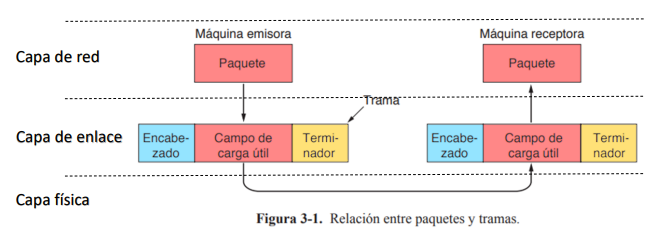
# **La capa de enlace**

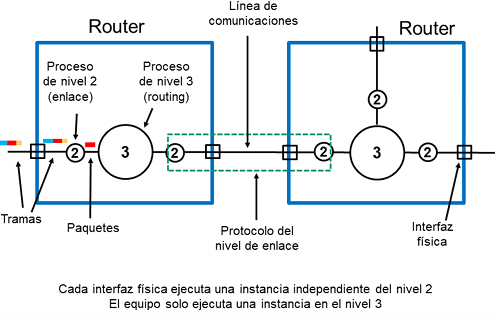
## **Funciones de la capa de enlace**

* Provee el control de la capa física
* Detecta y/o corrige errores de transmisión
* Regula el flujo de datos: que un emisor rápido no sature a un receptor lento, para eso puedo agregar un bit que representa receive not ready
* Entramar

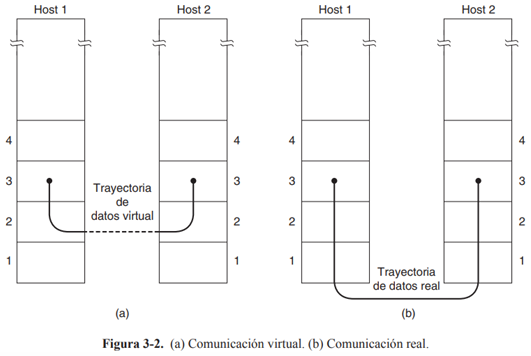
### **Relación entre los paquetes y las tramas**



### **La capa de enlace en un router**



### **La capa de enlace en el contexto del modelo de capas**



### **Servicios de la capa de enlace**

* Servicios no orientado a la conexión sin confirmación de recepción  
  Origen envía tramas sin que el destino confirme recepción.
* Servicio no orientado a la conexión con confirmación de recepción  
  Se confirma la recepción de cada trama
* Servicio orientado a la conexión con confirmación de recepción.  
  Se establece la conexión antes de transmitir datos y se confirma la recepción.

### **Funciones de capa de enlace**

* Obligatorias:
  + Identificar tramas (agrupación de bits que se intercambia a nivel de enlace)
  + Detección de errores
* Opcionales:
  + Control de flujo
  + Corrección de errores

### **Tipo de transmisión**

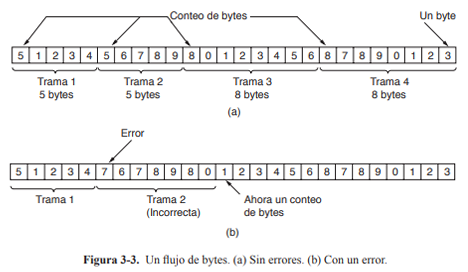
* Síncrona: la trama se envía sin separación entre los bytes. Cuando no hay nada que enviar el emisor envía una secuencia determinada de forma ininterrumpidapara asegurar que no se pierde el sincronismo.
* Asíncrona: cada byte se envía de forma independiente. Cuando no hay datosque enviar la línea está en silencio.

### **Delimitación de tramas**

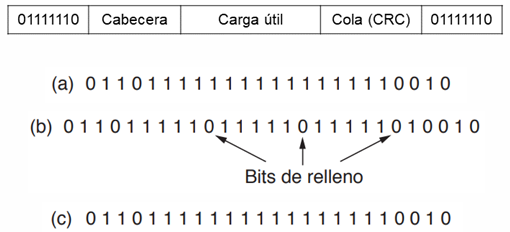
* La capa de enlace siempre agrupa los datos en entidades denominadas tramas.
* Es necesario generar las tramas para poder realizar el control de errores (detección y/o corrección)
* Problema que se plantea es cómo determinamos la frontera de una trama con la siguiente.

### **Tecnicas de identificacion de tramas**

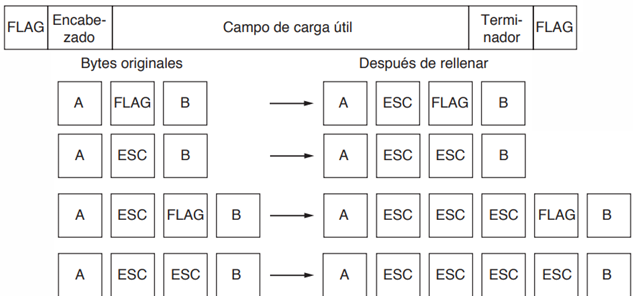
#### **Contador de caracteres**

primer campo que indique cuál es la longitud total de la trama.  


#### **Secuencia de bits indicadora de inicio y final (HDLC) Utiliza bits de relleno**

normalmente 01111110; si en los datos aparecen cinco bits seguidos a 1 se intercala automáticamente un 0  


#### **Caracteres de inicio y final con caracteres de relleno**

Seria lo mismo pero en byte  


#### **Violaciones de código de la capa física**

Seria mandando un código que en la codificación no existe, es decir una violación. No esta tan bien porque estaría metiéndome en el trabajo de la capa de fisica

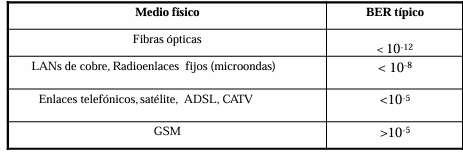
* Utilizar un atajo desde la capa física.
* Codificación de bits como señales incluye a menudo redundancia para ayudar al receptor.
* Esta redundancia significa que algunas señales no ocurrirán en los datos regulares. Por ejemplo, en el código de línea 4B/5B se asignan 4 bits de datos a 5 bits de señal para asegurar suficientes transiciones de bits.
* Podemos usar algunas señales reservadas para indicar el inicio y el fin de las tramas.

### **Control del flujo**

* Necesario para no 'agobiar' al receptor.
* Se realiza normalmente a nivel de transporte, también a veces a nivel de enlace.
* Utiliza mecanismos de retroalimentación (el receptor advierte al emisor). Por tanto:
  + Requiere un canal semi-duplex o full-duplex
  + No se utiliza en emisiones multicast/broadcast
  + Suele ir unido a la corrección de errores
  + No debe limitar la eficiencia del canal.

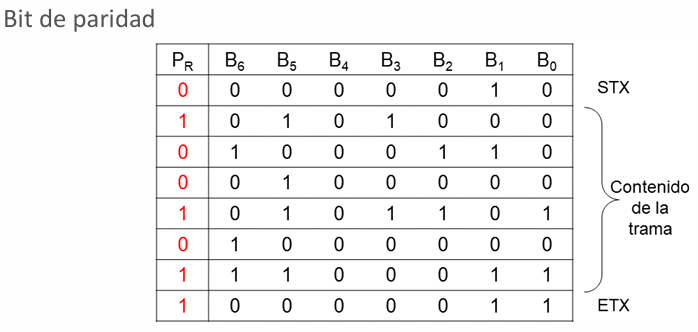
### **Tasa de errores (BER)**

* La tasa de errores de un medio de transmisión se mide por la BER (BitError Rate) que se define como:  
  BER = bits erróneos / bits transmitidos
* Un BER de 10-6 significa que hay un bit erróneo por cada millón de bits transmitidos



### **Control de errores**

* Los códigos pueden ser:
  + Detectores de errores: p. ej. Bit de paridad, Checksum, CRC (Cyclic Redundancy Check)
  + Correctores de errores: p. ej. Hamming, RS (Reed-Solomon). Un RS con 10% de overhead puede mejorar el BER en 10-4 (p. ej. de 10-5 a 10-9)
  + Los códigos detectores tienen menos overhead, pues necesitan incorporar menos redundancia.



## **Protocolos de parada/espera**

Supuestos:

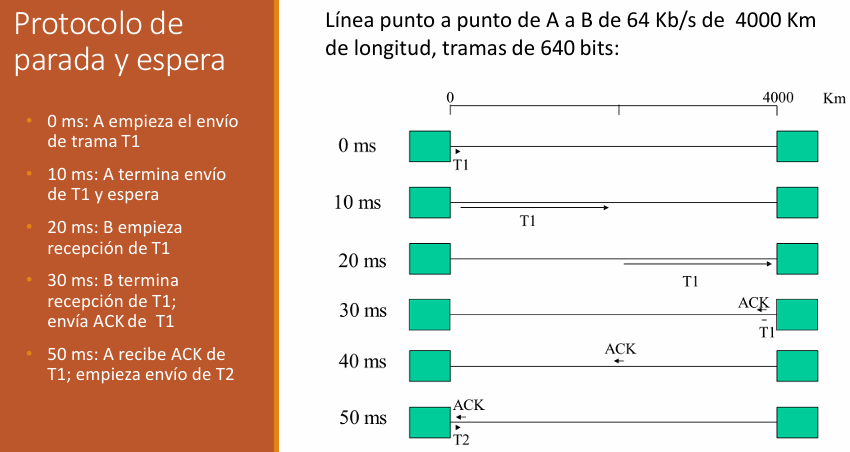
* Canal libre de errores
* Tramas siempre llegan a destino

Evitar que el emisor sature a receptor

Solución?

Proporcionar retroalimentación al emisor

* ACK
* Receptor envía al receptor una pequeña trama que autoriza al emisor a enviar la próxima trama



Eficiencia 10/50=30%

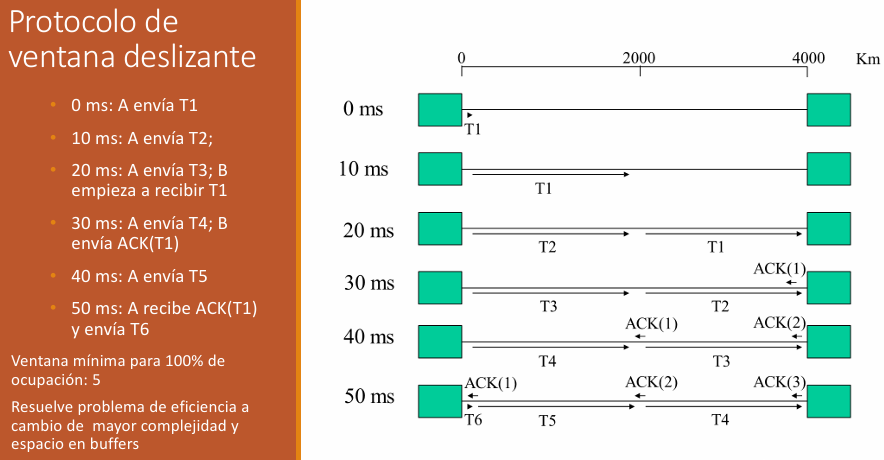
Para mejorarlo tendría que mandar una trama detrás de la otra

### **Protocolo parada y espera para un canal con ruido**

* Situación normal: canal de comunicaciones que comete errores
* Tramas pueden llegar dañadas o perderse por completo
* Variación del protocolo anterior: agregar temporizador
  + Emisor envía la trama
  + Receptor envía una trama de confirmación si los datos llegan correctamente
  + Si el temporizador expira, emisor envía trama nuevamente
* Problema: Qué pasa si se pierde el ACK?
  + Implementamos números de secuencia

## **Protocolos con ventana deslizante**

* Canal full-dúplex: utilizar el mismo enlace en ambas direcciones
* El receptor envía un paquete junto con la confirmación de recepción de la trama anterior.
* Retardar temporalmente las confirmaciones de recepción para que puedan viajar en la siguiente trama
  + Mejor aprovechamiento del ancho de banda del canal
* ¿Cuánto tiempo demorar el envío?
* En cualquier instante el emisor mantiene en buffer un conjunto de Nº secuencia en la ventana emisora.
* Del mismo modo el receptor mantiene una ventana receptora de tramas que tiene permitido aceptar





