones totalmente independientes, y que todas usan el mismo canal para transmitir y recibir tramas.

Cada máquina puede:

- Detectar que el canal está en uso
- Detectar una colisión en el canal

En las LANs actuales, cada estación puede detectar cuando el canal está en uso. Los protocolos que detectan cuando están ingresando bits al canal se llaman: Protocolos de detección de portadora.

- Se evita generar colisión al no poner tramas cuando se sabe que están llegando bits de alguna otra trama.

En las LAN actuales cada estación puede **detectar si está ocurriendo una colisión** cuando está transmitiendo una trama.

Para detectar colisiones:

- El hardware de una estación escucha el cable mientras transmite.
- Si lo que lee es distinto de lo que puso en él, sabe que está ocurriendo una colisión.

Si una estación que está transmitiendo una trama detecta que está ocurriendo una colisión,

- no tiene sentido seguir enviando la trama;
- por lo tanto es mejor que las estaciones **aborden sus transmisiones tan pronto como detecten una colisión.**

Estas dos funcionalidades son necesarias para poder definir diferentes PAMs.

Protocolos de accesos múltiples.

PAM: ALOHA

El emisor:

- Transmite cuando tiene datos para enviar.
- Escucha el canal por un tiempo igual a la demora de propagación de ida y vuelta máxima en la red + un incremento fijo de tiempo.
- Si se escucha un ack en ese tiempo, todo anduvo bien.
- Sino se espera un tiempo aleatorio y la trama se manda de nuevo
- Si se falla en recibir un ack luego de varias retransmisiones se tira la toalla.

El receptor

- Al recibir una trama chequea su validez y si lo es, inmediatamente manda un ack.
- Si la trama es inválida el receptor la ignora.
 - La trama puede ser inválida por ruido o por colisión.

Evaluación de ALOHA puro:

- El método ALOHA puro bajo carga baja es eficiente y tiene una demora baja.
- En ALOHA puro *una estación no escucha el canal antes de transmitir*; esto generará probablemente muchas colisiones.
- Como el número de colisiones crece rápidamente a medida que aumenta la carga, la máxima utilización del canal alrededor del 18%.

CSMA persistente 1

Protocolo CSMA persistente-1 para el emisor

- Si una estación tiene datos por enviar, primero escucha el canal para saber si otra está transmitiendo en ese momento.
- Si el canal está ocupado, entonces la estación espera hasta que se desocupe.
- Cuando la estación detecta un canal inactivo, transmite una trama.
- Si ocurre una colisión, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo.

Comportamiento luego que emisor envió una trama:

- La estación espera un tiempo razonable por un ack
 - Teniendo en cuenta el tiempo de propagación de ida y vuelta máximo en la red y el hecho que la estación receptora también debe competir por el canal para responder.
- Si no recibe ack en ese tiempo, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo.

Protocolo CSMA persistente-1 para el receptor

- Al recibir una trama chequea su validez y si lo es, manda un ack.
 - Tener en cuenta que para eso hay que competir por el canal.
- Si la trama es inválida el receptor la ignora.
 - La trama puede ser inválida por ruido o por colisión.

El **retardo de propagación** tiene un efecto importante en el desempeño de CSMA persistente 1.

- Caso de que justo después de que una estación comienza a transmitir, otra estación está lista para enviar;
- si la señal de la primera estación no ha llegado aun a la segunda, esta última detectará un canal inactivo y comenzará a enviar también,
 - eso producirá una colisión.
- *Cuanto mayor sea el tiempo de propagación, más importante será este efecto.*

Aun si el retardo de propagación es cero, habrá colisiones.

□ **Situación:** dos estaciones quieren enviar y detectan que una tercera está transmitiendo.

- Luego que la tercera termine de transmitir las dos estaciones que quieren enviar detectarán un canal inactivo,
 - por lo tanto enviarán y se producirá una colisión.

CSMA/CD con detección de colisiones.

Este PAM es el que se utiliza en las LANs Ethernet.

En CSMA/CD el emisor

1. Antes de transmitir una trama detecta la portadora.
2. Si el canal está libre transmite.
3. Sino espera hasta que el canal se desocupe para transmitir.
4. Si el emisor detecta una colisión, aborta la transmisión, espera un tiempo aleatorio, y una vez que pasó este tiempo: goto 1.

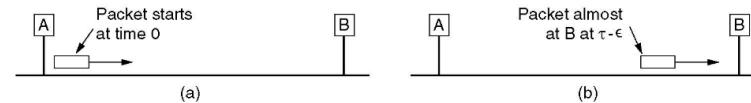
En CSMA/CD el receptor

1. Recibe una trama buena si no hubo colisión y el medio no cometió errores.
2. En caso contrario (hubo colisión o el medio cometió errores) recibirá una trama dañada la cual será descartada.
3. Al mandar una confirmación de recepción hace los pasos del emisor (ver filmina previa).

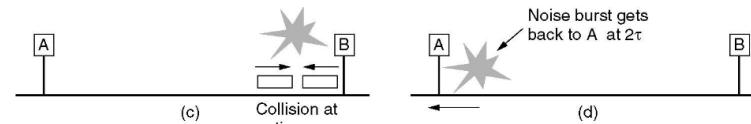
Como una estacion se da cuenta de la colision?

Decimos que una estacion tomo el canal cuando todas las demas estaciones sabian que estaba transmitiendo y no interfirieron. Que las estaciones sepan que tomaron el canal, y quien tomo el canal es fundamental para evitar las colisiones.

El tiempo minimo para detectar una colision es el tiempo que tarda la señal en propagarse de una estacion a otra.



Una estacion no puede estar segura de que tomo el canal hasta que transmitio durante 2τ sin detectar colision.



Las tramas deben tardar al menos 2τ en enviarse, por lo que las tramas tienen un tamaño minimo.

- τ el tiempo que tarda una señal en propagarse entre las dos estaciones más lejanas A y B
- **Cómo ocurre una colisión en CSMA/CD y cuándo se enteran las estaciones de ella:**
 1. A comienza a transmitir en $t = 0$.
 2. En $\tau - \epsilon$ un instante antes de que la señal llegue a B, B comienza a transmitir.
 3. B detecta la colisión casi de inmediato y se detiene.
 - En Ethernet se genera ráfaga de ruido de 48 bits.
 4. La ráfaga de ruido causada por la colisión no regresa a A hasta pasados $2\tau - \epsilon$.

