Control de acceso al medio

Tema 4

Alcaraz, S., Roig, P.J.

Fundamentos de Redes de Telecomunicación
Grado en Ingeniería de Tecnologías de la Telecomunicación

Area de Arquitectura y Tecnología de Computadores
Departamento de Física y Arquitectura de Computadores
Universidad Miguel Hernández

{salcaraz,proig}@umh.es

05/01/2025

Objetivos de aprendizaje

Después de abordar la unidad, el estudiante será capaz de:

Comprender el problema del acceso al medio compartido.
Entender los métodos de acceso aleatorio.
Explicar la existencia de colisiones en medios compartidos y su recuperación.
Explicar los métodos Aloha y Aloha ranurado.
Comprender los métodos CSMA, CSMA/CD y CSMA/CA.
Entender las diferencias entre métodos de acceso cableados e inalámbricos.
Explicar los métodos de acceso controlado
Distinguir entre métodos de acceso aleatorio y controlado
Razonar sobre el rendimiento de las diferentes estrategias de acceso al medio.
Conocer los orígenes y evolución de Ethernet.
Distinguir entre topologías bus y estrella.
Explicar el modelo de referencia IEEE 802.
Comprender la funcionalidad del puente.
Distinguir entre hub y switch.
Conocer las arquitecturas inalámbricas.
Distinguir entre los diferentes dispositivos de interconexión.

Control de acceso al medio

1. Introducción
2. Protocolos de acceso aleatorio
3. Protocolos de acceso controlado
4. Familia Ethernet
5. Redes inalámbricas
6. Dispositivos de interconexión

Control de acceso al medio

El problema del acceso al medio

Ejemplo:

- Clase: mucha gente reunida en una habitación.
- Medio de difusión: aire.

Protocolos/normas de cortesía:

"*Dar la oportunidad a alguien para que hable*"

"*No hablar mientras alguien te está hablando*"

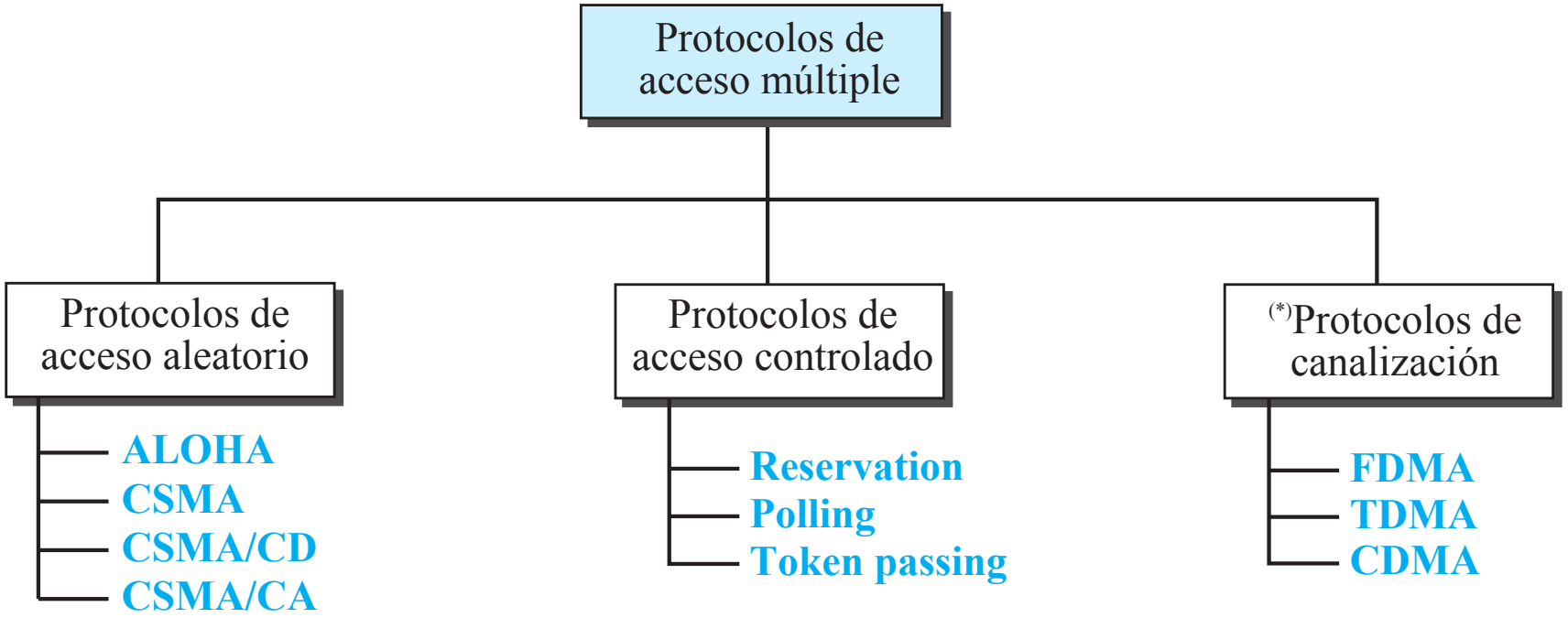
"*No monopolizar la conversación*"

"*Levantar la mano si tienes alguna cuestión*"

"*No interrumpir mientras alguien está hablando*"

"*No dormirte mientras alguien más está hablando*"

Protocolos de acceso al medio



(*) Contenido fuera del alcance de esta asignatura.

Control de acceso al medio

1. Introducción
2. ***Protocolos de acceso aleatorio***
3. Protocolos de acceso controlado
4. Familia Ethernet
5. Redes inalámbricas
6. Dispositivos de interconexión

Acceso aleatorio

Se denominan métodos de **acceso aleatorio** o **métodos de contención**.

No requiere coordinación: no hay ninguna estación, jerárquicamente superior, que tenga asignado el control.

Flexible: en cada instante, la estación que tiene datos para enviar utiliza un procedimiento definido en el protocolo para tomar la decisión de enviar o no. La decisión depende de que el medio esté libre u ocupado.

Buen rendimiento en entornos de carga baja.

Sin garantías de entrega.

Hay dos características que subrayan el término **aleatorio**:

- No hay planificación de tiempo para la transmisión de datos ⇒ las estaciones realizan una transmisión aleatoria (**acceso aleatorio**).
- No hay reglas que especifiquen el orden de participación en el envío ⇒ las estaciones compiten entre sí para acceder al medio (**métodos de contención**).

Si más de una estación intenta transmitir al mismo tiempo, se produce un **conflicto** o **colisión**, y todas las tramas involucradas son destruidas o modificadas.

Para evitar los conflictos, cada estación sigue un procedimiento que responde a las siguientes preguntas:

- *¿Cuándo puede acceder al medio?*
- *¿Qué puede hacer si el medio está ocupado?*
- *¿Cómo puede determinar si la transmisión ha sido realizada con éxito o fallo?*
- *¿Qué puede hacer si se ha producido conflicto en el acceso?*

Las ideas desarrolladas en Aloha han sido fundamentales en el desarrollo de protocolos, tanto cableados (Ethernet) como inalámbricos (WiFi).

Aloha

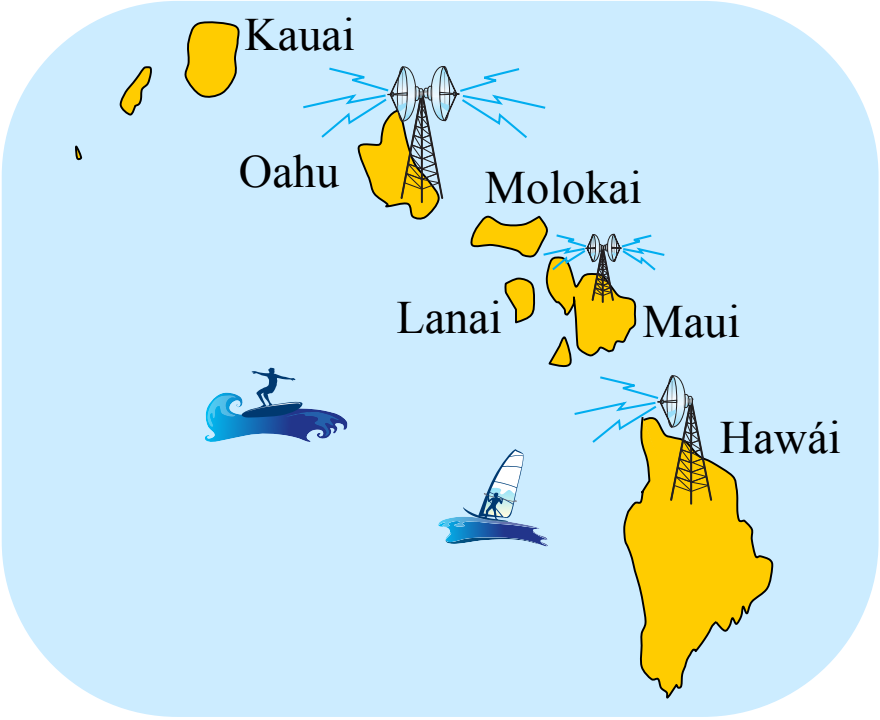
Aloha: origen histórico

Alohanet, diseñado por la Universidad de Hawái en 1970 como método de acceso a radio-enlaces, pero sus principios pueden ser aplicados a cualquier medio compartido.