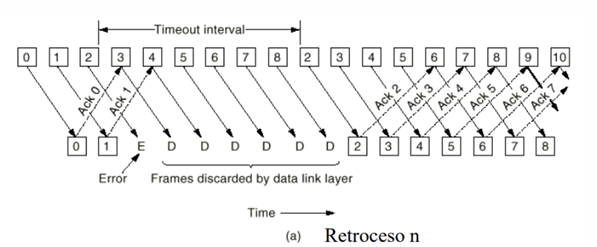
### **Tamaño de ventana**

* La ventana mínima para 100% de ocupación es la que ‘llena el hilo’ de datos en ambos sentidos, mas uno:
  + : tamaño de ventana - es decir cuanto buffer tengo que tener
  + : tiempo de propagación – tiempo de viaje
  + : velocidad de la línea - bps
  + : tamaño de trama
  + Ej.: τ=20ms, v = 64 Kb/s, t = 640 bits →W = 5

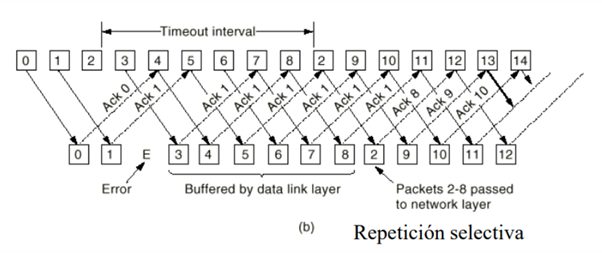
### **Puede ser**

* **Retroceso n:** no se acepta una trama hasta haber recibido las anteriores
* **Repetición selectiva:** se admite cualquier trama en el rango esperado y se pide solo la que falta.
* Repetición selectiva es más complejo pero más eficiente, y requiere más espacio en buffers en el receptor.
* Tamaño de ventana
  + **Retroceso n**: Número de secuencia – 1
  + **Repetición selectiva:** Número de secuencia/2

#### **Protocolo de ventana deslizante: Retroceso N**



#### **Protocolo de ventana deslizante: Repetición selectiva**



## **Protocolos de nivel de enlace: HDLC, PPP**

El protocolo es una definición de como se va a hacer cierto trabajo en una capa, los estándares agrupan varios protocolos

Orientado a la conexión y confiable (creo)

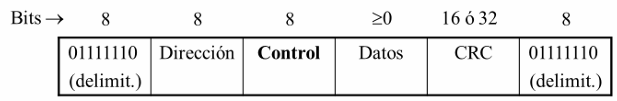
Orientado al bit

### **Familia de protocolos HDLC (High level Data Link Control)**

* HDLC es un estándar ISO. Deriva del SDLC desarrollado por IBM en 1972
* Es un protocolo de ventana deslizante muy completo
* Prácticamente todos los protocolos de enlace actuales son subsets de HDLC:
  + PPP: Internet
  + LAP-B: X.25
  + LAP-F: Frame Relay
  + LLC (IEEE 802.2): redes locales

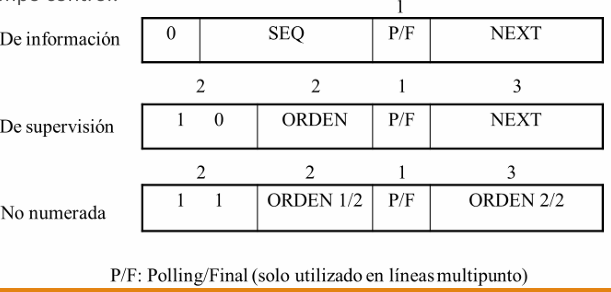
#### **HDLC: formato de trama**

* Se utiliza relleno de bits
* El campo dirección siempre vale 11111111 (dirección broadcast) salvo en líneas multipunto.
* El campo control es el que realiza todas las tareas propias del protocolo
* El CRC es normalmente de 16 bits, pero puede ser de 32

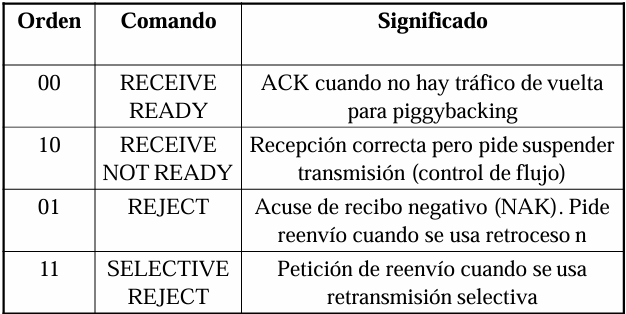


#### **HDLC: tipos de tramas**

Las tramas HDLC pueden ser de tres tipos según el valor de los primeros bits del campo control:



#### **Comandos en tramasde supervisión HDLC**



#### **Elaboración de tramas HDLC**

En el emisor:

1. Concatenar campos dirección, control y datos
2. Calcular el CRC de la cadena resultante
3. Realizar el relleno de bits poniendo un bit a cero siempre que en la cadena a enviar aparezcan cinco unos seguidos
4. Añadir a la trama los delimitadores de inicio y final (01111110). Si se envían dos tramas seguidas el delimitador de final de una sirve como inicio de la siguiente

El receptor procede de manera inversa (4,3,2,1)

## **PPP - Point to Point Protocol**

RFC1663

No es orientado a la conexión y no es confiable

Orientado al byte

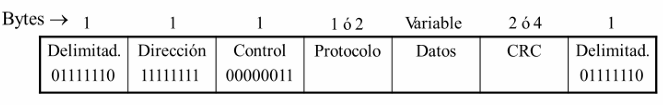
* El protocolo de enlace ’característico’ de Internet es el PPP, que se utiliza en:
  + Líneas dedicadas punto a punto
  + Conexiones RTC analógicas o digitales(RDSI)
  + Conexiones de alta velocidad sobre enlaces SONET/SDH
* Puede funcionar de forma síncrona o asíncrona (puerto COM de un PC)
* Es multiprotocolo, una comunicación soporta simultáneamente varios protocolos a nivel de red.

### **PPP – Características**

* Un método de entramado que delinea sin ambigüedades el final de una trama y el inicio de l siguiente.
* Un protocolo de control de enlace para activar líneas, probarlas, negociar opciones y desactivarlas ordenadamente cuando ya no son necesarias. Este protocolo se llama LCP
* Un mecanismo para negociar opciones de capa de red con independencia del protocolo de red usado. El método consiste en tener un NCP (Protocolo de control de Red) distinto para cada protocolo de capa de red soportado

### **PPP – Formato de la trama**

* La trama siempre tiene un número entero de bytes
* El campo dirección no se utiliza, siempre vale 11111111
* El campo control casi siempre vale 00000011, que especifica trama no numerada (funcionamiento sin ACK).
* Generalmente en el inicio se negocia omitir los campos dirección y control (compresión de cabeceras)



### **PPP – Componentes**

* LCP (Link Control Protocol): negocia parámetros del nivel de enlace en el inicio de la conexión, Ej.:
  + Supresión de campos dirección y control
  + Uso de protocolos fiables (con ACK)
* NCP (Network Control Protocol): negocia parámetros del nivel de red:
  + Protocolos soportados (IP,IPX, OSI, CLNP,XNS)
  + Asignación dinámica de dirección IP.
* CHAP (Challenge Handshake Authentication Protocol): realiza tarea de autentificación deusuario

# **La subcapa de control de acceso al medio**

Recordemos que las redes pueden ser:

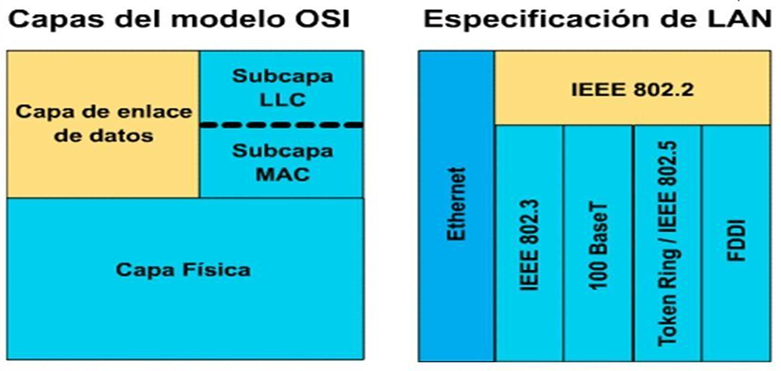
* **Redes Punto a Punto:** conexión directa entre dos nodos de una red
* **Redes que utilizan canales de difusión:** utilizan un mismo canal para transmitir información.

## **La capa de enlace de datos**

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

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

## **Comparando OSI e IEEE 802.3**



## **La subcapa LLC**

Fue creada con el propósito de proporcionar a las capas superiores (capa de red) una interfaz independiente de la tecnología empleada en la capa de enlace de datos y en la capa física

## **La subcapa MAC**

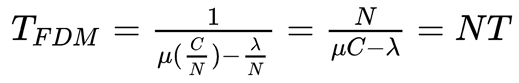
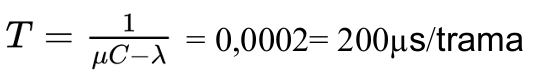
* Los protocolos usados para determinar quien sigue en un canal multiacceso pertenecen a una SubCapa de la Capa de enlace llamada MAC (Control de Acceso al Medio)
* Se encarga de la topología lógica de la red y del método de acceso a ésta.
* Cada tecnología de red tiene una subcapa MAC diferente.
* En la subcapa MAC residen las direcciones MAC
* Siempre que hay un medio compartido, es necesario definir las reglas de juego que regulen el acceso al canal.
* Esto es lo que denominamos protocolo de control de acceso al medio (Media Access Control)
* Ejemplos de redes que utilizan subcapa MAC:
  + Redes vía satélite
  + Redes CATV
  + Redes Wifi
  + Redes PLC
  + Redes FTTH

## **El problema de asignación de canales**

* **Asignación estática de canal**
  + Dividir la capacidad mediante esquemas de multiplexión vistos (FDM, TDM)
  + Tiene sentido, cuando existe un número pequeño y constante, N, de usuarios y cada uno tiene suficientes datos para mantener ocupado el canal
  + Existe desperdicio potencial del ancho de banda cuando algunos usuarios no transmiten o transmiten por ráfagas
* **Asignación dinámica de canal**
  + Puede hacer mejor uso del ancho de banda

## **Asignación estática de canales**

(nosotros nos vamos a basar en la asignación dinámica)

* **Eficiencia**, como el tiempo promedio de retardo T con λ tramas/segundo y 1/µ longitud de la trama (bits/trama)
  + Un solo canal con velocidad de datos C bps  
    
  + El canal con velocidad de datos C bps se divide en N subcanales  
      
    El retardo promedio al usar el canal compartido es N veces peor que si todas las tramas irían por una cola central
* **Ejemplo:** λ=5000 tramas/segundo, 1/µ=10.000 bits/trama, C=100 Mbps  
  

## **Asignación dinámica de canales – 5 supuestos –**

1. **Tráfico independiente:** N estaciones independientes, después de generar una trama cada estación se bloquea hasta que su trama es transmitida. **Probabilidad** de Tx de trama λ ∆t. (λ = tasa de llegada de tramas nuevas)
2. **La suposición de canal único:** Solamente hay un canal para todas las estaciones y todas son equivalentes.
3. **La suposición de colisión:** Si dos estaciones transmiten simultáneamente hay colisión y las estaciones reconocen las colisiones. La trama colisionada debe transmitirse después. Son los únicos errores.
4. Hay mas probabilidad de colisiones en un tiempo continuo que en un tiempo ranurado
   1. **Tiempo continuo:** La transmisión puede iniciar en cualquier instante del tiempo, no hay reloj maestro
   2. **Tiempo Ranurado:** El tiempo se divide en ranuras de tiempo o slots, la transmisión se inicia siempre al inicio del slot si la transmisión tuvo éxito
   3. **Detección de portadora:** Las estaciones no transmiten si el canal está ocupado y pueden detectar esta situación
   4. **Sin detección de portadora:** Las estaciones no pueden detectar el canal antes de intentar usarlo. Simplemente transmiten. Sólo después pueden determinar si la transmisión tuvo éxito.