Alguna de las tareas que tiene que realizar la capa de enlace como el entramado, control de errores, detección de portadora y colisiones. Se puede hacer por hardware por lo que se tienen dos componentes de hardware:

- Transceptor: maneja detección de portadora y colisiones
- Tarjeta controladora: se encarga de
 - ensamblar los datos en el formato de trama adecuado
 - calcular terminador de las tramas de salida
 - comparar las tramas de entrada (detección de errores)

Cableado de ethernet SCAM(MAC)

Cada cable tiene una longitud máxima de cable por segmento, es decir que a medida que se va propagando la señal por un cable, esta se va debilitando. Por ende se necesitan usar repetidores para recorrer largas distancias. Un repetidor amplifica la señal y la retransmite en ambas direcciones.

Hay diferentes formas de crear cableados.

1. Un cable pasa entre cuarto y cuarto y cada estación se conecta a él en el punto más cercano.

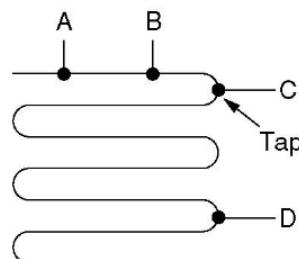
2. Una **columna vertical** corre del sótano a la azotea y en cada piso se conectan cables horizontales a dicha columna.

- ¿hacen falta repetidores?

- En cada piso conectar cable a columna con un repetidor entre ambos.

3. Topología de **árbol**:

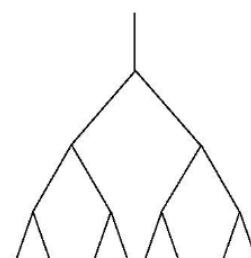
- El medio de transmisión es un cable que **se divide en ramas**.
- El árbol tiene puntos conocidos como **headends**, donde uno o más cables comienzan (a su vez cada uno de estos podrá tener ramas).
- La transmisión desde una estación se propaga por el medio y puede ser recibida por todas las otras estaciones.



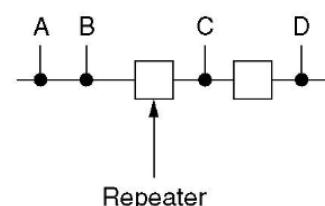
(a)



(b)



(c)



(d)

Cable topologies. (a) Linear, (b) Spine, (c) Tree, (d) Segmented.

Como definir el tamaño mínimo de una trama.

El tamaño mínimo de una trama estará determinado por como está formado el cableado y su velocidad, ya que eso define el tiempo de propagación, por ende debemos generar tramas que tarden 2T en transmitirse por lo menos. Para lograr lo nombrado anteriormente

Ejercicio: Para una LAN de 10 Mbps con una longitud máxima de 2500 m y cuatro repetidores, el tiempo de ida y de vuelta es aproximadamente de 50 µseg en el peor caso.

- ¿Qué tamaño conviene que tenga la trama mínima?

Solución:

- La trama mínima debe tomar por lo menos 50 µseg en transmitir.
- A 10 Mbps, un bit tarda 100 nseg por lo que 500 bits es la trama más pequeña que se garantiza funcionará.
 - Para agregar algún margen de seguridad, este número se redondeó a 512 bits o 64 bytes.

A medida que aumente la velocidad de la red, la longitud mínima de la trama debe aumentar o la longitud máxima del cable debe disminuir, de manera proporcional.

Tras una colisión el tiempo se divide en ranuras cuya longitud es igual a 2T. Cuando una estación encuentra una colisión, debe esperar cierto tiempo hasta volver a intentar enviar una trama. La idea es que cuando ocurre una, las estaciones involucradas esperan x cantidad de ranuras.

Algoritmo de retroceso exponencial binario:

- Tras la primera colisión cada estación espera de 0 a 1 tiempos de ranura antes de intentarlo de nuevo.
 - Si dos estaciones entran en colisión, y ambas escogen el mismo número aleatorio, habrá una nueva colisión.
- Despues de la segunda colisión cada una escoge 0,1,2 o 3 al azar y espera ese número de tiempos de ranura.
- Si ocurre una tercera colisión, entonces para la siguiente vez el número de ranuras a esperar se escogerá al azar en el intervalo 0 a 7.
- Tras i colisiones se escoge un número aleatorio entre 0 y $\exp(2,i)-1$ y se salta ese número de ranuras.
- Tras haberse alcanzado 10 colisiones el intervalo de aleatorización se congela en un máximo de 1023 ranuras.
- Tras 16 colisiones el controlador tira la toalla y avisa de un fracaso a la computadora. La recuperación posterior es responsabilidad de las capas superiores.

Evaluación:

- El algoritmo asegura un retardo pequeño cuando unas cuantas estaciones entran en colisión.
- El algoritmo asegura que la colisión se resuelva en un intervalo razonable cuando hay colisiones entre muchas estaciones.

Formato de trama de Ethernet

Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preamble	Destination address	Source address	Type	Data ss	Pad	Check-sum

Trama DIX Ethernet (Dec, Intel, Xerox)

- Preambulo de 8 bytes, cada uno es 10101010
- Direcciones de 6 bytes:
 - . 6 pares de digitos hexa separados por -
 - . el bit de orden mayor de la direccion de destino es 0 para las direcciones ordinarias y 1 para las direcciones de grupo.
 - . Una trama que consiste unicamente de bits 1 en el campo de destino, se acepta en todas las estaciones de la red(broadcasting)
- Campo tipo:
 - . Uso de multiples protocolos de CR a la vez en la misma maquina
 - . El kernel debe saber a cual entregarle la info de la trama que llego
 - . Indica al receptor a que proceso entregarle la trama
- Longitud de trama minima
 - . Las tramas deben tener al menos 64 bytes de largo, desde la direccion de destino hasta la suma de verificacion
 - . Si la porcion de datos de una trama es menor a 46, se usa el campo de relleno para alcanzar los 64B.
- Suma de verificacion:
 - . 32 bits de largo, se usa el metodo de deteccion de errores llamado codigo polinomial