El medio es compartido entre todas las estaciones.

Redes de radio paquetes.

"*Free for all*": si una estación tiene una trama para enviar, la envía.



Las técnicas de detección de colisiones y medios compartidos desarrollados en Alohanet se aplicaron en la Ethernet original.

Aloha: descripción del protocolo

Los nodos transmiten sobre un **canal compartido**.

Cuando dos transmisiones se solapan, **colisionan**.

Los receptores chequean el FCS y dirección destino.

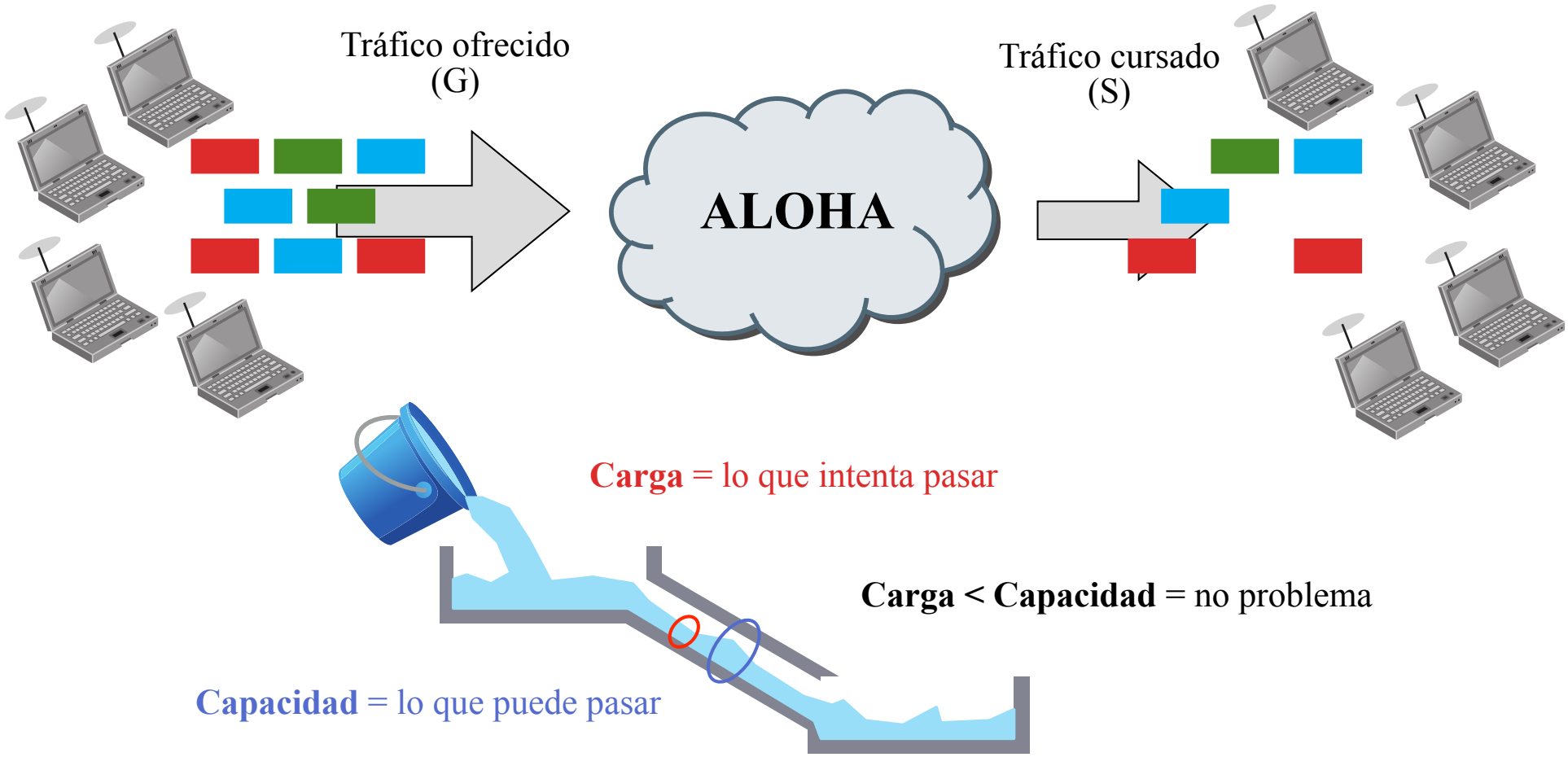
El nodo destino **confirma** las tramas correctas que recibe.

Cuando un nodo no recibe una confirmación (ACK), en un determinado **timeout**, supone que la trama ha colisionado.

Cuando una trama colisiona, el nodo transmisor planifica la retransmisión después de un **retardo aleatorio**.

Si no recibe ACK, re-envía la trama un número limitado de veces, y entonces, desiste.

Rendimiento en métodos de acceso aleatorio



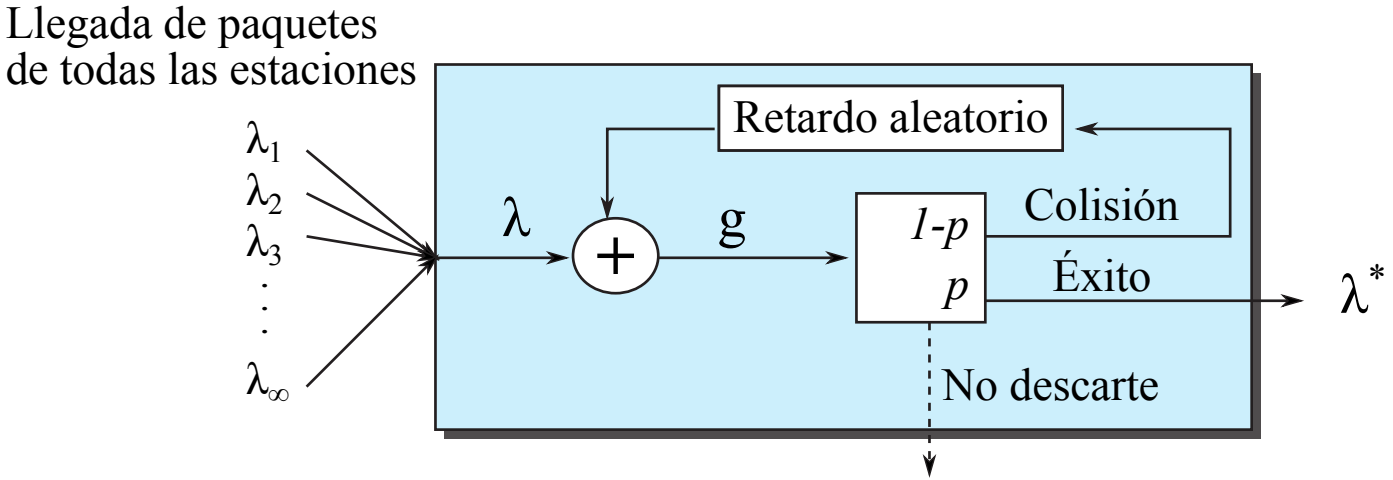
La entrada al sistema son todos los paquetes que se intentan enviar.

No todos los paquetes enviados se reciben en el destino (colisiones).

¿Cómo de eficiente es la red?

¿Cuánto tráfico puede atravesar la red?

Aloha: descripción del protocolo



λ, media de paquetes nuevos generados por una población infinita (**intensidad de tráfico**)

g, media de intentos de transmisión (nuevos y viejos).