## **Definiciones**

* **Colisión:**Cuando dos o más tramas son enviadas simultáneamente por el canal único
* **Contienda = Contención = Competencia:**Cuando múltiples sistemas deben tratar de ganar el canal común para su uso irrestricto
* **Persistencia:**La característica de un protocolo de iniciar la transmisión al encontrar el canal libre después de esperar por él

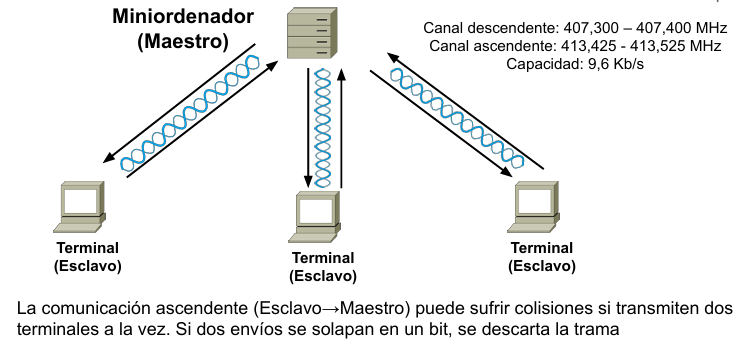
## **Protocolos de acceso múltiple**

* ALOHA
* Protocolos de Acceso Múltiple con Detección de Portadora (Carrier Sense Multiple Access Protocols)
* Protocolos sin Colisiones (Collision-Free Protocols)
* Protocolos de Contienda Limitada (Limited- Contention Protocols)
* Protocolos de Acceso Múltiple por División de Longitud de Onda
* Protocolos de LANs Inalámbricas

### **ALOHA**

#### **Antecedentes**

* 1969: Nace ARPANET
* 1970: Abramson crea red Alohanet (Additive Links Online Hawaii Area) en Univ. de Hawaii utilizando emisoras de radio taxis viejos
* Arquitectura maestro-esclavo (como los radio taxis)
* Dos canales:
  + Descendente (Maestro→Esclavo): un solo emisor
  + Ascendente (Esclavo→Maestro): compartido por 3 esclavos

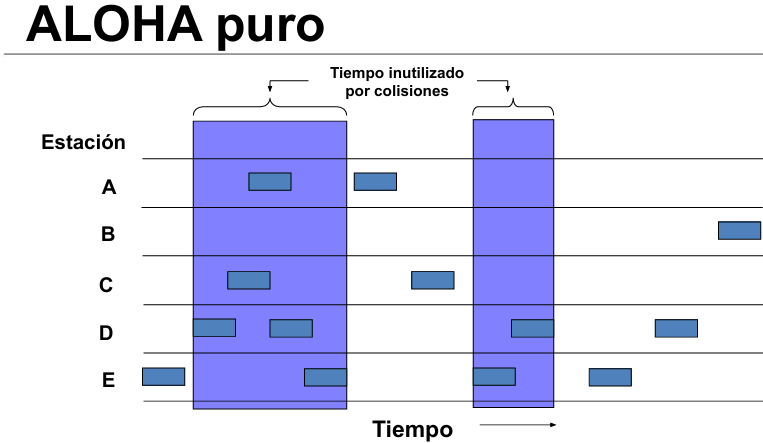


#### **ALOHA puro**

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

No requiere sincronización global del tiempo.

Eficiencia es: 



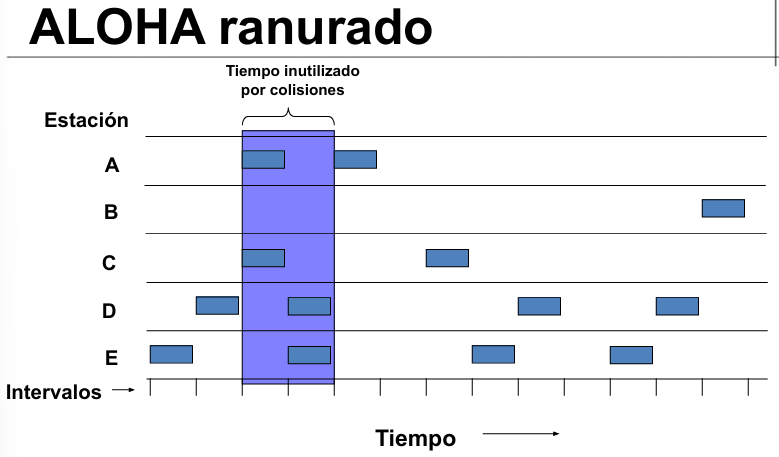
#### **ALOHA ranurado**

En ALOHA ranurado (slotted), el tiempo es discreto, cada ventana de tiempo corresponde al tiempo de una trama.

Las estaciones únicamente inician la transmisión al principio de la ventana de tiempo

El tiempo vulnerable se reduce a la mitad

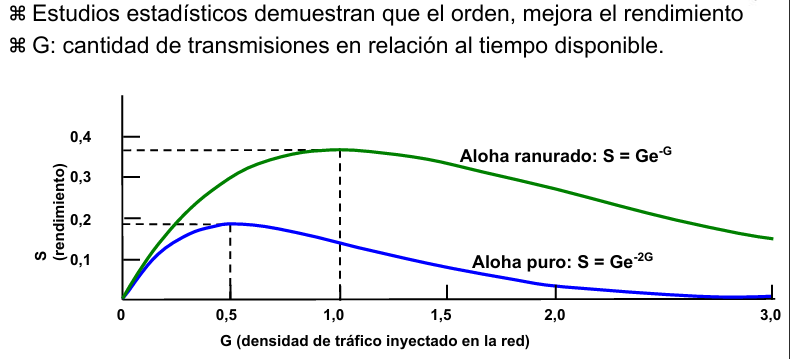
La eficiencia es: 



#### **Eficiencia de ALOHA puro**

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

#### **Rendimiento de ALOHA puro y ranurado**



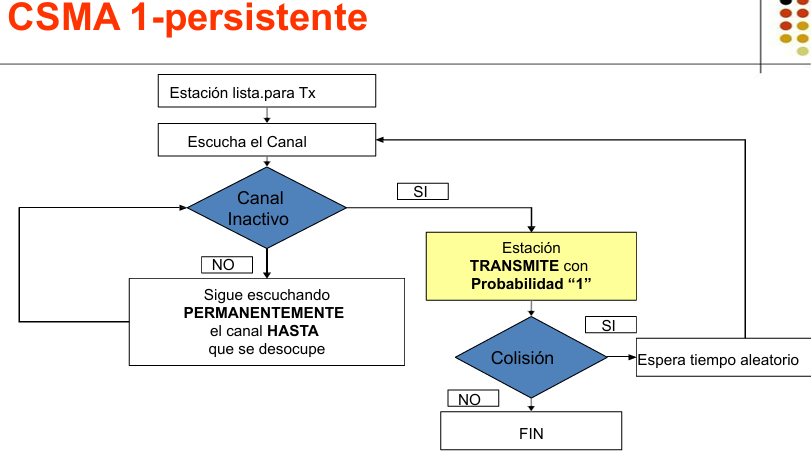
### **Protocolos de Acceso Múltiple con Detección de Portadora (Carrier Sense Multiple Access Protocols)**

Los protocolos en los que las estaciones ESCUCHAN LA PORTADORA (es decir, una transmisión) y actúan de acuerdo con ello se llaman PROTOCOLOS DE DETECCIÓN DE PORTADORA

* CSMA = (Acceso Múltiple con Detección de Portadora)
* CSMA 1-persistente
* CSMA no persistente
* CSMA p-persistente
* CSMA/CD

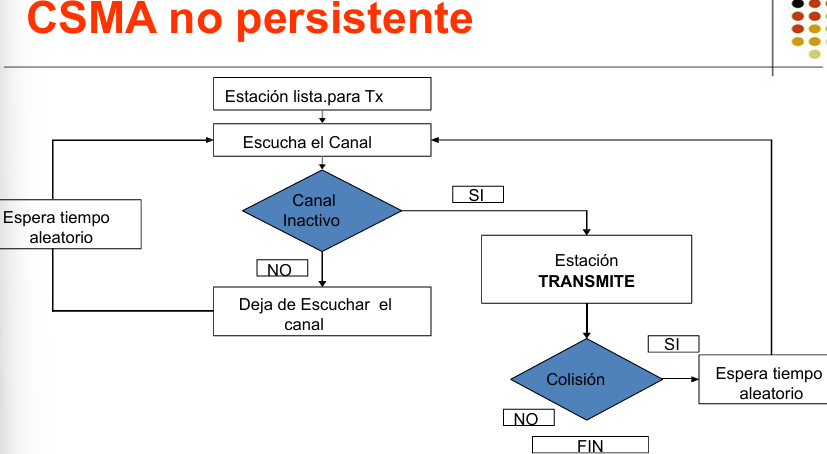
#### **CSMA 1-persistente**

El protocolo inicia la transmisión con una probabilidad 1 cuando encuentra el canal libre después de esperar



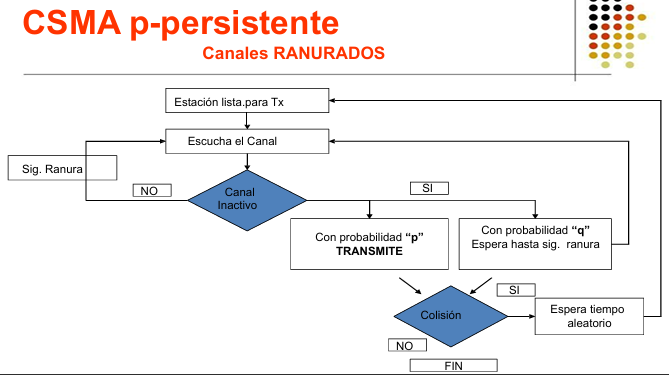
#### **CSMA no persistente**

Antes de enviar, una estación escucha el canal. Si nadie más está transmitiendo, la estación comienza a hacerlo. Sin embargo, si el canal ya está en uso, la estación no lo escucha de manera continua a fin de tomarlo de inmediato al detectar el final de la transmisión previa. En cambio, espera un periodo aleatorio y repite el algoritmo.

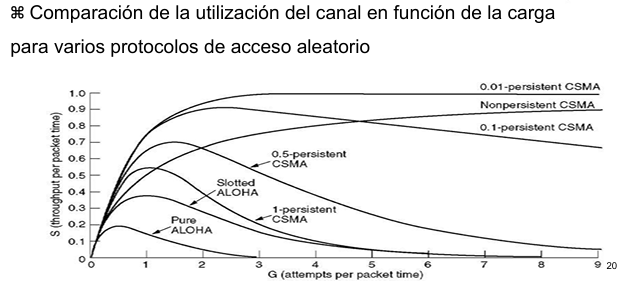


#### **CSMA p-persistente**

En canales de tiempo discreto, el protocolo inicia la transmisión con una probabilidad “p” cuando encuentra el canal libre/inactivo después de esperar o la difiere con probabilidad q = (1-p)



#### **CSMA persistente y no persistente**



#### **CSMA/CD: CSMA con detección de colisiones**

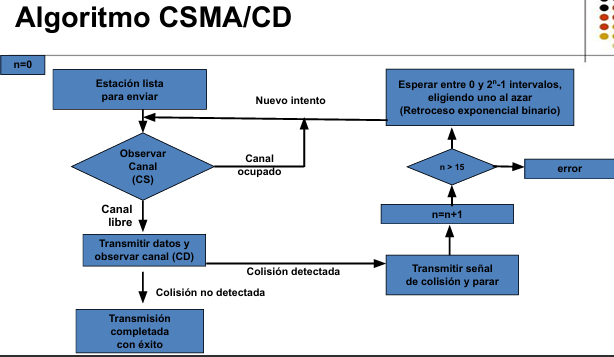
El protocolo CSMA/CD consiste en:

1. Oír antes de empezar a hablar (CS, Carrier Sense)
2. Hablar solo cuando los demás callan
3. Si mientras hablamos oímos que otro habla nos callamos (CD, Collision Detect)

Dicho en pocas palabras el protocolo CSMA/CD consiste en ser educado y prudente

* Al detectar la colisión, todas las estaciones que están transmitiendo se callan, esperan un tiempo aleatorio y luego lo intentan de nuevo
* Usado en Ethernet
* CSMA/CD puede estar en uno de tres estados: contienda, transmisión, o en reposo
* Solo puede haber colisiones en el tiempo de contienda