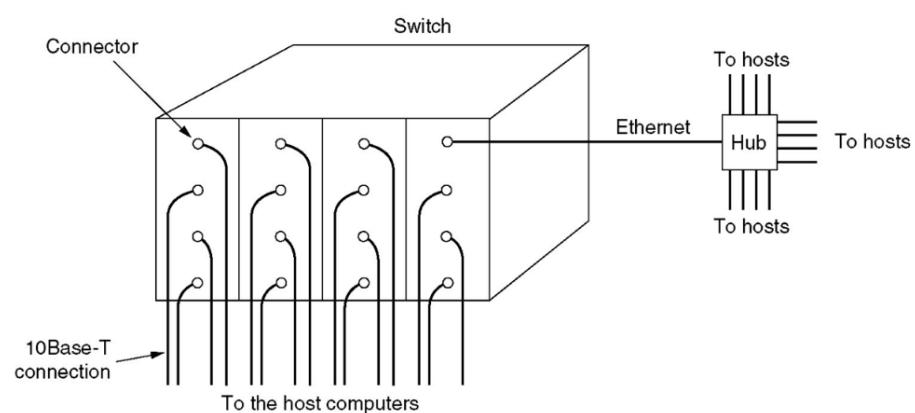
Bytes	8	6	6	2	0-1500	0-46	4	
	Preamble	S o F	Destination address	Source address	Length	Data ss	Pad	Check-sum

Formato IEEE 802.3

- Cuando IEEE estandarizó la Ethernet hizo los siguientes cambios al formato DIX:
 - Reducir el preámbulo a 7 bytes y usar el último byte para un **delimitador de inicio de trama**.
 - Cambiar el campo de Tipo por un **campo de Longitud**.
 - Poner un pequeño encabezado a los datos para dar informacion de tipo.

Ethernet conmutada

A medida que se agregan mas estaciones, aumenta el trafico y hay que evitar que se sature la LAN. Para ello se utilizan los conmutadores(switches). Tienen varios dominios de colisiones y son muy rapidos para enviar de una maquina de un dominio de colisiones a otra en otro dominio.



Almacena y reenvia tramas de Ethernet.

No deben ser configurados

- **Solución:** usar una **Ethernet commutada**.

- Un **comutador (switch)** contiene una **matriz de conmutación** de alta velocidad y de 4 a 32 **tarjetas de línea**,
- Cada tarjeta de línea contiene de 1 a 8 **conectores**.
- Hay matrices de conmutación que funcionan a más de 1 Gbps.

Si dos máquinas conectadas a la misma tarjeta de conexión transmiten tramas al mismo tiempo:

- Si todos los puertos de la tarjeta forman una LAN local dentro de la tarjeta,
 - las colisiones en esta LAN en tarjeta se detectan y manejan igual que en una red CSMA/CD.
 - Las tarjetas pueden estar transmitiendo en paralelo.
- Si cada puerto de entrada se almacena en un **búfer**,
 - todos los puertos de entrada reciben y transmiten tramas al mismo tiempo, para una operación en paralelo duplex.
 - Cada puerto es un dominio de colisión independiente.

Cada comutador tiene una **tabla de comutador**:

- <dirección MAC del host, interfaz para alcanzar el host, estampilla de tiempo>

Un comutador **aprende** cuáles hosts pueden ser alcanzados a través de cuales interfaces

- **Cuando el comutador recibe una trama**
- registra el par emisor/localización en la tabla del comutador.

Con un switch se pueden enviar tantos datos por segundo como la capacidad de la matriz.

Como tiene un bufer por cada tarjeta de entrada, entonces ocurren menos colisiones.

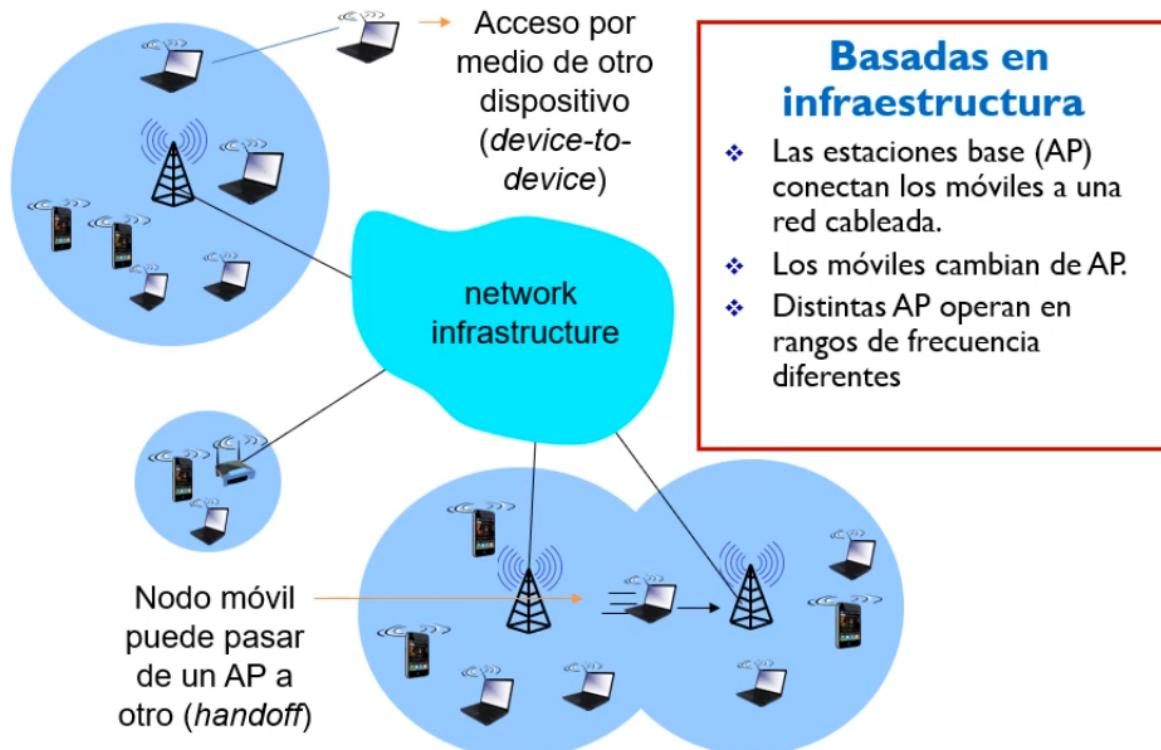
Reenvío de una trama recibida por el comutador:

1. Registrar enlace de ingreso, dirección MAC del host emisor de la trama.
- **Identificación de la interfaz del destino:**
2. Se Busca en la tabla del comutador la dirección MAC del destino.
3. **if** se encuentra la entrada para el destino
then {
 - if** el destino está en el segmento por el cual vino la trama
then descartar trama
 - else** enviar trama en la interfaz indicada por la entrada
- }
 ➤ **si no se encuentra una entrada para el destino:**
else inundar /* enviar en todas las interfaces excepto aquella por la que llegó la trama */

Aquí asumimos que cada tarjeta constituye un dominio de colisiones.