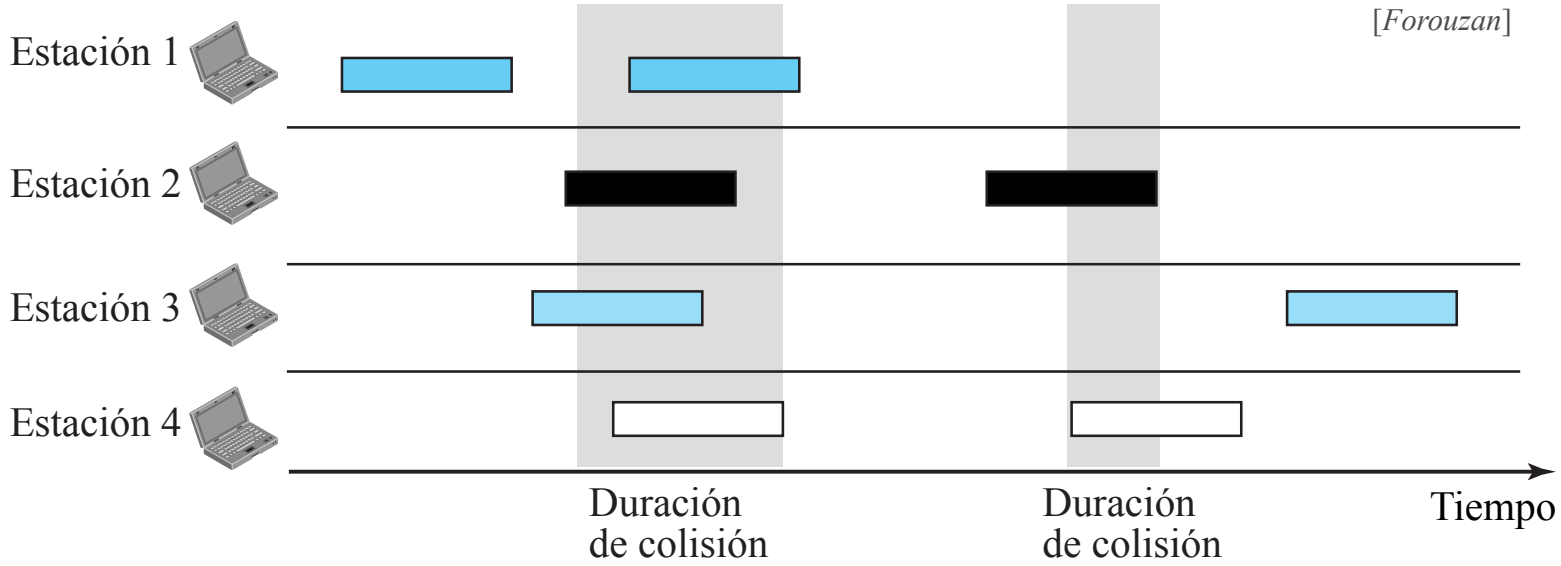
$\lambda^* = gP_0$, donde P_0 es la probabilidad de que una trama no sufra colisión.

Si sistema estable entonces retardo finito $\Rightarrow \lambda^* = \lambda$

Aloha

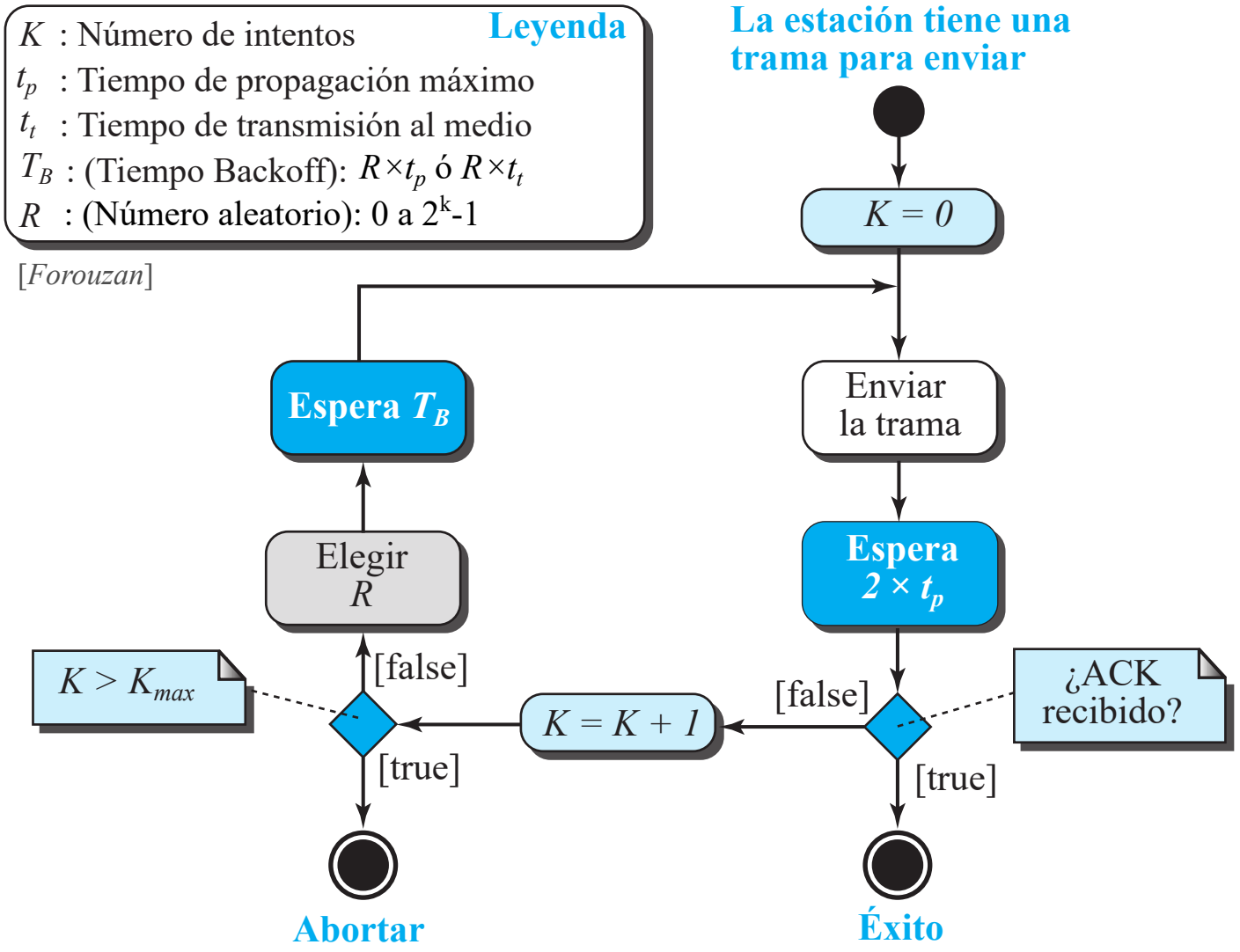
En **Aloha**, cada estación envía una trama si tiene tramas para enviar (acceso múltiple).

Por lo tanto, como sólo hay un canal para compartir, hay la posibilidad de colisión entre tramas de diferentes estaciones.

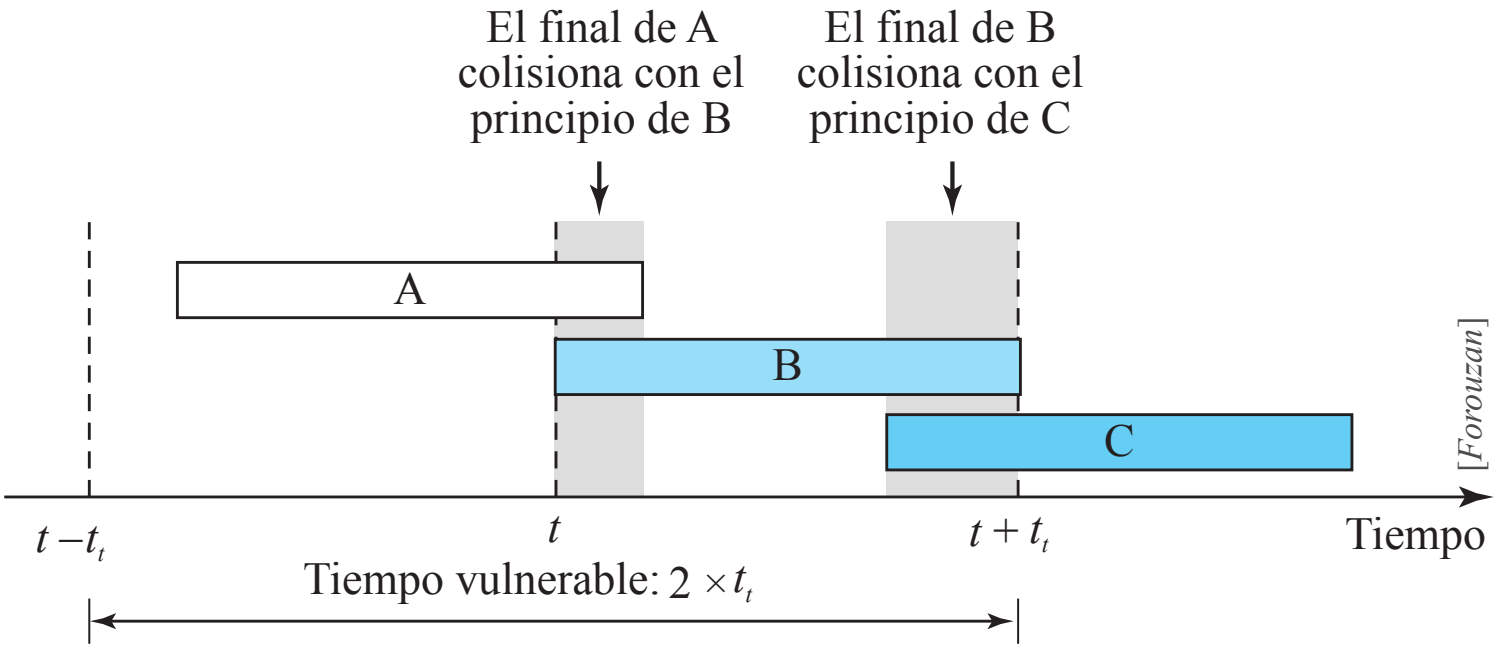


- Hay cuatro estaciones compitiendo por el medio físico compartido.
- Cada estación envía dos tramas (total 8 tramas).
- Seis tramas entran en conflicto y sólo sobreviven dos tramas.
- Las tramas que han entrado en conflicto deberán ser reenviadas.
- Es evidente que, aunque un sólo bit de una trama coincida en el tiempo con algún otro bit de otra trama, el total de ambas tramas son destruidas.