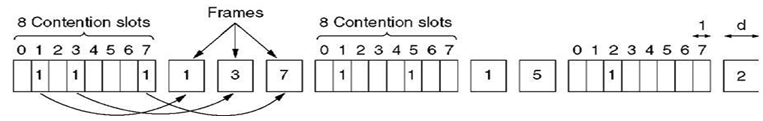




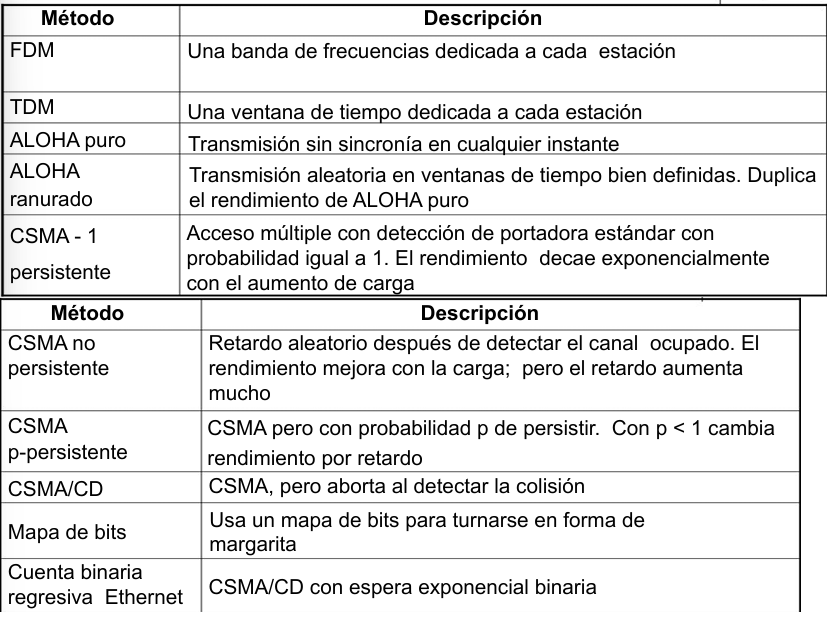
* El tiempo que se tarda en detectar la colisión es como máximo el doble del tiempo de propagación de un extremo a otro del cable
* Se modela el intervalo de contienda como un ALOHA ranurado (slotted ) con un ancho 2τ
* La colisión debe poder detectarse; por ello la codificación de la señal debe permitir la detección (no puede haber bits de 0 voltios)
* El sistema es inherentemente half-duplex

### **Protocolos sin Colisiones (Collision-Free Protocols)**

#### **Mapa de bits**

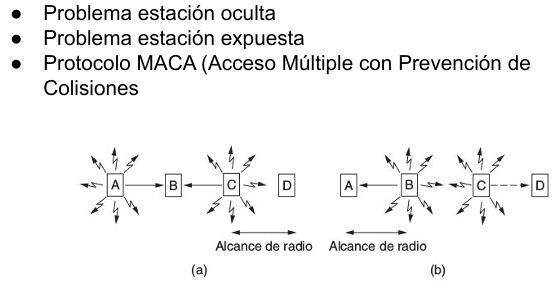
* El protocolo básico de mapa de bits (bit-map) es un protocolo de reservación  
    
  d = bits (cantidad de datos) N = Estaciones
* Eficiencia a baja carga = d/(N+d)
* Eficiencia a carga alta por canal = Nd/(Nd+N) = d/(d+1)
* No escala bien para miles de estaciones

### **Resumen**



### **Protocolos de LANs Inalámbricas**

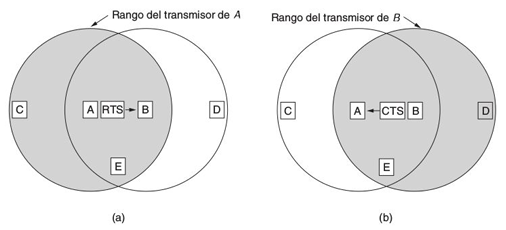
* Sistema de computadoras portátiles que se comunican por ondas de radio
* Inconvenientes
  + Sistemas inalámbricos no pueden detectar la colisión en el momento en que ocurre
  + Rango de radio limitado
* Enfoque CSMA? Escuchar si hay otras transmisiones y sólo transmitir si nadie lo está haciendo
  + Problema estación oculta
  + Problema estación expuesta



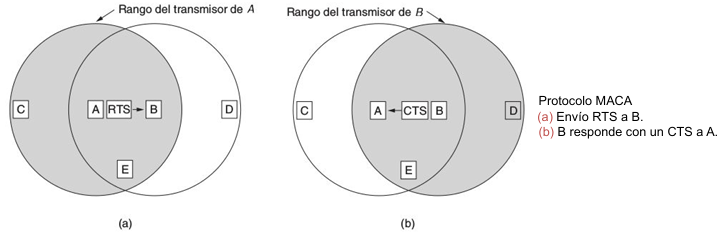
En (a): Si C ve que el canal esta libre porque A no esta en su radio, enviara el mensaje a B y se producirá colision en B. Esto es estación oculta.

En (b): Problema estación expuesta. C se queda callado suponiendo que D…

* Emisor estimula al receptor para enviar una trama corta, de manera que las estaciones cercanas detecten esta transmisión y eviten transmitir durante la siguiente trama (trama grande)



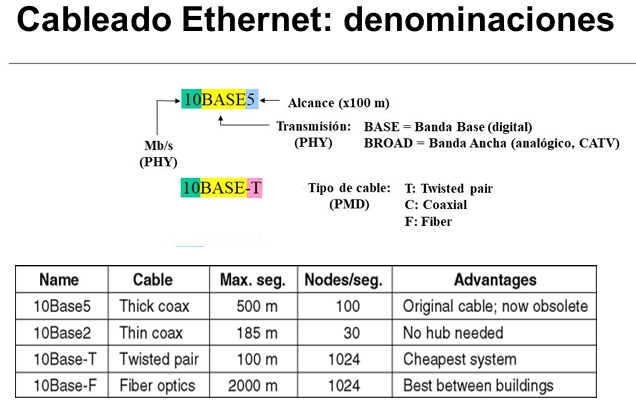
* A comienza enviando una trama RTS (Solicitud de Envío, Request To Send) a B
* Esta trama corta contiene la longitud de la trama de datos que seguirá después.
* B contesta con una trama CTS (Libre para Envío, Clear To Send )
* La trama CTS contiene la longitud de los datos (que copia de la trama RTS)
* Al recibir la trama CTS, A comienza a transmitir.



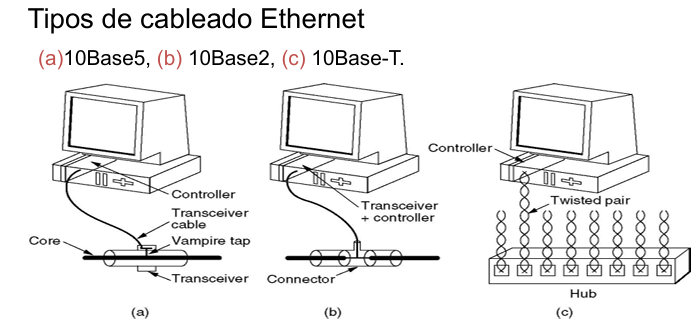
## **Ethernet**

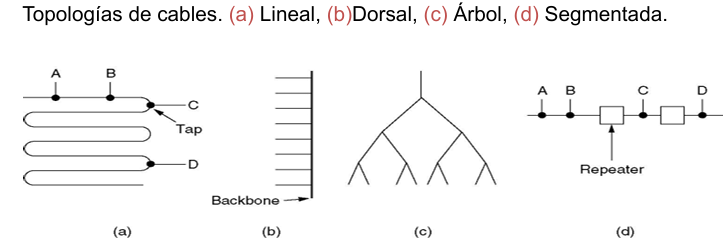
No orientado a la conexión y no confiable porque no manda ack. Si el transmisor no detecta que hubo una colision

### **Cableado ethernet**

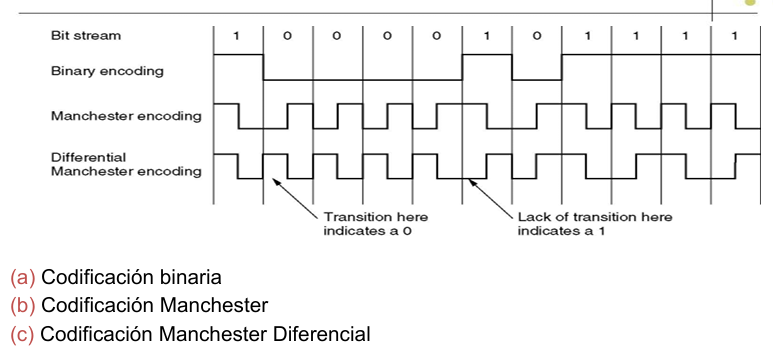


El HUB trabaja solo en capa física, a diferencia del switch que lee hasta capa de enlace





### **Codificacion manchester**



### **Protocolo de la subcapa MAC Ethernet**

Formatos de trama

1. DEC-Intel-Xerox: DIX Ethernet
2. IEEE 802.3



El preambulo solo sirve para sincronizar el receptor. Los bytes del preámbulo no son parte de la trama, no suma al tamaño de la trama

Pregunta de parcial: Cuantos bytes tiene de mínimo una trama? No le sumo el preambulo.

Length: tamaño de datos

Pad: si tengo 0 datos transmitidos, el pad es 46, si tengo 46 bytes transmitidos, el pad es 0. Por lo que el pad es relleno para que la cantidad de datos llegue a 64.

El tamaño mínimo de trama es 64 bytes. Nunca debe tener menos que eso.

Pregunta de parcial: Por que quiero tener 64 bytes mínimo? Viene por el tiempo de contienda, es el tiempo en el que una estación toma el canal pero no esta segura de que no sabe que el canal es de el. 2tau, el tiempo que tarda en ir al receptor y volver. La regla dice, como estas en tiempo de contienda, debes sebir transmituendo y escuchando por colisiones, si después de 2t no hay colision. 2t es tiempo, 64bytes es datos. Modular 64bytes nos va a llevar un tiempo de 2tau

El 2tau tarda 51,2microsegundos porque la velocidad de ethernet es 10mbps

En el 10 base 5 la máxima distancia es 2500m, al calcular el tiempo de iida da 12,5 microsegundos de ida + 12,5 microsegundos de vuelta + 25microsegundos de repetidores da 50 microsegundos, de tiempo total. Para transmitir 500biys necesito 512 bits porque debe estar en base 2, a 10mbit/s me queda 51,2 microsegundos. Lo que da 64bytes

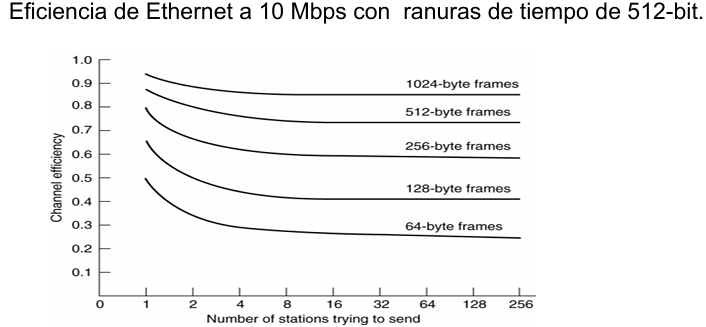
Para 100mbits, si hago lo mismo me da 5120bits o 640bytes. Para compensar y que siga dando 64bytes achico a 250m la distancia

Para 1gbps no puedo achicar la distancia a 25m y tampoco puedo transmitir 6400bytes. Lo que se hace es juntar varias tramas y mandar una ráfaga de tramas. No se juntan datos, sino que se juntan tramas.

Para 10gb solo se usa la técnica de trama, pero usa un concepto totalmente distinto ya que no tiene en cuenta que el canal sea compartido.