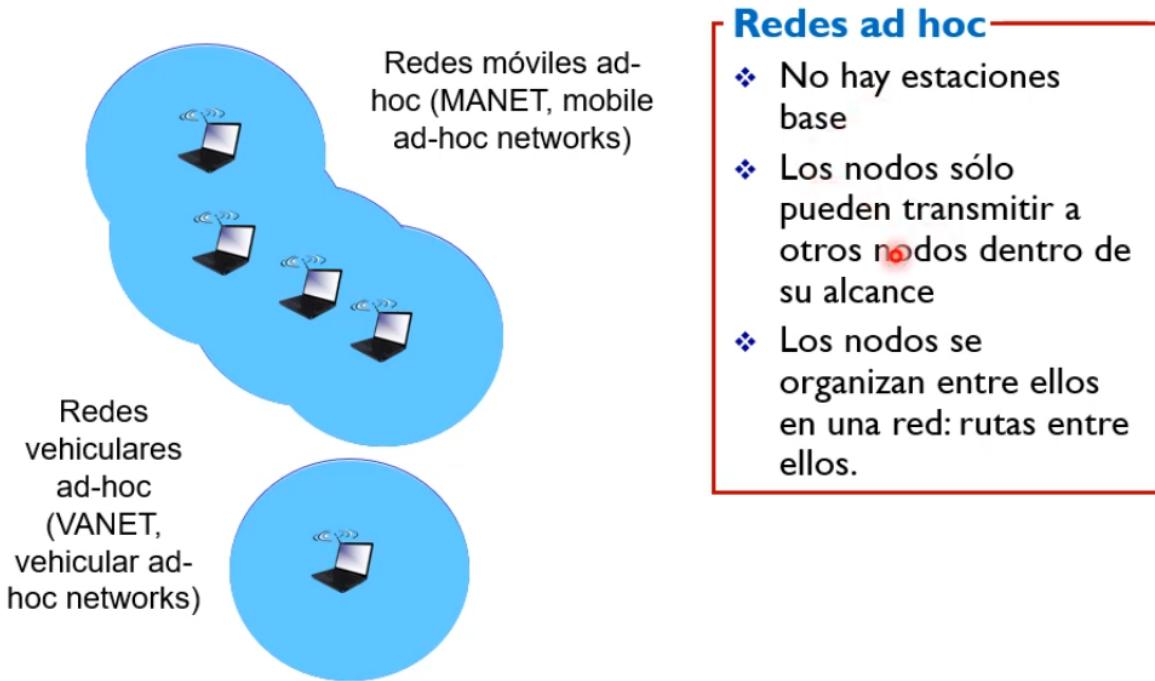
Redes inalámbricas

Las redes inalámbricas tienen la particularidad de que los nodos, o hosts. Pueden ir cambiando de área y por ende de conexión inalámbrica. Hay diferentes tipos de redes, las redes basadas en infraestructura.



Basadas en infraestructura

- ❖ Las estaciones base (AP) conectan los móviles a una red cableada.
- ❖ Los móviles cambian de AP.
- ❖ Distintas AP operan en rangos de frecuencia diferentes



Las redes basadas en infraestructura, tienen la funcionalidad de acceder a la internet, es decir todos los dispositivos conectados tendrán acceso. En cambio en las red adhoc, no necesariamente existe esta conexión a internet sino son para transmitir datos entre esos dispositivos. Y si o si deben estar dentro de su alcance. No tienen jerarquía.

En las redes de infraestructura, un nodo puede cambiarse de área de AP, y conectarse a otro AP sin perder la conexión o darse cuenta de eso.

Al igual que en las redes cableadas, la información se transmite en señales. Pero hay más problemas y peligros de perder la intensidad y calidad de la señal. .

- **Intensidad decreciente de la señal**
 - Dispersión, atenuación
- **Interferencias de otros orígenes**
 - Ruido electromagnético, bandas abiertas ISM
- **Propagación multi-camino (*multipath*)**
 - Rebotes en objetos

Mayor tendencia a errores en el bit que redes cableadas

por lo que...

Usan técnicas de detección y recuperación de errores más robustas

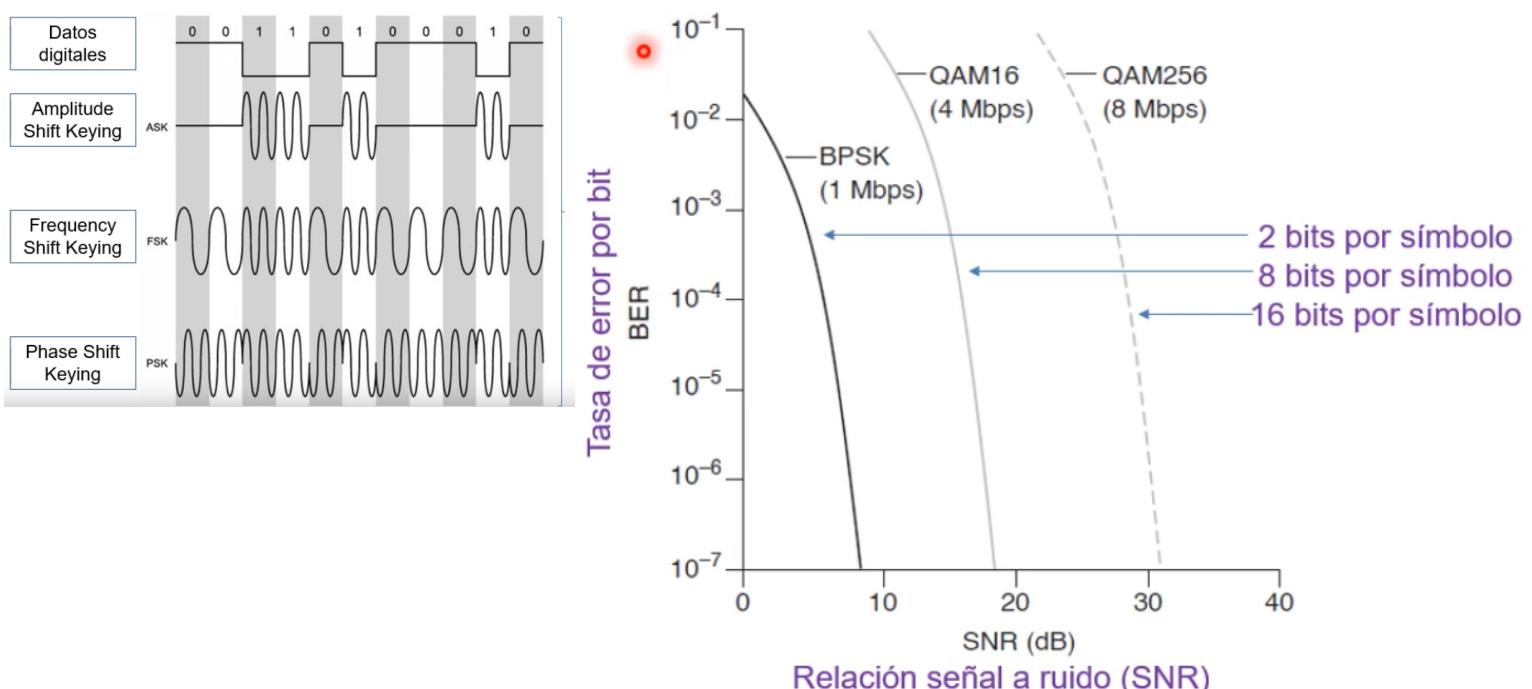
Las señales, son electromagnéticas, entonces se necesitan que los receptores tengan otras capacidades extras, y por ende la calidad de la señal también.