Aloha: procedimiento



Aloha puro: periodo vulnerable



Se define **Periodo** o **tiempo vulnerable** al intervalo de tiempo donde hay posibilidad de colisión.

Supongamos que cada estación envía tramas de longitud fija, y que cada trama necesita t_t segundos para ser transmitido.

La transmisión de un paquete (nuevo o viejo) es éxito si ningún otro paquete se planifica para transmisión en el intervalo $[t - t_t, t + t_t]$.

$$\boxed{\text{Periodo vulnerable} = 2 \times t_t}$$

Aloha puro: rendimiento (I)

La distribución de Poisson expresa la probabilidad de que ocurrra un determinado número de eventos (k), en un periodo de tiempo, dada una frecuencia de ocurrencia media (λ):

$$P[k] = \frac{\lambda^k e^{-\lambda}}{k!}$$

Si la generación de tramas (nuevas y retransmitidas) sigue un proceso de Poisson de media g, la probabilidad de generar k tramas en un intervalo de tiempo T (tiempo de transmisión de trama), sería gT.

Por simplicidad, normalizamos T a la unidad, por lo tanto:

$$P[k] = \frac{g^k e^{-g}}{k!}$$

Por lo tanto, la **probabilidad de éxito** (no colisión), y por tanto, que no se genere ninguna trama, $(k = 0)$, en el intervalo T:

$$P[k = 0] = e^{-g}$$

Como en Aloha, el periodo vulnerable es $2T$, la probabilidad de éxito:

$$P_0 = P[k = 0] \times P[k = 0] = e^{-2g}$$

Aloha puro: rendimiento (II)

Dada una red de acceso múltiple formada por N estaciones, con una tasa de transmisión de tramas (f), tiempo de transmisión de trama (t), ancho de banda nominal (C) y longitud de trama (L).

Entonces, la **carga de tráfico normalizada**, para cada nodo:

$$g = f \times t = f \times \frac{L}{C}$$

Carga de tráfico ofrecida (G):

$$G = N \times g$$

Alternativamente:

$$G = \frac{N \times f \times L}{C} = \frac{\lambda_0}{C}$$

$$\lambda_0 = GC$$

Carga de tráfico cursada (S) o **Productividad**:

$$S = GP_0 = Ge^{-2G}$$

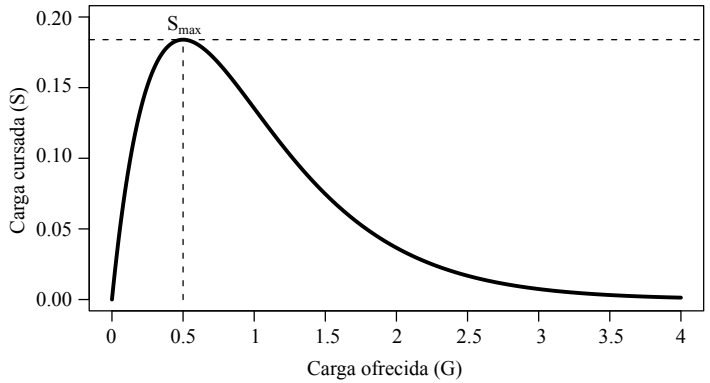
λ_0, **intensidad de tráfico** (bps).

Maximizando la productividad:

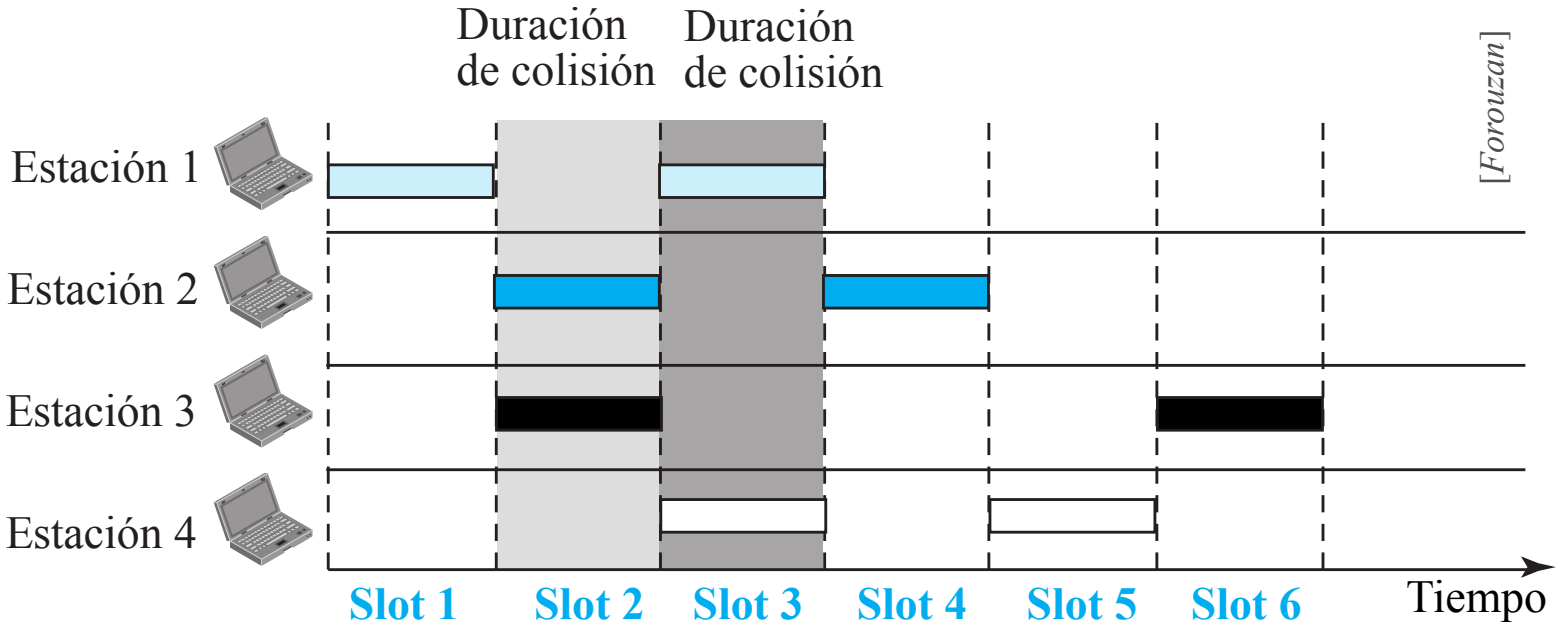
$$\frac{\partial S}{\partial G} = e^{-2G} - 2Ge^{-2G}$$

$$\frac{\partial S}{\partial G} = 0 \Rightarrow \begin{cases} G = \frac{1}{2} \\ S = \frac{1}{2e} \approx 0{,}18 \end{cases}$$

$\Rightarrow$



Aloha ranurado (*slotted*)