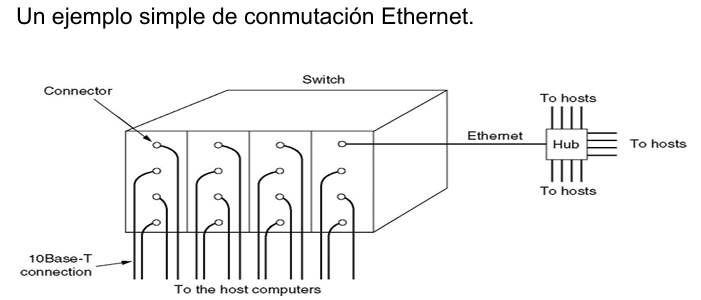


### **Rendimiento de ethernet**



### **Conmutacion ethernet**

Se llama switch porque conmuta tramas al nivel de ethernet



Lee la trama, en la capa de enlace lee el origen es a y el destino es b y hace una conexión dedicada entre los dos hosts. Por lo que evita celisiones. No evita todas las colisiones ya que puede haber cuando se quiere hacer dos conexiones con el mismo host.

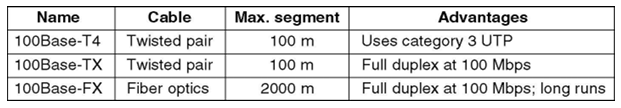
**Dominio de broadcasting:** son todos los switches que están conectados entre si. Una solución para dividir el dominio de broadcasting es subiendo a la capa 3. Es decir se mete un enrutador entre los dos. Lo malo de hacer esto es que cualquier dato debe pasar por la capa 3, por lo que incrementa el costo de tiempo. La mejor solución es usar una VLAN, ya que esta a nivel de capa 2.

**Dominio de colisiones:** donde colisionan dos paquetes. En un hub es el hub. En un switch, el dominio se divide en cada uno de los puertos. Con el switch se divide el dominio de colisiones

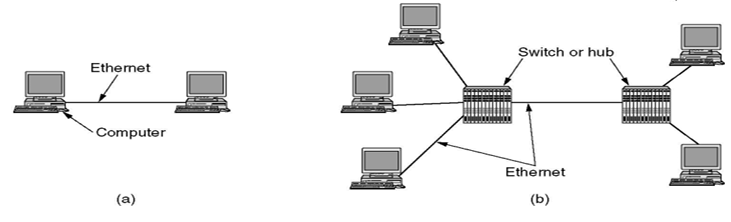
### **Fast Ethernet, gigabit ethernet**

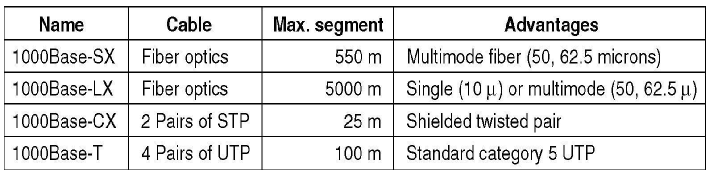
Es lo que puse más arriba, en fast se acorta distancia y en gigabit se mandan ráfagas. PARA ESTO LEER DEL LIBRO

### **Fast ethernet**

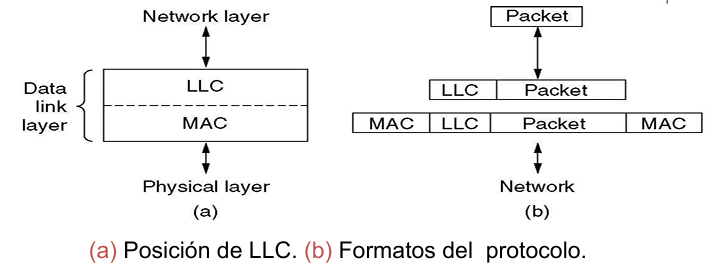


### **Gigabit Ethernet**

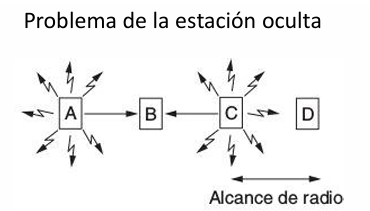




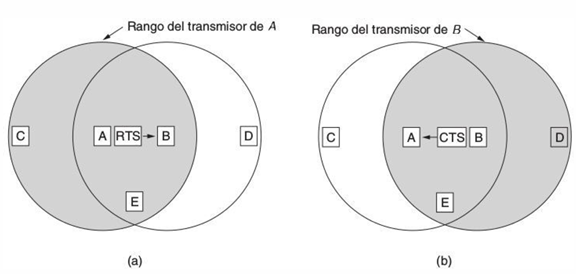
### **IEEE 802.2: Control lógico de enlace (LLC – Logical Link Control)**

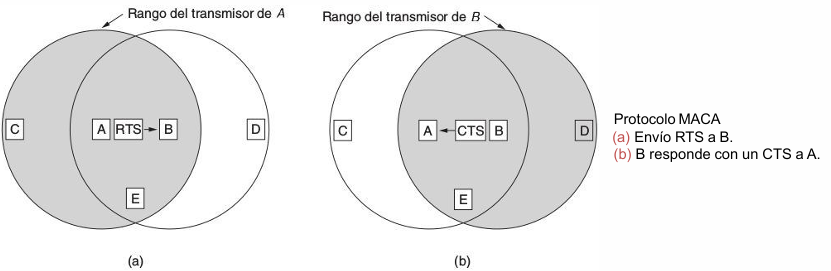


## **Protocolos para LANs inalámbricas**

* Sistema de computadoras portátiles que se comunican por ondas de radio
* Inconvenientes
  + Sistemas inalámbricos no pueden detectar la colisión en el momento en que ocurre
  + Rango de radio limitado
* Enfoque CSMA? Escuchar si hay otras transmisiones y sólo transmitir si nadie lo está haciendo
  + Problema estación oculta  
    
  + Problema estación expuesta  
    

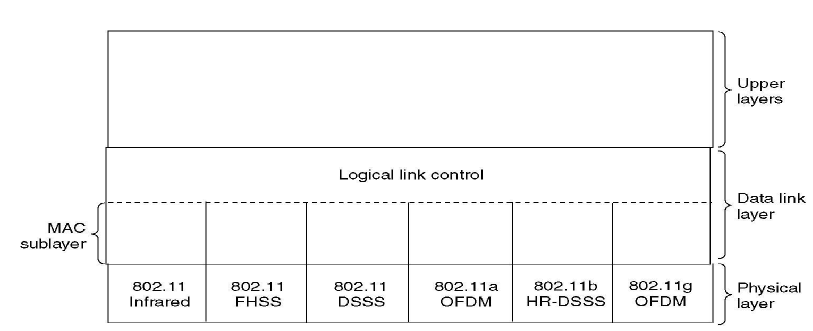
### **Protocolo MACA (Multiple Access with Collision Avoidance)**

* Emisor estimula al receptor para enviar una trama corta, de manera que las estaciones cercanas detecten esta transmisión y eviten transmitir durante la siguiente trama (trama grande)  
  
* A comienza enviando una trama RTS (Solicitud de Envío, Request To Send) a B
* Esta trama corta contiene la longitud de la trama de datos que seguirá después.
* B contesta con una trama CTS (Libre para Envío, Clear To Send)
* La trama CTS contiene la longitud de los datos (que copia de la trama RTS)
* Al recibir la trama CTS, A comienza a transmitir.



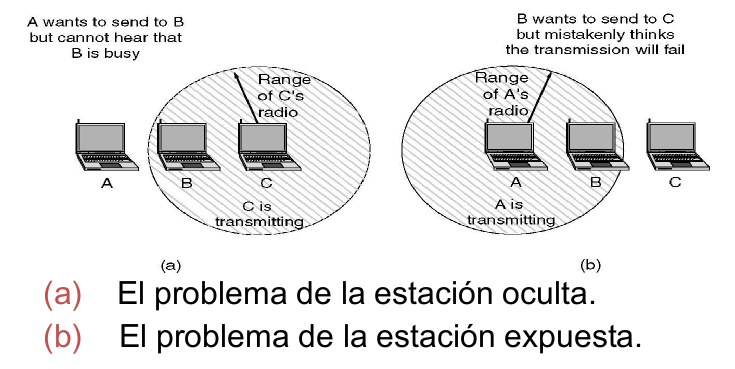
## **LANs inalámbricas**

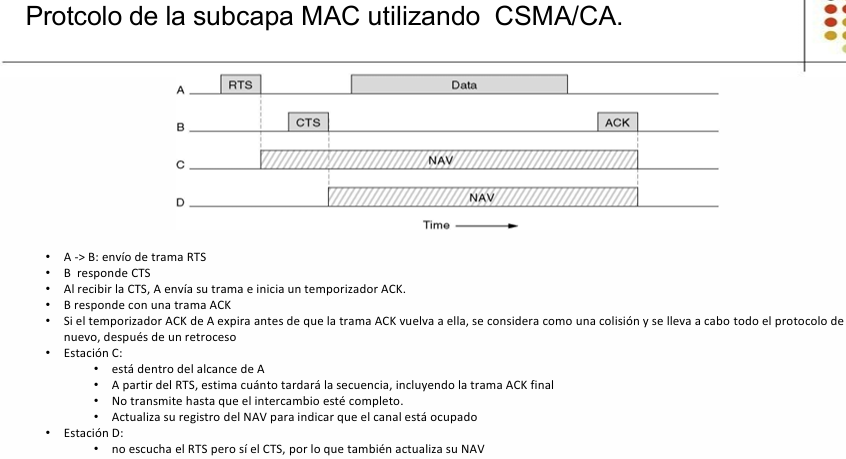
### **La pila de protocolos 802.11**

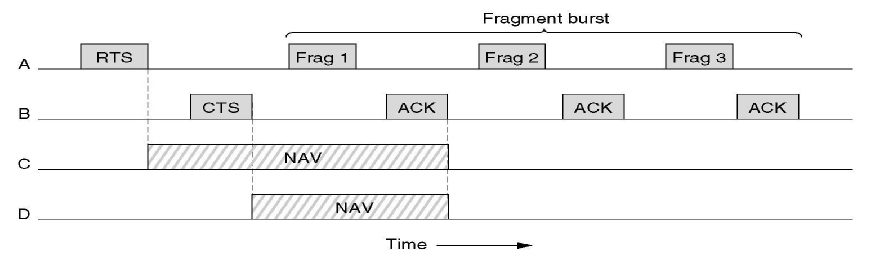


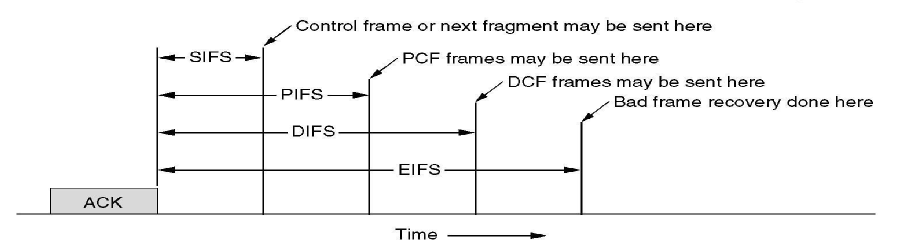
### **El protocolo de la subcapa MAC 802.11**

Problema de la estación oculta y problema de la estación expuesta:

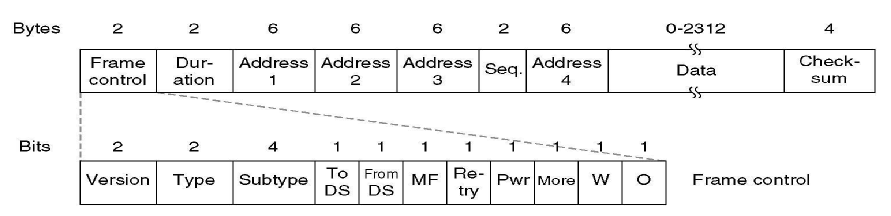


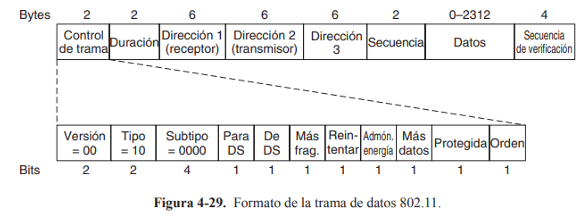






### **Estructura de la trama 802.11**





### **Servicios 802.11**

802.11 define los servicios que los clientes, los puntos de acceso y la red que los conecta deben proveer para poder ser una LAN inalámbrica que se apegue a dicho estándar. Estos servicios se dividen en varios grupos