- Es necesario que la intensidad de la señal sea igual o superior a la sensibilidad del nodo receptor (RSSI). Para que el receptor pueda detectarla.
- Es necesario que la relación señal ruido es una relación que existe entre la potencia de la señal, y el ruido del medio. La señal debe ser lo suficientemente limpia para que pueda ser interpretada por el receptor. (SNR)

Se miden en dB y dBm

La tasa de error (BER) dependerá de las características anteriores.

Según la modulación de la señal, esta dada la relación señal a ruido.



Para un esquema de modulación, cuanto mayor es la SNR, menor BER

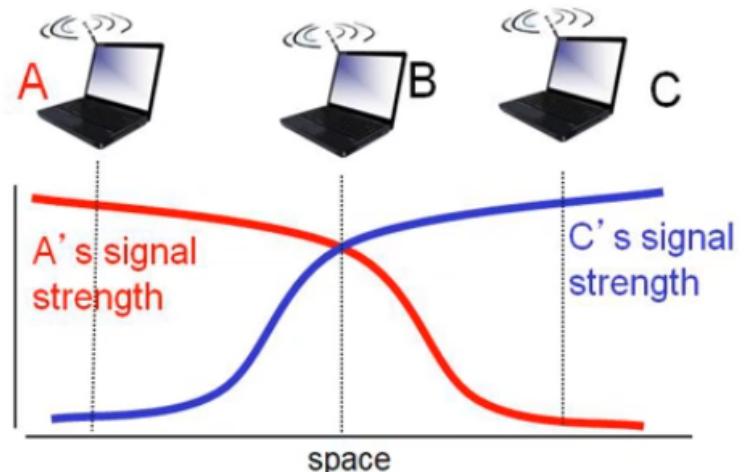


Para una SNR dada, una modulación con tasa de bit más alta tendrá un mayor BER

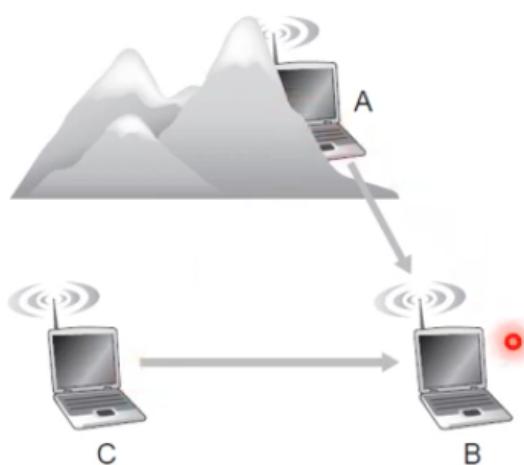
Puede utilizarse una **selección dinámica del esquema de modulación y de la potencia de transmisión adaptativas** para cumplir con un BER objetivo (WiFi, 4G...)

Problemas de las comunicaciones inalámbricas.

- Los nodos inalámbricos usualmente no pueden transmitir y recibir al mismo tiempo.
- La potencia generada por el emisor es mucho más alta que lo que probablemente será una señal recibida y así se satura el circuito receptor.
- No se puede comparar lo que se transmite con lo que se escucha para detectar colisiones.
- En lugar de **CSMA/CD** (Acceso Múltiple con Detección de Portadora y Detección de Colisiones) (**Ethernet**) se usa **CSMA/CA** (Acceso Múltiple con Detección de Portadora y Evitación de Colisiones) (**WiFi 802.11**)



Problema de la estación oculta.



- C transmite a B
- B recibe la transmisión
- A quiere transmitir a B y escucha el canal a ver si alguien lo esta usando. Como nadie lo esta usando (en realidad C, pero A no ve a C) A transmite.
- A y C están transmitiendo a B, B no entiende nada pq hay colisiones.

Problema de la estación expuesta.

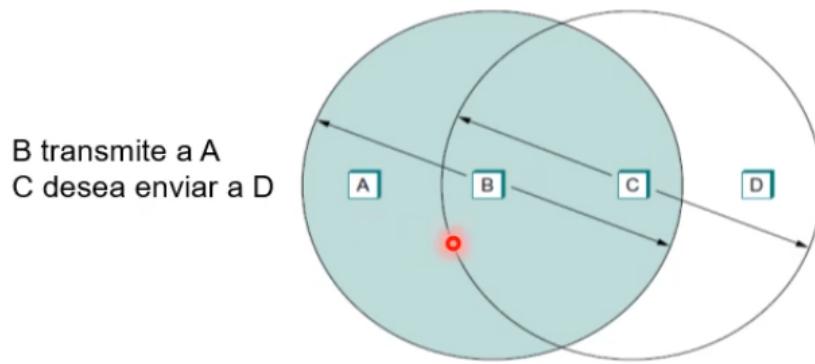


FIGURE 2.31 The exposed node problem. Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A and D's reaches are not shown.)

- B tiene acceso a A y C, y C a A y D.

Si B quiere transmitir a A, lo puede hacer sin problemas.