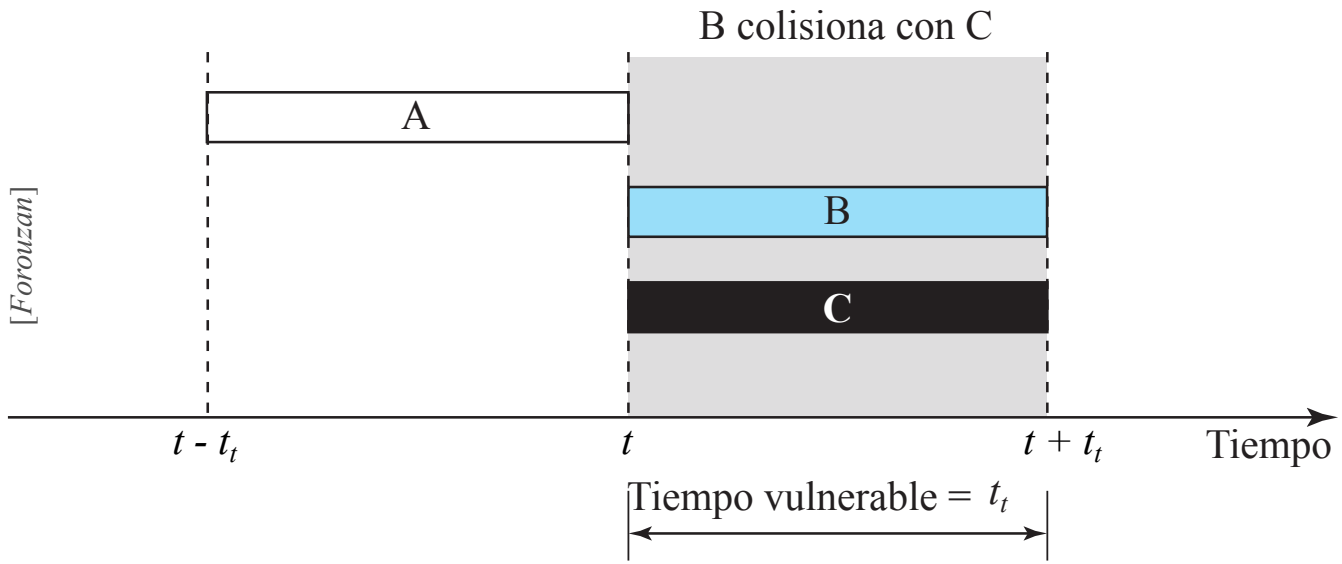
Todas las transmisiones están sincronizadas.

El tiempo en ranuras (slots) de t_t segundos y las estaciones son forzadas a enviar tramas sólo al principio de cada ranura.

Si no se consigue éxito en la transmisión, cada usuario colisionado, independientemente de los otros, planifica su retransmisión en una ranura aleatoria en el futuro.

La ranura aleatoria es para evitar que un conjunto de paquetes no colisionan indefinidamente

Aloha ranurado: periodo vulnerable



Como sólo está permitido enviar al principio de cada ranura, si una estación pierde la oportunidad de transmitir, deberá de esperar a la siguiente ranura.

Cada estación que comience al principio de cada ranura, se asegura que ha finalizado la transmisión de las otras tramas.

Evidentemente, no se elimina la posibilidad de colisión si dos estaciones inician transmisión al principio de la ranura.

El periodo vulnerable se reduce a la mitad:

$$\text{Periodo vulnerable} = t_t$$

Aloha ranurado: rendimiento

Sea el periodo vulnerable T, **tráfico ofrecido** G. Sabemos que la probabilidad de no generación de tráfico, en el intervalo T:

$$P[k = 0] = e^{-G}$$

entonces, la probabilidad de éxito en el intervalo T:

$$P_0 = P[k = 0] = e^{-G}$$

por lo tanto, el **tráfico cursado (Productividad)**:

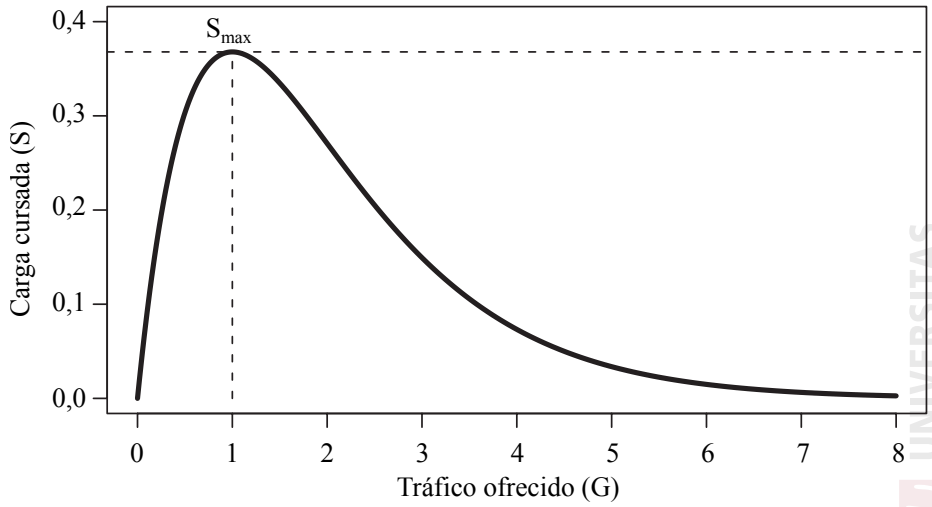
$$S = P_0 G = e^{-G} G$$

Maximizando la productividad:

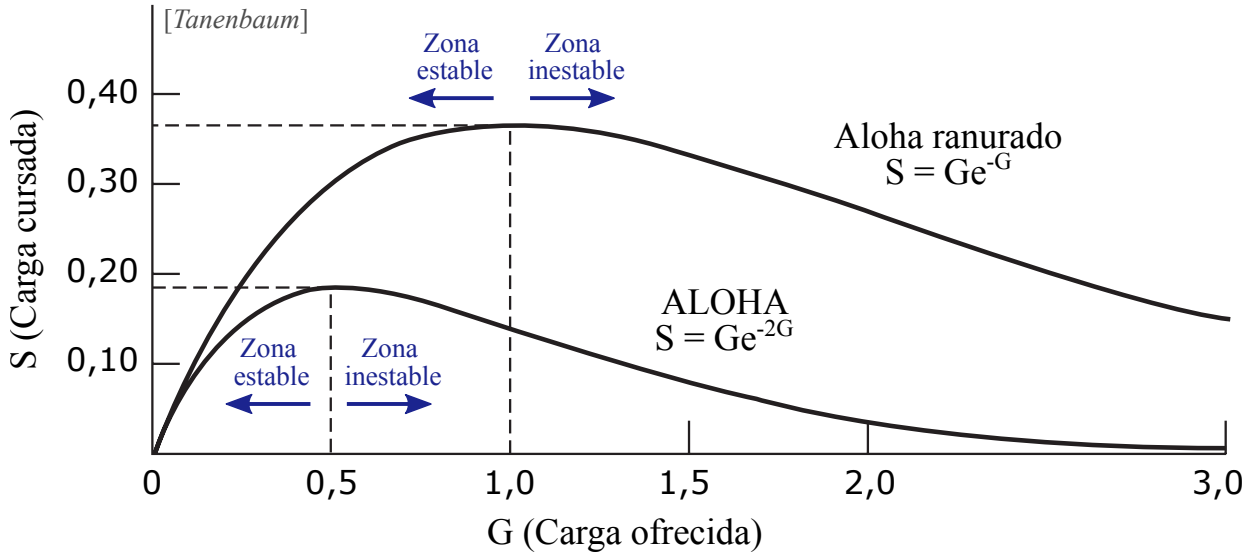
$$\frac{\partial S}{\partial G} = e^{-G} - G e^{-G}$$

$$\frac{\partial S}{\partial G} = 0 \Rightarrow \begin{cases} G = 1 \\ S = \frac{1}{e} \approx 0{,}37 \end{cases}$$

$\Rightarrow$



Aloha y Aloha ranurado: inestabilidad (I)



Para cualquier valor $0 \leq S < \eta_{max}$, la ecuación $S = f(G)$ tiene dos soluciones distintas, dependiendo de G_0, G_1 con $G_0 < G_1$:

G_0: tráfico ofrecido bajo $\rightarrow$ Baja probabilidad de colisión
G_1: tráfico ofrecido elevado $\rightarrow$ Alta probabilidad de colisión

Teorema de Inestabilidad:
Para cualquier punto de operación inicial (G_i, S_i), la transición a (G_1, S_1) en un intervalo T es casi segura si $T \rightarrow \infty$ *(inestabilidad)*.

Aloha y Aloha ranurado: inestabilidad (II)

¿Cuántas tramas serán retransmitidas en función de G?