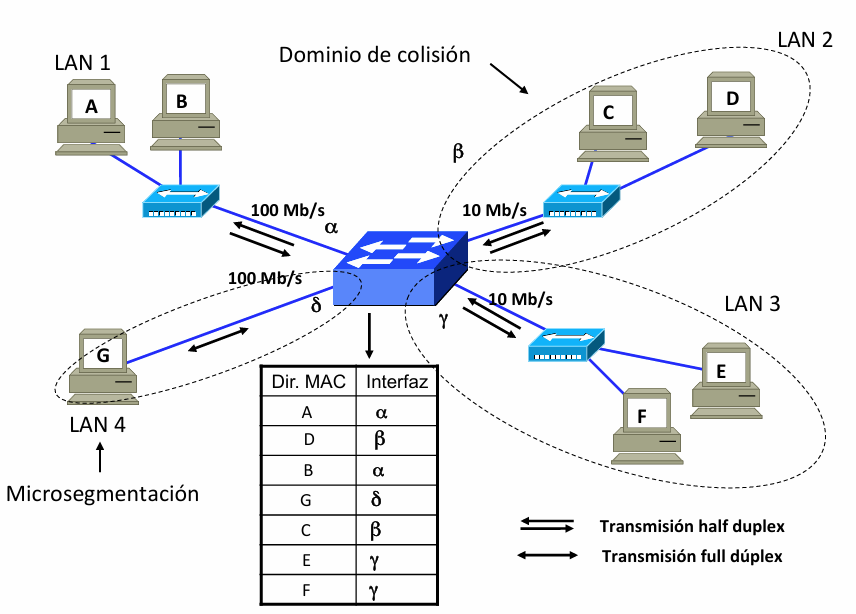
* **Distribución** **de** **servicios**
  + **Asociación:** Utilizado por estaciones móviles para conectarse ellas mismas a los AP
  + **Desasociación**: Utilizado por estaciones móviles para desconectarse con los AP
  + **Reasociación**: Estaciones móviles que cambian de un AP a otro en la misma LAN 802.11 extendida
  + **Distribución**: Una vez que las tramas llegan al AP, el servicio de distribución determina cómo encaminarlas.
  + **Integración**: Maneja cualquier traducción necesaria para enviar una trama fuera de la LAN 802.11
* **Servicios** **intracélulas**
  + **Autenticación**: Estaciones se autentican antes de poder enviar tramas por medio del AP. La autentificación se maneja en formas distintas dependiendo del esquema de seguridad elegido
  + **Desautenticación**
  + **Privacidad**: Un servicio de privacidad que administra los detalles del cifrado y el descifrado.
  + **Entrega** **de** **datos**: Permite a las estaciones transmitir y recibir datos mediante el uso de los protocolos estudiados

# **Conmutacion en capa de enlace**

## **Conmutador (switch)**

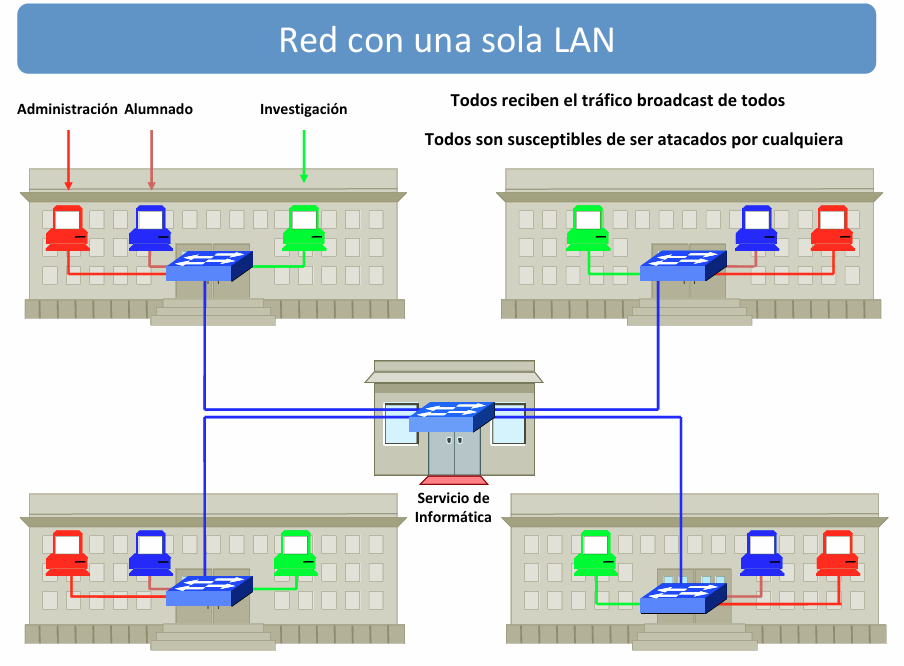
* Un conmutador es equivalente a un puente transparente.
* El conmutador ejecuta el algoritmo de conmutación a nivel de hardware, para ello utiliza tecnología ASICs.
* El conmutador es mucho más rápido que un puente, pudiendo funcionar a la velocidad nominal de la interfaz, simultáneamente por todas las interfaces.
* Hoy en día los puentes (hubs creo) se han dejado de utilizar.

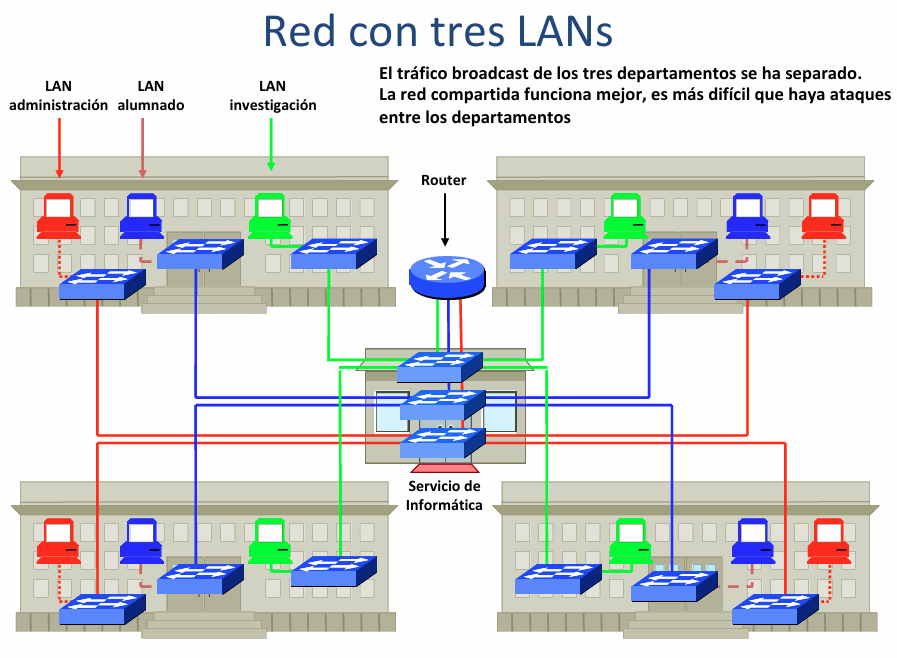
### **Conmutador con cuatro interfaces**



## **Tabla de direcciones**

* La tabla de direcciones MAC de los conmutadores LAN se denomina tabla CAM (Content Addressable Memory)
* Las entradas de las tabla CAM tienen un tiempo de vida limitado para permitir la movilidad
* La tabla CAM incluye las direcciones de la mayoría de las estaciones activas de todas las LANs conectadas directa o indirectamente al conmutador.
* La tabla CAM se mantiene en memoria dinámica y tienen un tamaño limitado (típico 1K-16K direcciones)



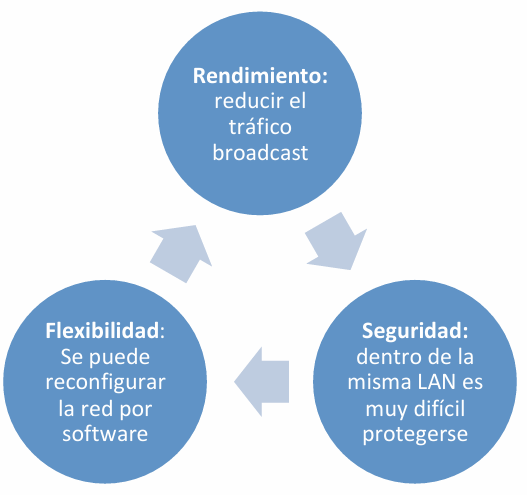


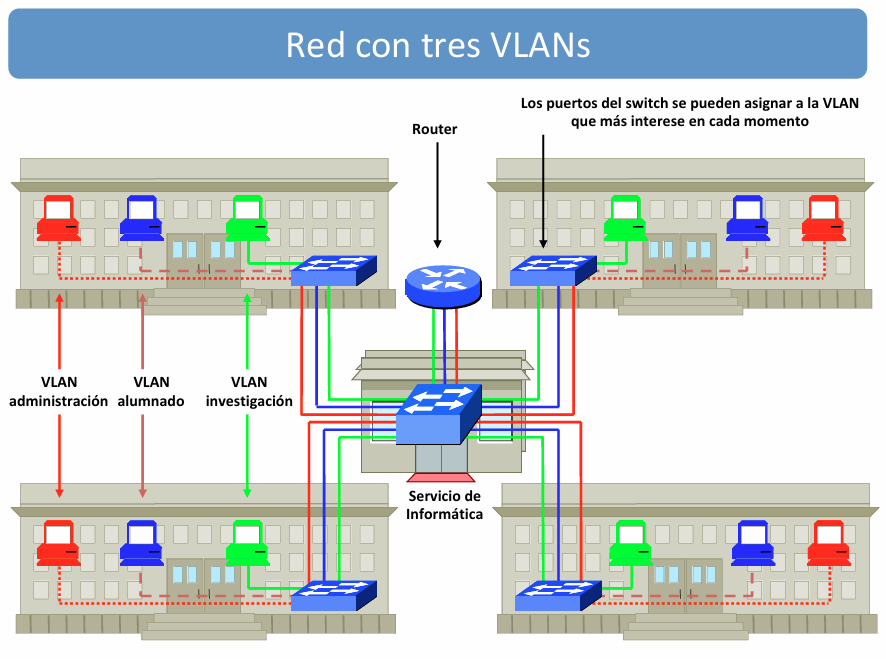
## **Problemas de implementar varias LANs**

* La separación en varias LANs obliga a tener múltiples conmutadores por edificio, incluso por rack.
* También es preciso tender cables independientes entre los conmutadores de cada LAN, entre racks y entre edificios
* La red es poco flexible, pues para cambiar un ordenador de LAN hay que ir físicamente al armario y cambiar la conexión a otro conmutador
* Se puede dar la circunstancia de que un conmutador tenga puertos sobrantes, mientras que otro está lleno y no tiene sitio para ampliaciones
* Para resolver todos estos problemas se inventaron las VLANs (Virtual LANs)

## **Redes locales virtuales o VLANs**

Equivalen a dividir o ‘partir’ lógicamente un conmutador en otros más pequeños.