C quiere transmitir a D, entonces escucha el canal. Si bien tienen rangos diferentes A y D, y se podrían hacer estas dos transmisiones al mismo tiempo. Cuando C intente escuchar el canal, escuchará a B, entonces decide no transmitir.

Pero en realidad no hay problema si C transmitiera a D, porque no interfiere en la capacidad de A de recibir señales.

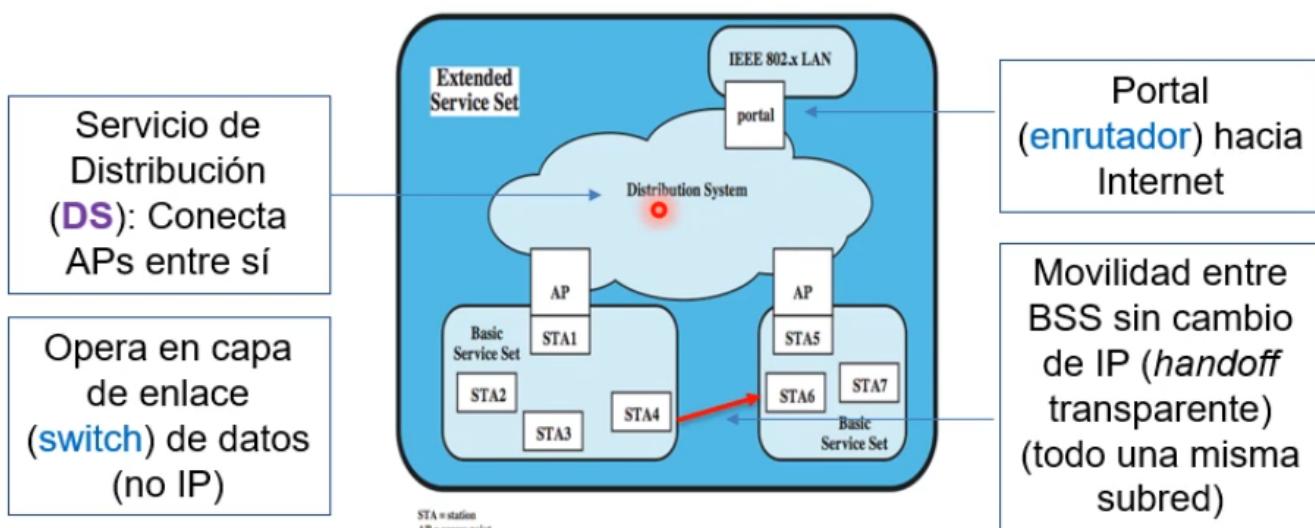
El problema que si puede suceder es que C le intentara enviar a B, y ahí si interfiere con A.

Pero ese no es el problema. Sino es que hay dos nodos expuestos, que tienen rango entre ellos y no pueden compartir simultáneamente a nodos diferentes.

En redes inalámbricas se usa el mismo formato de trama y control de acceso al medio (MAC), cambia la capa física.

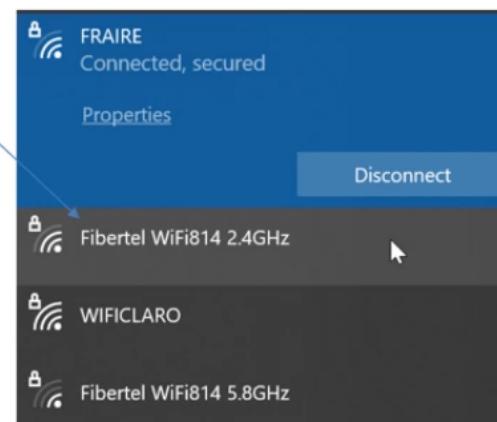
Un componente fundamental del WIFI, o redes inalámbricas. Son los BSS que consiste de un Acces Point(AP) y uno o más nodos. Este acces point está conectado a un switch o router y de ahí a la internet. Por ejemplo las redes hogareñas.

Las BSS están integradas en un conjunto de servicio extendido (ESS). STA son hosts. Todos los BSS están conectados a un DS, que conecta a los AP entre sí. El portal tiene una IP, y cada STA tiene una IP. Pero todos están bajo el mismo dominio. De modo que si una STA se cambia de AP, mantiene su misma IP y puede seguir conectada a internet de la misma forma.



Canales y Asociación

- Cada host necesita **asociarse** con un AP antes de poder enviar o recibir datos de la capa de red
 - Puede haber más de 1 AP
 - Se crea un “cable virtual” entre el host y el AP
- AP → Identificador (**SSID, Service Set Identifier**)
- AP → 11 canales parcialmente solapados
 - Depende del estándar:
i.e., 85 MHz dentro de la banda 2,4 GHz a 2,4835 GHz



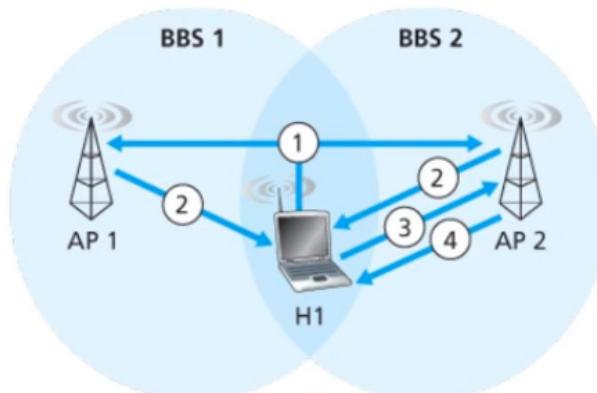
El identificador del AP es necesario para poder establecer la conexión, se le llama SSID.

El protocolo de internet 802.11 no especifica como un host elige con cual AP conectarse.

Puede haber dos situaciones.

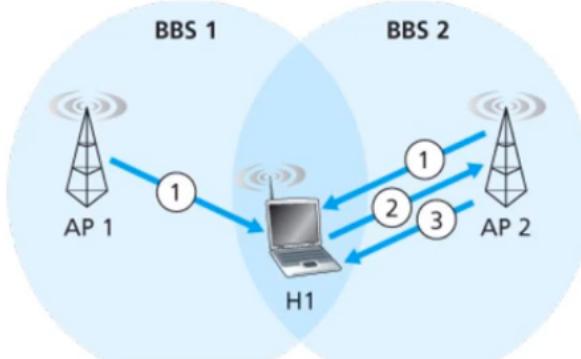
- Un nodo no esta asociado con ningun AP y quiere asociarse, escucha sus 11 canales y detecta cuales AP tiene disponibles. De ahí elige uno para conectarse y se asocia.
- Un nodo puede pasar de estar insatisfecho con su AP y querer conectarse a otro.
 - Mala señal
 - red muy cargada

- **Escaneo Activo:** iniciado por el host
 1. El nodo manda una **trama de prueba**
 2. Los AP al alcance responden con una trama de respuesta
 3. El nodo elige el AP y envía **trama de pedido de asociación**
 4. El AP responde con una **trama de respuesta de asociación**
 - Re-asociación: el nuevo AP notifica al AP anterior del cambio.