Sea $P_k = \{$*Prob. de que una transmisión requiera exactamente* k *intentos*$\}$, es decir, la probabilidad de que se produzcan $(k-1)$ colisiones, seguida de éxito:

$$P_k = (1 - P_0)^{k-1} P_0$$

si la consideramos una distribución geométrica, entonces, la media de retransmisiones:

$$\mu[P_k] = \sum_{k=1}^{\infty} k P_k = \frac{1}{P_0}$$

Por lo tanto:

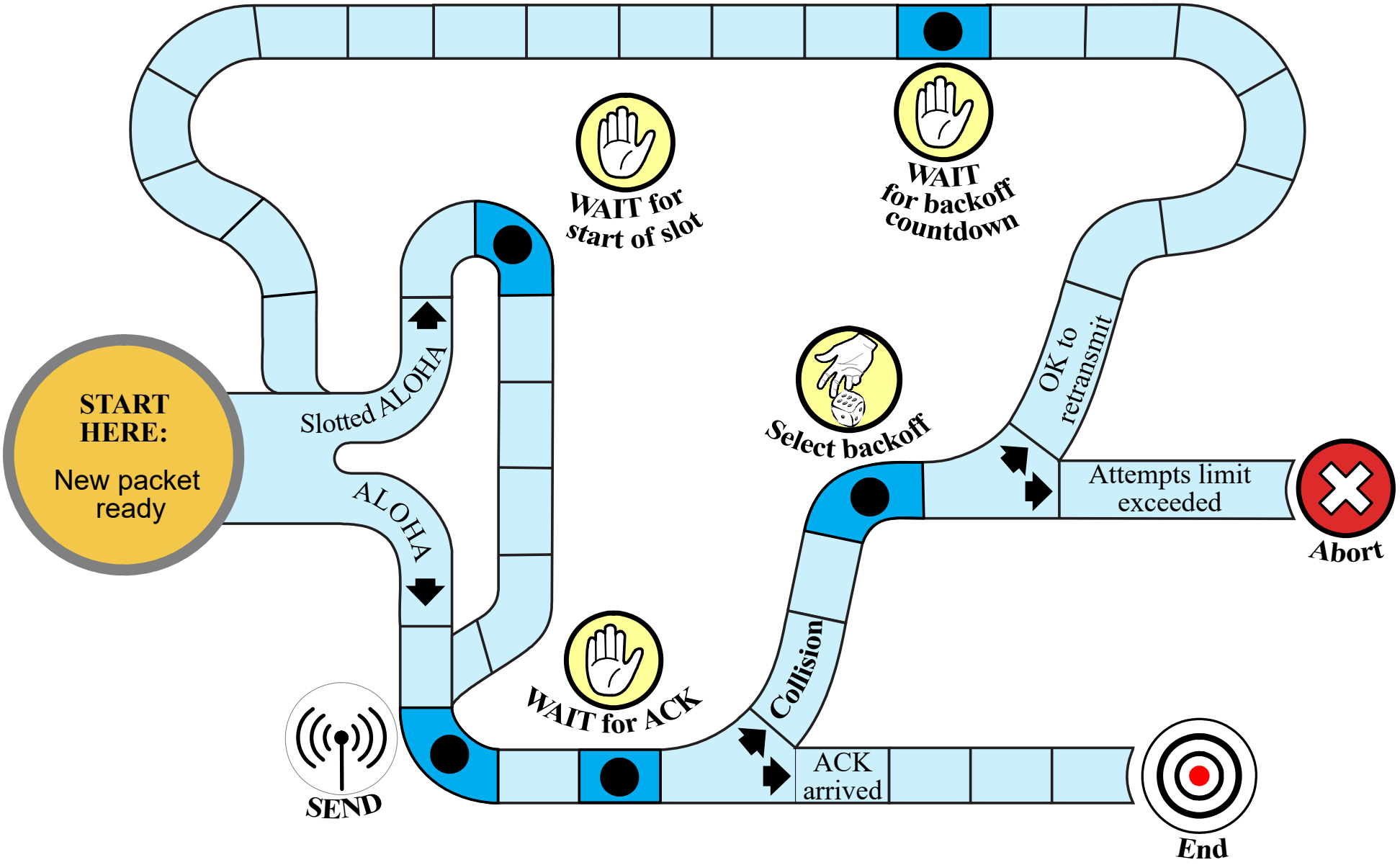
$$[\text{Aloha}] \Rightarrow P_0 = e^{-2G} \Rightarrow \mu_{Aloha} = e^{2G}$$

$$[\text{Aloha-r}] \Rightarrow P_0 = e^{-G} \Rightarrow \mu_{Aloha-r} = e^{G}$$

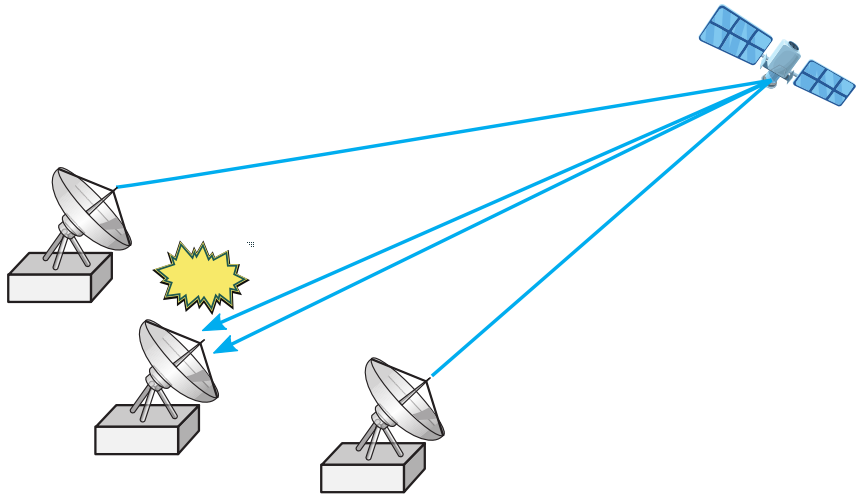
Existe una dependencia exponencial de μ (retransmisiones) respecto de G: pequeños aumentos en la carga del canal pueden reducir drásticamente su eficiencia.

El efecto de la carga del canal y su efecto en el rendimiento es más acentuado en Aloha que en Aloha-r.

Aloha vs Aloha ranurado



Resumen Aloha



Resuelve el problema de acceso al medio de forma simple.

No son demasiado eficientes (máximos 18 %-36 %).

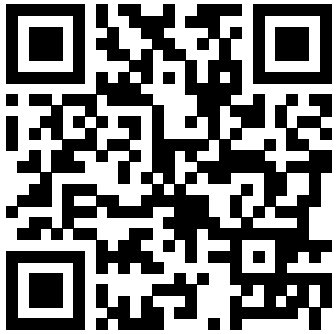
El tiempo de propagación no afecta en protocolos Aloha.

Determinantes los tiempos de llegada al receptor: **si llegan de forma simultánea, se produce colisión**.

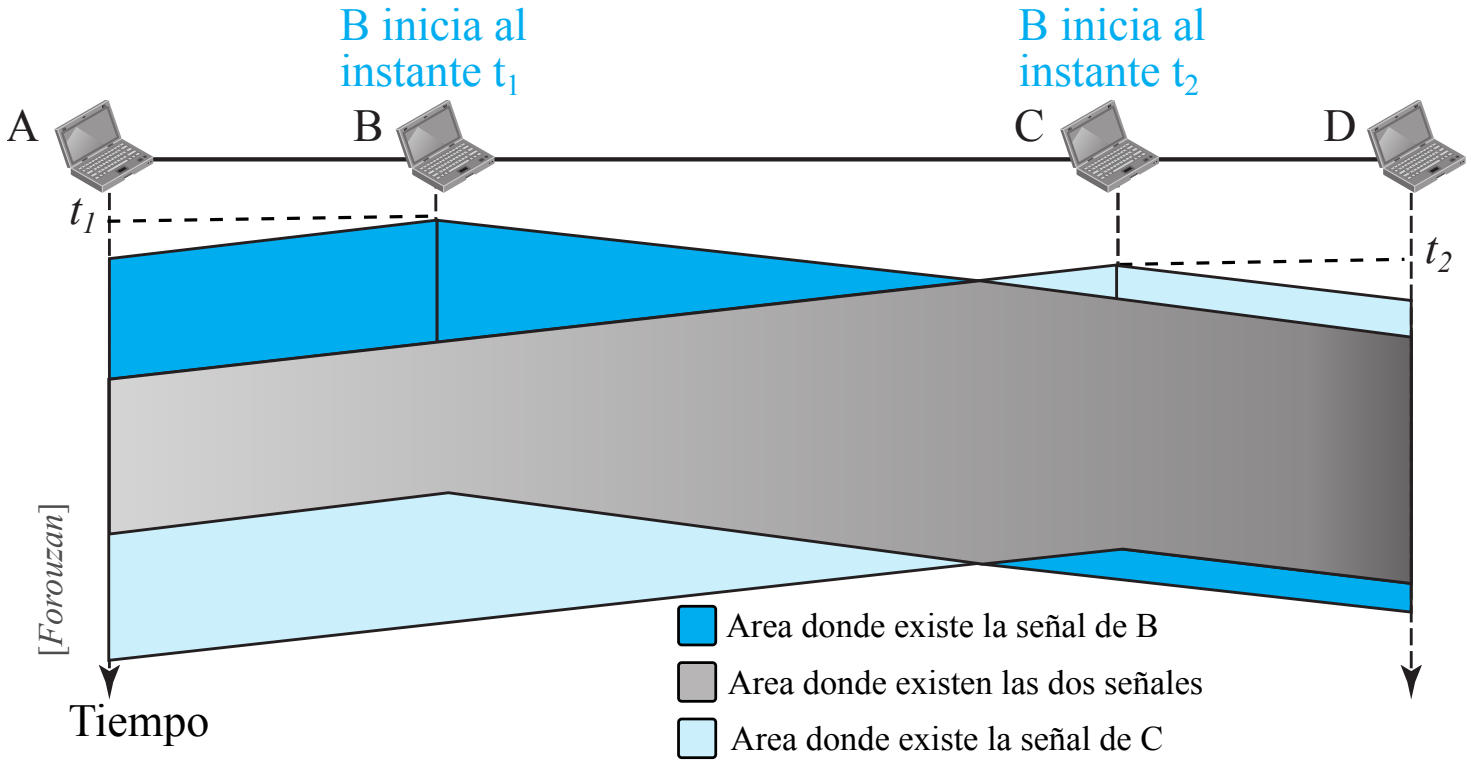
Funcionan independientemente de que el tiempo de propagación sea grande o pequeño comparado con el de transmisión.