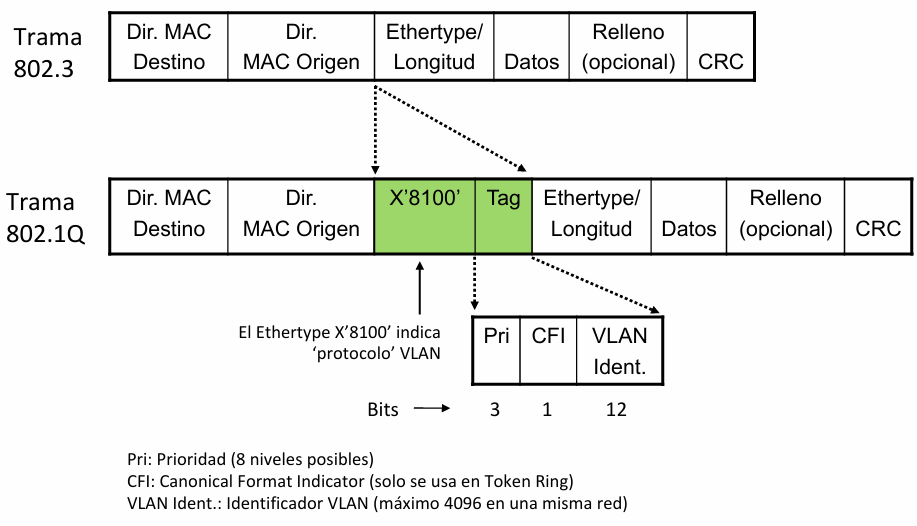
## **Interconexión de VLANs y enlaces ‘trunk’**

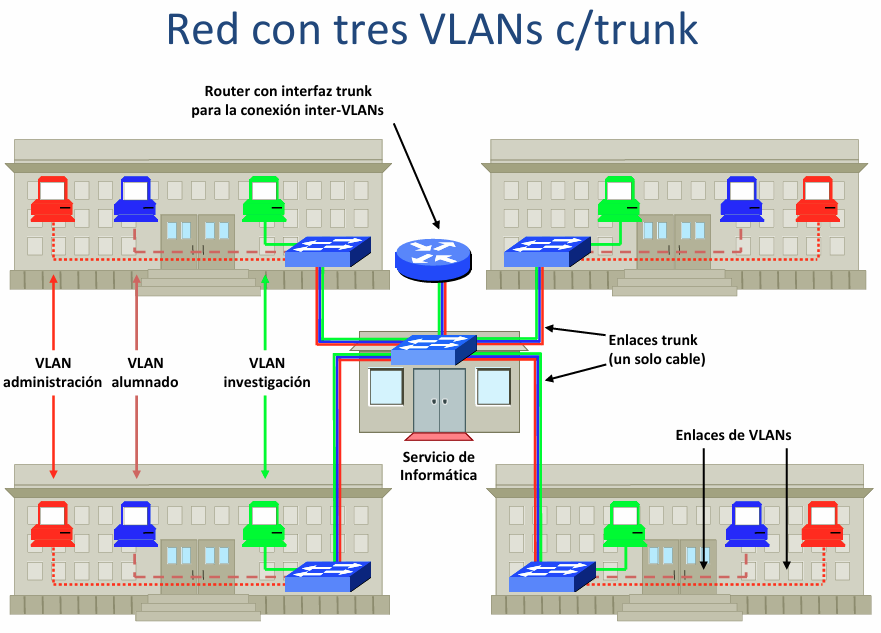
* Cuando se configuran VLANs en un conmutador los puertos asignados a cada VLAN se comportan como un conmutador independiente
* Si se interconectan dos conmutadores por un puerto solo se comunica la VLAN a las que estos puertos pertenecen
* Si tenemos varias VLANs y las queremos conectar todas hemos de establecer un enlace diferente para cada una. Esto puede consumir muchos puertos en los conmutadores y muchos cables en la red
* Para evitarlo se pueden configurar puertos que conectan todas las VLANs automáticamente; se les llama puertos ‘trunk’

## **Estándar IEEE 802.1Q**

* En un enlace ‘trunk’ viajan mezcladas tramas de diferentes VLANs. Para separarlas correctamente en destino hay que marcarlas antes de enviarlas por el enlace ‘trunk’
* Al principio cada fabricante estableció su sistema de marcado propietario. Esto impedía establecer enlaces trunk entre conmutadores de diferentes fabricantes
* En 1997 el IEEE aprobó 802.1Q, un estándar que establecía una forma de marcado de VLANs independiente de fabricante
* Para ello hubo que insertar un campo nuevo en la estructura de la trama Ethernet…. Todo un desafío.

### **Etiquetado de tramas según 802.1Q**





### **Asignacion de puerto a VLANs**

Hay básicamente tres mecanismos de asignación de puertos de switch a VLANs:

* **Estático, por configuración:** se especifica en la configuración a que VLAN pertenece cada puerto
* **Dinámico, por dirección MAC:** el switch asigna el puerto a la VLAN correspondiente de acuerdo con una asignación MAC-VLAN previamente almacenada en una base de datos
* **Dinámico, por autentificación usuario/ 802.1x):** password (protocolo el switch, después de validar al usuario, asigna el puerto a la VLAN que le corresponde, de acuerdo con la información contenida en una base de datos que relaciona usuarios y VLANs

Los vlan determinan que divisiones las mac del puerto 1,2,3 no se pueden conectar con las 4,5,6 por ejemplo.

Consiste en dividir el switch en pedazos. Para conectar las vlan entre si agrego un enrutador en el switch principal.

Si tengo 10VLAN esto se vuelve insoportable ya que debo subir 10 cables al router. Esto se soluciono con switches propietarios de alguna empresa que mandan un solo cable. Luego de esto salió el estándar IEE802.1Q que define de que VLAN es la trama. Esto se llama trunk.

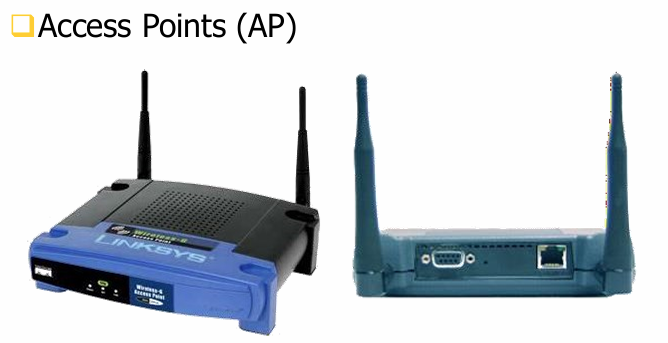
Con VLAN el dominio de broadcasting se limita a cada VLAN.

# **IEEE 802.11 Standard**

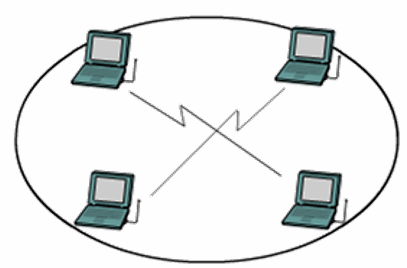
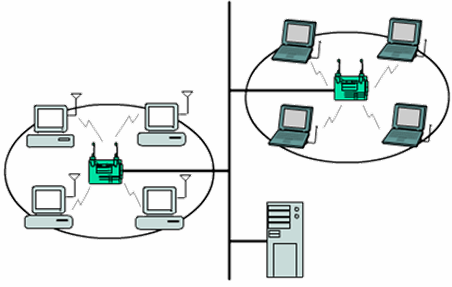
## **Comunicación Inalámbrica**

* **Características:** ondas electromagnéticas que no requieren un medio físico para su transmisión
* **Ventajas:**
  + Flexibilidad en la instalación y movimiento de los nodos
* **Desventajas**:
  + Seguridad
  + Interoperabilidad
  + Interferencia

## **Dispositivos**

## **Modos de Configuracion**

* Modo Ad hoc  
  
* Modo Infraestructura  
  

## **Normalizacion**

Antes de que existieran los estándares inalámbricos, los sistemas:

* Tenían bajas velocidades de datos,
* Eran incompatibiles
* Tenían elevados costos

La normalización proporciona todos los siguientes beneficios:

* Interoperabilidad entre los productos de múltiples fabricantes
* Desarrollo más rápido de productos
* Estabilidad
* Capacidad para actualizar
* Reducciones de costos

Es importante que todos los dispositivos sean compatibles al mismo estándar para asegurar la interoperabilidad.

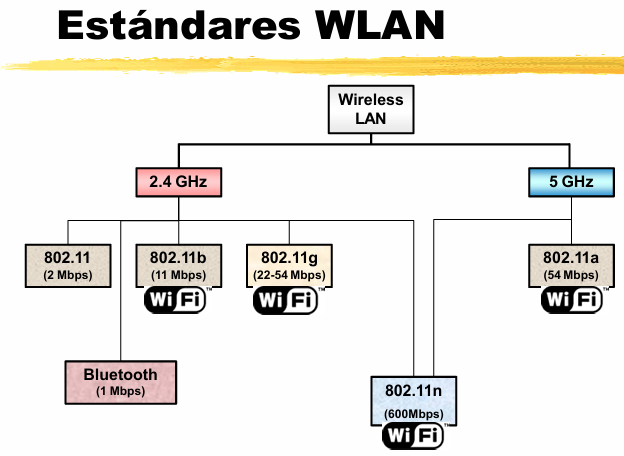
El cumplimiento con el estándar 802.11 actual puede crear una WLAN funcional, independiente del fabricante.

Los problemas de roaming, seguridad y capacidad de administración aún pueden presentar incompatibilidades

## **IEEE 802.11**

El término 802.11 se refiere a una familia de protocolos, incluyendo:

* 802.11
* 802.11b
* 802.11a
* 802.11g
* 802.11n



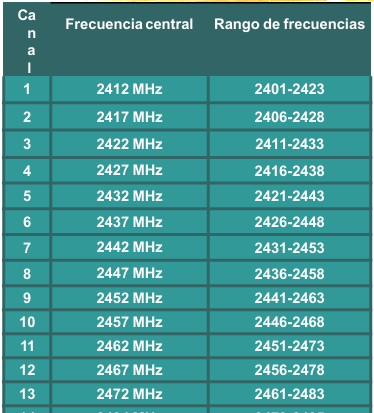
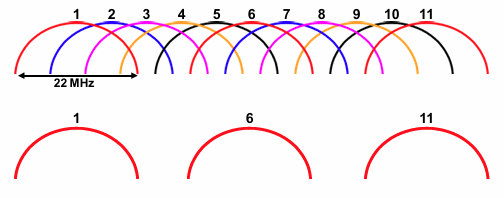
El estándar 802.11 define:

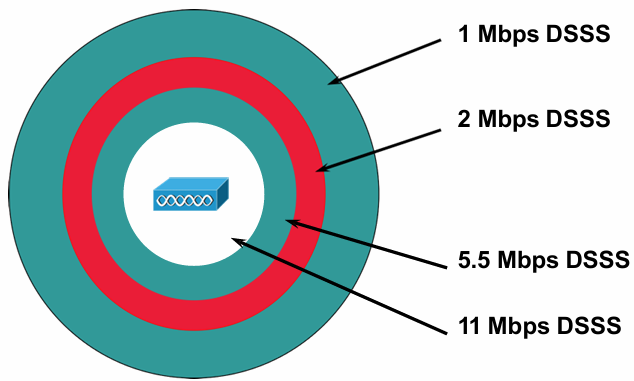
* MAC: Capa de enlace de datos Control de Acceso al Medio
* PHY: Capa Física (Frecuencias, señales, modulación, etc)
* Entrega tramas entre dispositivos pares que utilizan LLC en la capa de enlace de datos.