- **Escaneo Pasivo:** iniciado por el AP

1. AP difunde una **trama guía** periódicamente
 - Capacidades (i.e., tasas de transmisión) e identificador del AP, la hora, cuánto falta para la próxima trama guía, etc.
2. El nodo elige el AP y envía **trama de pedido de asociación**
3. El AP responde con una **trama de respuesta de asociación**



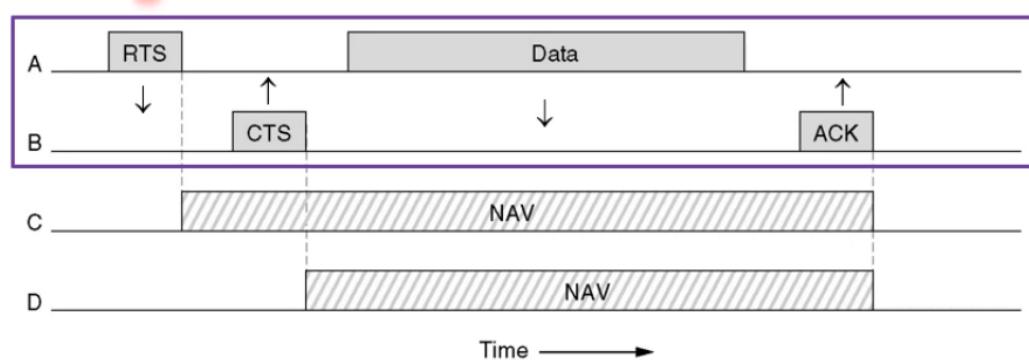
802.11 tiene una subcapa MAC, es decir un protocolo de como se accede al medio cada host.

- Usa CSMA/CA, acceso multiple con detección de portadora y evitación de colisiones.
 - escucha primero si hay otro dispositivo transmitiendo y si no hay, entonces pide comenzar a transmitir. En este caso, mientras transmito no puedo escuchar al mismo tiempo, entonces no puedo detectar las colisiones como en ethernet.

Solo dos modos:

- DCF (función de coordinación distribuida) para redes ad-hoc
- PCF (función de coordinación puntual) redes basadas en infraestructura AP.

DCF



RTS: request to send

RTS y CTS solo existen en redes inalámbricas. Y existen para evitar las colisiones. Ya que los demás nodos van a escuchar el RTS, entonces sabrán que no pueden usar el canal.

A desea enviar a **B**; **C** es una estación que está dentro del alcance de **A**; y **D** está dentro del alcance de **B** pero no dentro del de **A**. Entonces:

1. **A**: envía una trama **RTS** a **B** (permiso para enviarle una trama)
2. **B**: recibe esta solicitud, y decide otorgarle el permiso: envía una trama **CTS**
3. **A**: recibe **CTS** y envía su trama. Comienza su temporizador de **ACK**. Si termina antes de que el **ACK** regrese, todo el protocolo se ejecuta de nuevo.
4. **B**: al recibir correctamente la trama, responde con una trama de **ACK**

Comportamiento de los hosts **C** y **D**:

1. **C**: recibe la trama RTS y desiste de transmitir hasta que el intercambio esté completo. Con la información en RTS, **C** estima cuánto tardará la secuencia, incluyendo el ACK final, e inicia un NAV (vector de asignación de red).
2. **D**: **D** escucha el CTS y también impone un canal NAV para si misma.

El nodo **C** escucha a **A** y **B** solo escucha a **B**. Es una estación oculta. Pero no ocurre ese problema, pq ambos escucharon o el RTS o CTS entonces se ponen en modo NAV.

En RTS y CTS se avisa el tamaño de los datos que se van a enviar, entonces **C** y **D** saben cuánto tiempo deben estar callados.

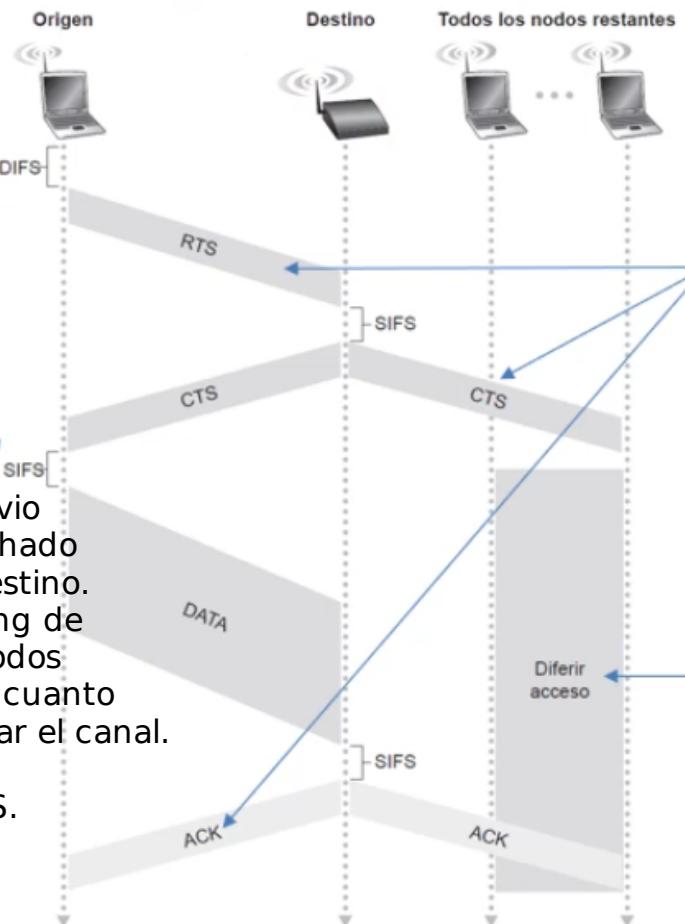
DCF

Tiempo entre tramas (lo vemos después), pero:

- DIFS: DCF
- SIFS: Short (misma conversación)

En este caso, el origen envió su RTS, pero no fue escuchado por otros. Pero si por el destino. Que este hace broadcasting de ese aviso. De modo que todos los otros nodos sepan por cuánto tiempo no van a poder usar el canal.