Protocolos Aloha se utilizan en escenarios de comunicaciones satélite.

CSMA



CSMA (*Carrier sense multiple access*)

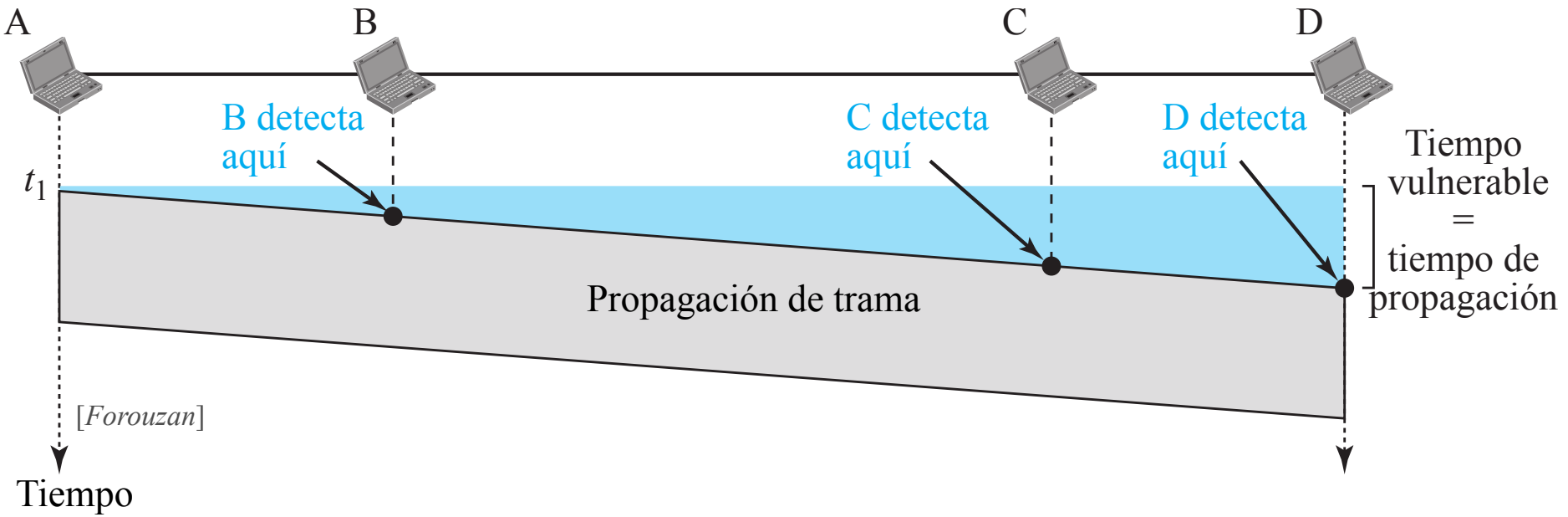


CSMA (*Carrier sense multiple access*) reduce la probabilidad de colisión, y por lo tanto, aumenta el rendimiento.

Si la estación escucha el medio antes de utilizarlo, se disminuye el riesgo de colisión.

CSMA reduce la posibilidad de colisión, pero no lo elimina, debido a la propagación de la señal en el medio compartido a lo largo del espacio y el tiempo.

CSMA



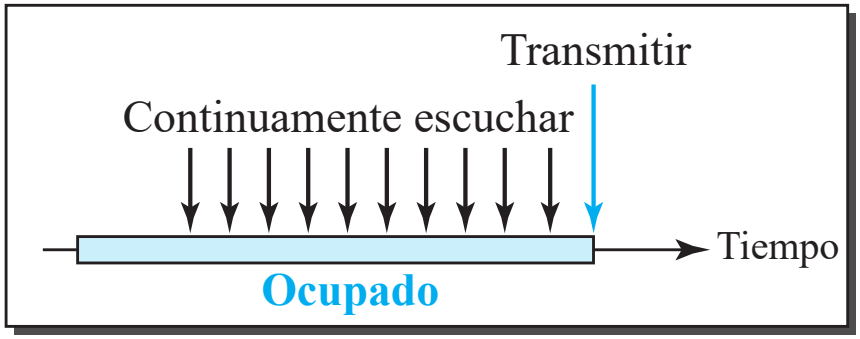
El **periodo vulnerable** en CSMA es el tiempo necesario para propagarse a lo largo del medio, es decir, el tiempo de propagación:

$$\boxed{\text{Periodo vulnerable} = t_p}$$

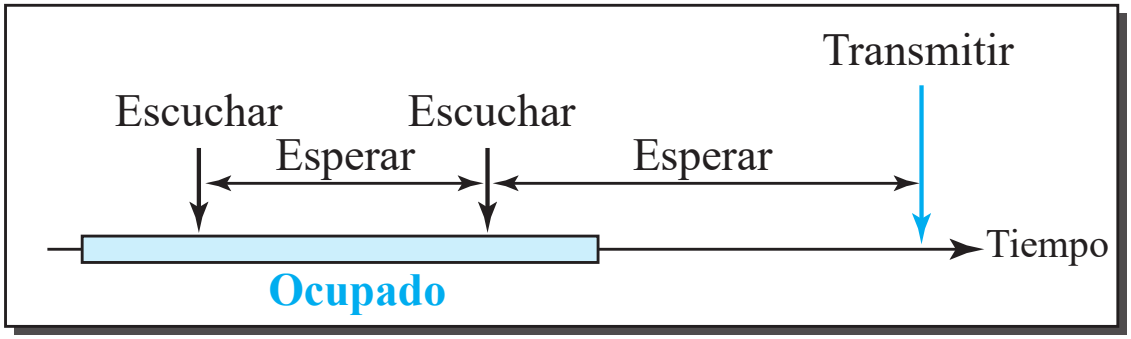
Si otra estación intenta transmitir durante este tiempo, se producirá colisión, pero si el primer bit de la trama alcanza el final del medio, en t_p, todos los medios habrán detectado que el medio está ocupado (*auscultación*), retrasarán su acceso al medio, evitando la colisión.

Métodos de persistencia (I)

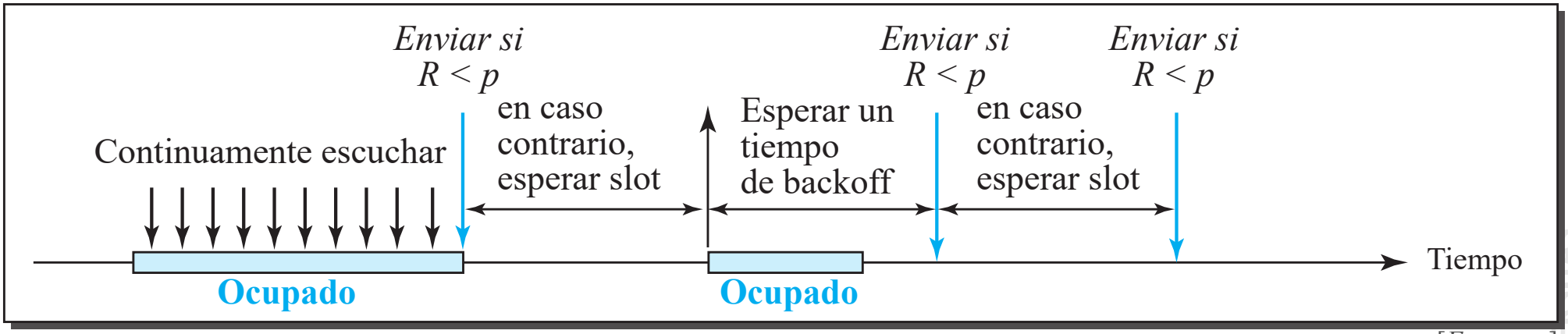
¿Qué debe hacer la estación si el medio está ocupado?