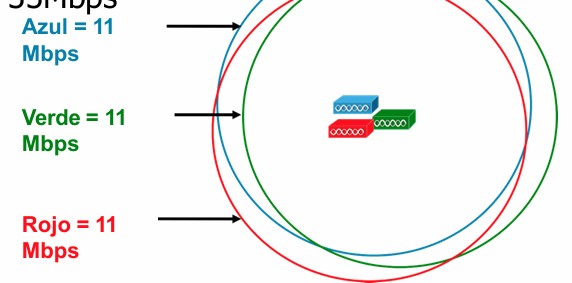
IEEE 802.11 ha ido evolucionando. Cada “enmienda” nueva define nuevas capacidades, anchos de banda y/o frecuencias  


## **IEEE 802.11b**

* Trabaja en el rango de frecuencias de 2401MHz a 2495MHz
* Divide el espectro en 14 canales.
* Cada canal tiene un ancho de 22MHz.
* En argentina se han homologado los primeros 11 canales
* Hay un solapamiento entre los canales
* La separación entre un canal y el siguiente es de 5MHz
* Cada canal se solapa con los tres canales inmediatamente anteriores y posteriores

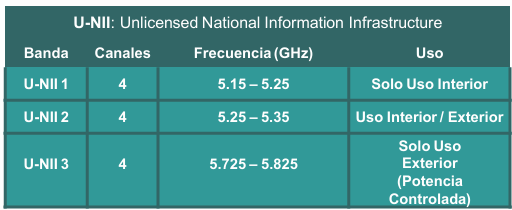
 

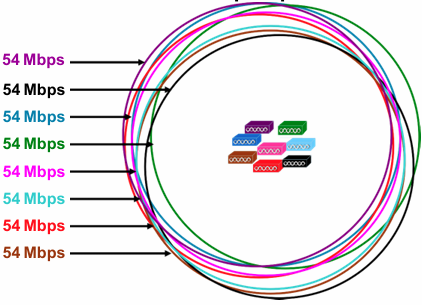


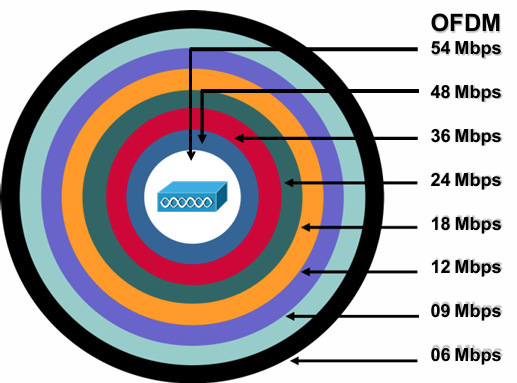
* Se pueden ubicar 3 dispositivos trabajando en canales no superpuestos: 33Mbps  
  

## **IEEE 802.11a**

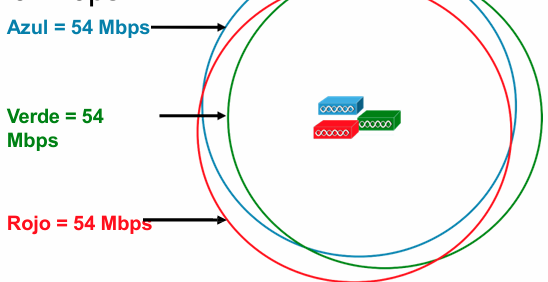
* Trabaja en el rango de frecuencias de 5GHz.
* Al usar una frecuencia superior tiene una cobertura menor
* No es compatible con 802.11b
* Define frecuencias para uso interior y para uso exterior

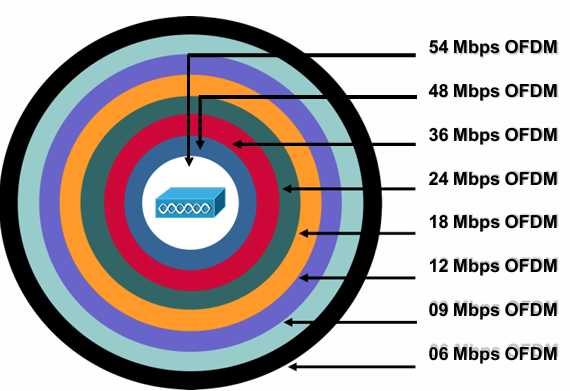
 

* Se pueden ubicar 8 dispositivos trabajando en canales no superpuestos: 432Mbps  
  

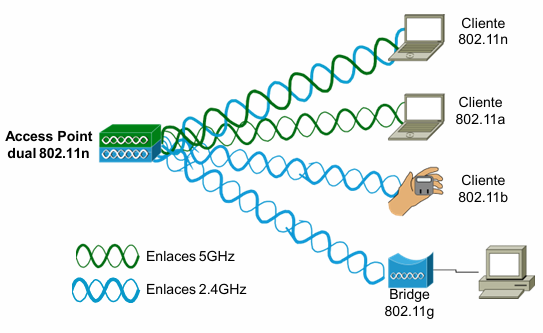


## **IEEE 802.11g**

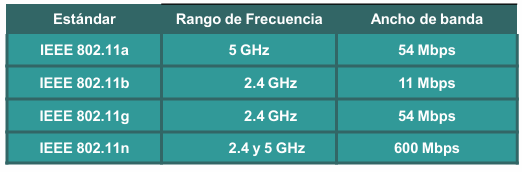
* Opera en el rango de frecuencias de 2.4GHz
* Ofrece un ancho de banda de 54Mbps
* Es compatible con 802.11b
* La existencia de equipamiento b reducirá su performance
* Tiene la misma división de canales que 802.11b
* Se pueden ubicar 3 dispositivos trabajando en canales no superpuestos: 162Mbps  
  



## **IEEE 802.11n**

* Última enmienda estandarizada
* Utiliza los dos rangos de frecuencia: 2.4 GHz y 5 Ghz
* Utiliza MIMO (Multiple-Input Multiple- Output)
* Puede alcanzar hasta 600Mbps
* IEEE 802.11n tiene una mayor cobertura
* Se aprovecha de los rebotes para amplificar y regenerar la señal.
* Es totalmente compatible con cualquiera de las especificaciones anteriores 802.11a/b/g  
  
* Existen productos que sólo operan en un rango de frecuencias (2,4GHz o 5GHz).

## **Comparacion estándares**



## **Metodo de acceso al medio (capa 2)**

802.11 define el método CSMA/CA: Carrier Sense, Multiple Access with Collission Avoidance

### **CSMA/CA**

* Debido a las particularidades que tiene la dispersión de la señal, no se puede implementar la detección de colisiones.
* Las colisiones deben ser eliminadas
* Se implementa una técnica para evitar que las estaciones colisionen entre sí

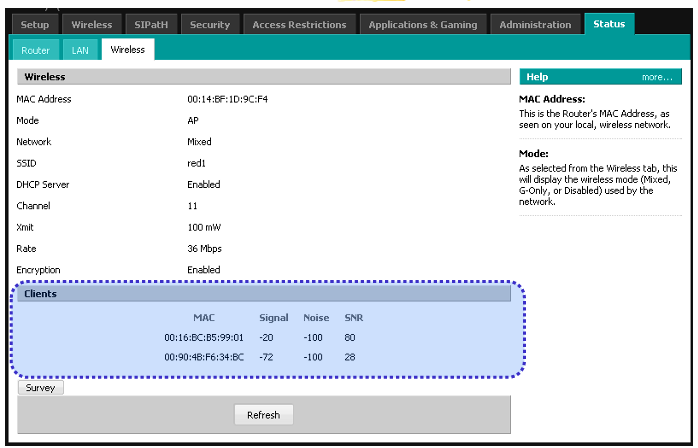


* Emisor A envía Request-to-Send (RTS)
* Receptor B envía Clear-to-Send (CTS)
  + Los nodos que escuchan CTS no pueden transmitir concurrentemente con A (rojo)
  + Nodos que escuchan RTS pero no escuchan CTS pueden transmitir (verde)
* A envía el frame de datos
* B anvía ACK
  + Los nodos que escuchan el ACK pueden transmitir
* Dos emisores pueden enviar RTS al mismo tiempo
* Ocurrirá una colisión
* No habrá CTS
* Los Emisores esperan por time-out, esperan un backoff timer y retransmiten

## **Asociacion, reasociacion y roaming**

### **Asociacion**

* Cuando una estación desea conectarse a un BSS debe realizar un proceso de sincronización de información con el Access Point a cargo
* Esta sincronización se denomina “Asociacion”



Existen dos métodos de asociación

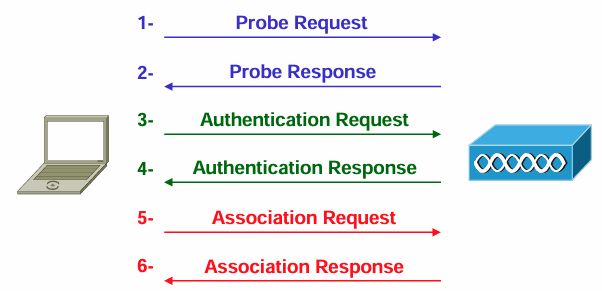
* Active scanning: El cliente busca activamente los APs
* Passive scanning: El cliente espera recibir avisos de los APs

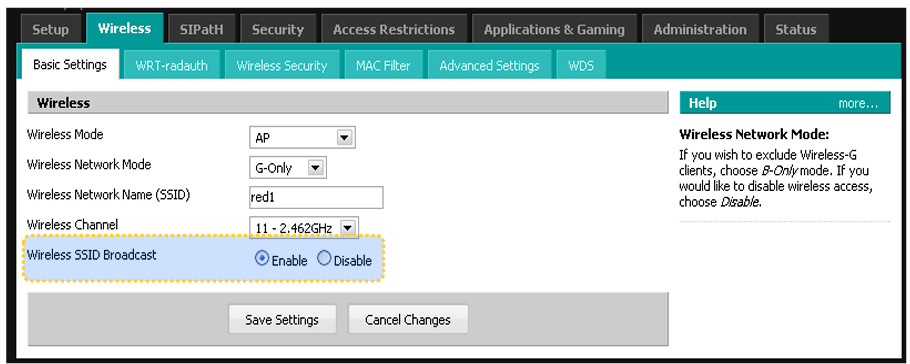
Al momento de realizarse la asociación, el AP y el cliente definen los parámetros de la conexión:

* Tipo de dispositivo (STA/AP)
* Tipo de Conjunto de Servicios (BSS/IBSS/ESS)
* SSID
* Canal utilizado
* Anchos de banda mínimos soportados
* Seguridad

#### **Active scanning**

* Los clientes envían tramas probe periódicamente
* Todos los APs que la escuchan responden con una trama probe response
* El nodo selecciona el mejor AP y le responde con un authentication request
* El AP lo reconoce con un authentication response





#### **Passive scanning**

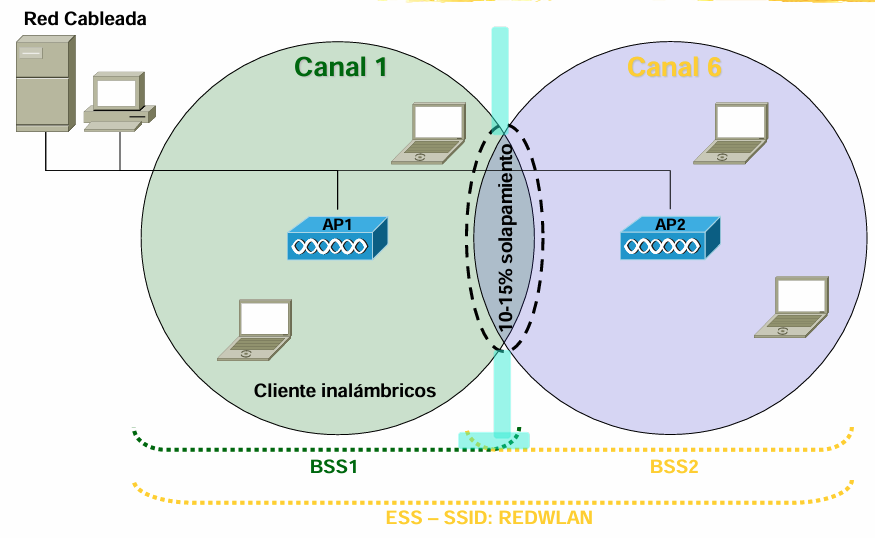
* Los APs se publican periódicamente enviando tramas beacon
* Los nodos se asocioan a un AP enviando un authentication request
* El AP los reconoce con un authentication response

### **Reasociación (creo que no importa)**

* Un cliente puede ir “saltando” entre diferentes APs que pertenecen al mismo ESS
* El cliente se reasocia de un AP a otro.

### **Roaming**

* Es la capacidad de que un cliente pueda moverse entre diferentes BSS sin pérdida de conectividad
* El estándar IEEE 802.11r permite una reasociación en menos de 50ms
* Sin soporte a IEEE 802.11r, dependiendo de su configuración, se puede llegar a realizar una reasociación por debajo de 1 segundo
* Recomendaciones para acelerar el tiempo:
  + Deben existir un solapamiento entre un 10 y un 15% en la zona de roaming
  + Deben trabajar en canales diferentes para evitar interferencias
  + Deben tener el mismo SSID y la misma configuración de seguridad
  + Cuanto menor es la seguridad, menor será el tiempo de reasociación



## **Performance**

* La performance real se encuentra muy por debajo del ancho de banda que provee el enlace físico.
* Diferentes factores afectan a la performance:
  + Método de acceso al medio
  + Topología
  + Convivencia de estándares
  + Solapamiento de canales

### **Metodo de acceso al medio**

* Se debe enviar un RTS y esperar a recibir un CTS
* Se debe esperar a recibir un ACK luego de transmitir
* Este tiempo perdido afecta el porcentaje de utilización del medio
* La performance máxima no será superior al 50% del ancho de banda del medio.