DIFS más grande que SIFS.



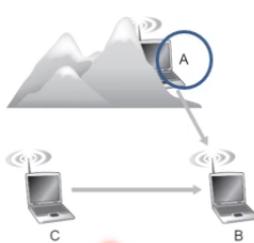
En general las tramas de control se transmiten a menor tasa de transferencia que las tramas de datos (menos probable que ocurran errores de transmisión)

Dos nodos pueden enviar RTS al mismo tiempo. Colisión! En ese caso ningún destino recibirá los RTS, entonces ningún emisor recibirá los CTS. Por lo que usando el algoritmo de retroceso exponencial binario, los emisores esperan y vuelven a intentar.

Se soluciona el problema de estación oculta porque A va a escuchar el CTS de B, entonces sabrá que no puede enviarle nada ya que otro le está enviando.

Estación oculta: CTS es escuchado por una estación oculta (establece el NAV)

- No envía nada (tiempo incluido en el RTS y CTS)
- Luego de ese tiempo más un pequeño intervalo el canal puede ser assumido disponible otra vez y otro nodo es libre de intentar enviar



Hay una relación uno a uno entre hosts y AP
(asociación) → BSS

AP: responsable de **enviar y recibir datos** (i.e. paquetes) desde y hacia hosts asociados con el AP

AP: responsable para **coordinar la transmisión** de varios hosts inalámbricos asociados

AP: sondea los nodos preguntándoles si tienen tramas para enviar

AP: → **no ocurren colisiones**

El AP se vuelve un intermediario.

El tiempo en el medio se divide en

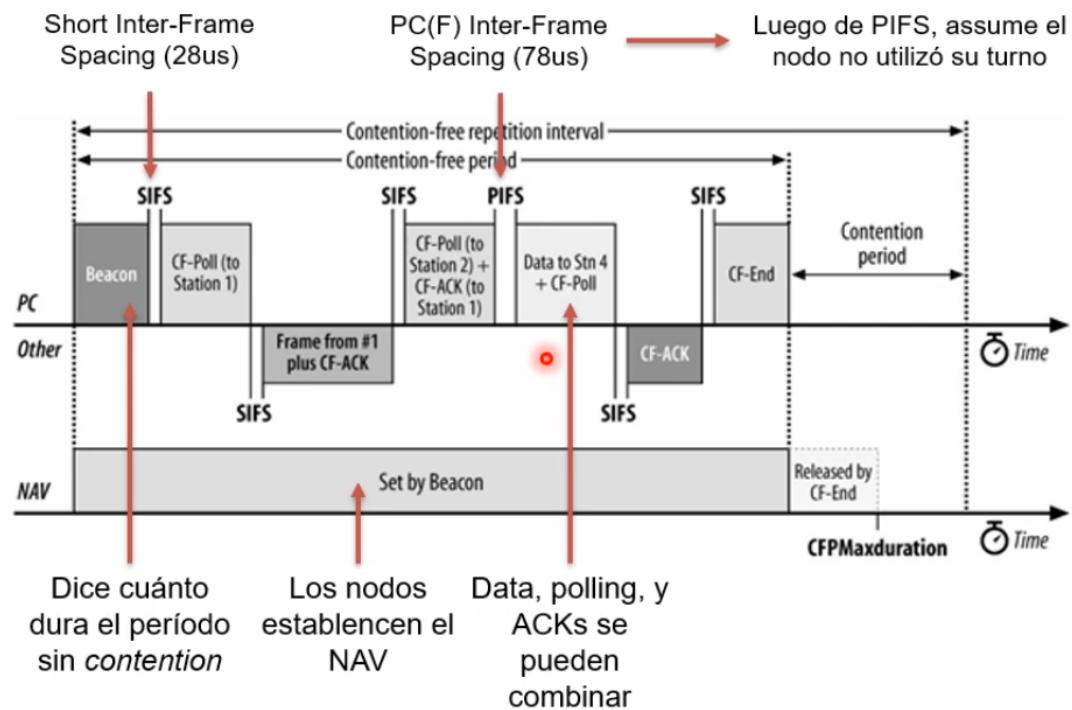
– **Período sin (*contention*) disputa** (PCF)

- Implementada en AP, quien coordina el acceso al medio
- Nodos transmiten sólo si lo pide el AP
- El AP tiene una lista de nodos “privilegiados”
- Los nodos se registran para estar en la lista

– **Período en (*contention*) disputa** (DCF)

- Implementado en los nodos
- Los nodos compiten por el medio

Si durante el periodo sin disputa no hubo ningun nodo que quisiera enviar datos, entonces se pasa al periodo con disputa.



Supongamos que un nodo no sabe PCF, pero se encuentra conectado a ese AP y con otros nodos que si entienden PCF. Como hace para no interrumpir esa conversación? Como un nodo que usa DCF debe primero esperar un tiempo DIFS antes de enviar su RTS, vemos que en ningun momento de la conversacion, en el contention free interval, hay un DIFS libre. Entonces los nodos que usen DCF no van a poder nunca enviar su RTS hasta que termine ese tiempo libre de contencion. Ya que siempre escuchara el canal como ocupado. Debe esperar al tiempo de disputa.

- **Beacon:** el AP demarca el inicio de la trama (i.e., baliza)
 - Contiene información de cuánto esperar para el próximo
 - Ese es el tiempo de un NAV, dentro del cual ocurren diálogos dentro del PCF
- **Poll:** el AP pide a la estación que transmite (i.e., sondeo)
 - Cuando esa estación termina de transmitir, termina su turno y el derecho a transmitir pasa a la siguiente estación
 - Ni el orden ni frecuencia son especificados en el estandard
- **SIFS (Short Inter Frame Space) de 28 us**
 - Intervalo entre tramas en un mismo dialogo (ACK, CTS, datos)
- **PIFS (Point Coordination IFS) de 78 us**
 - Intervalo entre tramas asumido por el AP (PCF)
- **DIFS (Distributed IFS) de 128 us**
 - Intervalo entre tramas asumido por nodos (DCF)

Beacon, es el mismo para asociacion pasiva.