(a) 1-persistente



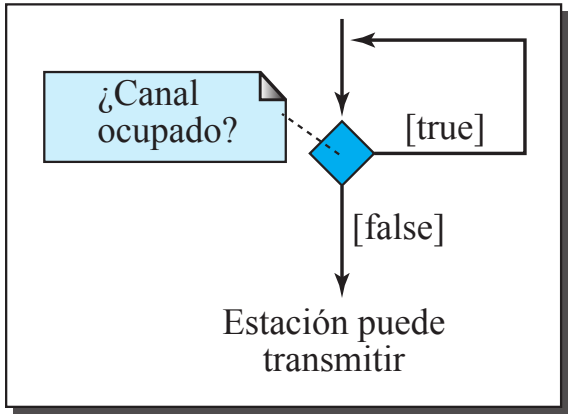
(b) No persistente



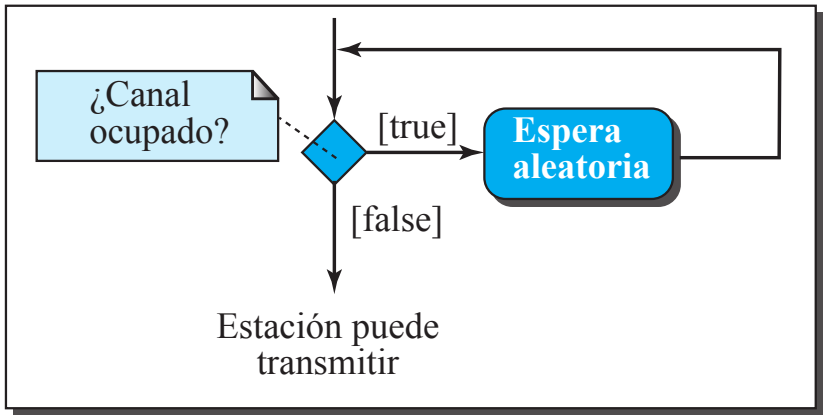
(c) p-persistente

[*Forouzan*]

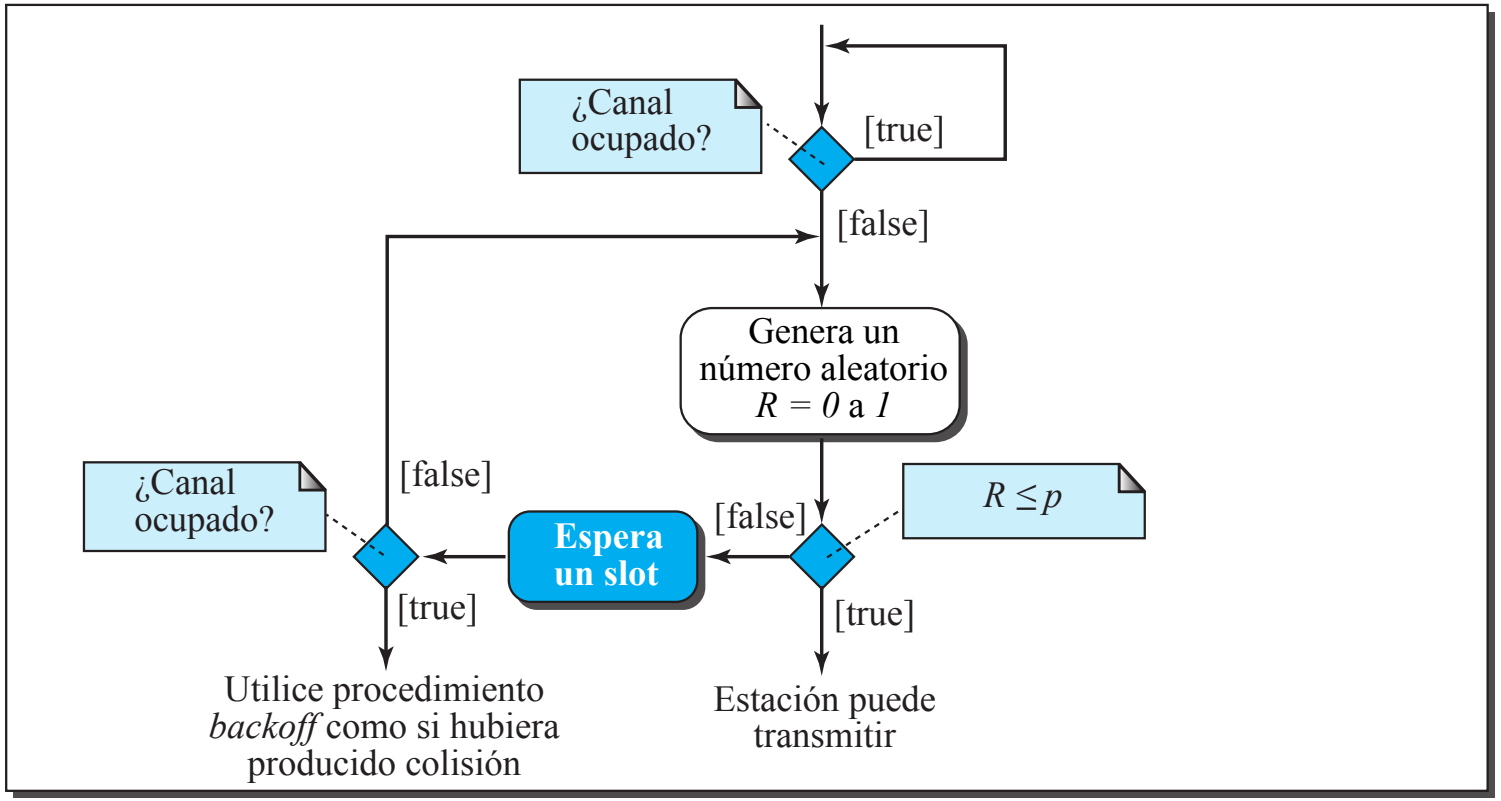
Métodos de persistencia (II)



(a) 1-Persistente



(b) No Persistente



[Forouzan]

(c) p-Persistente

CSMA: rendimiento

Sea:

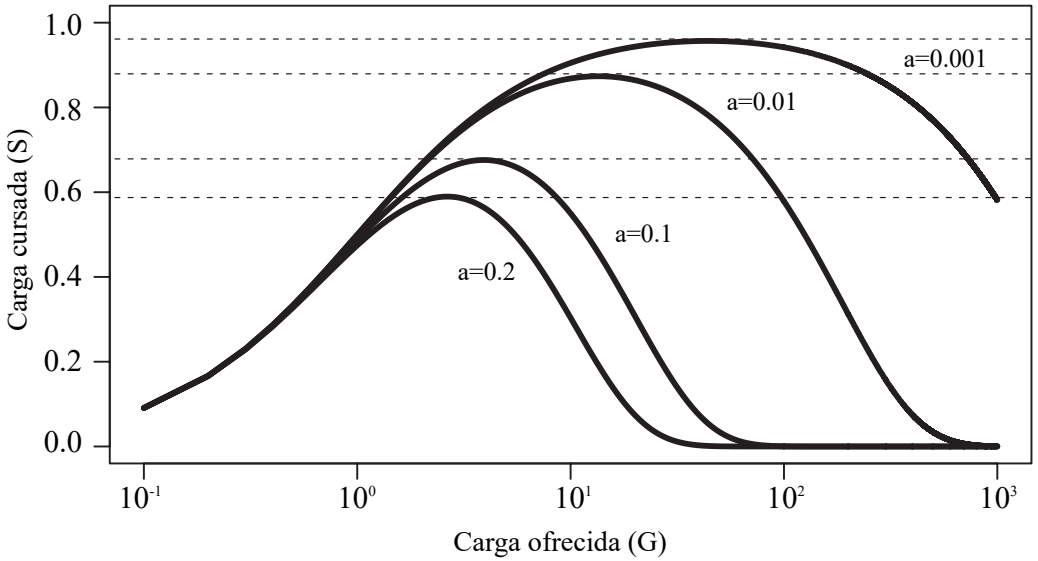
$$a = \frac{t_p}{t_t}$$

si normalizamos el tiempo de trama:

$$t_t = 1$$

entonces:

$$a = t_p$$



La **eficiencia**:

$$S = \frac{Ge^{-aG}}{G(1+2a) + e^{-aG}}$$

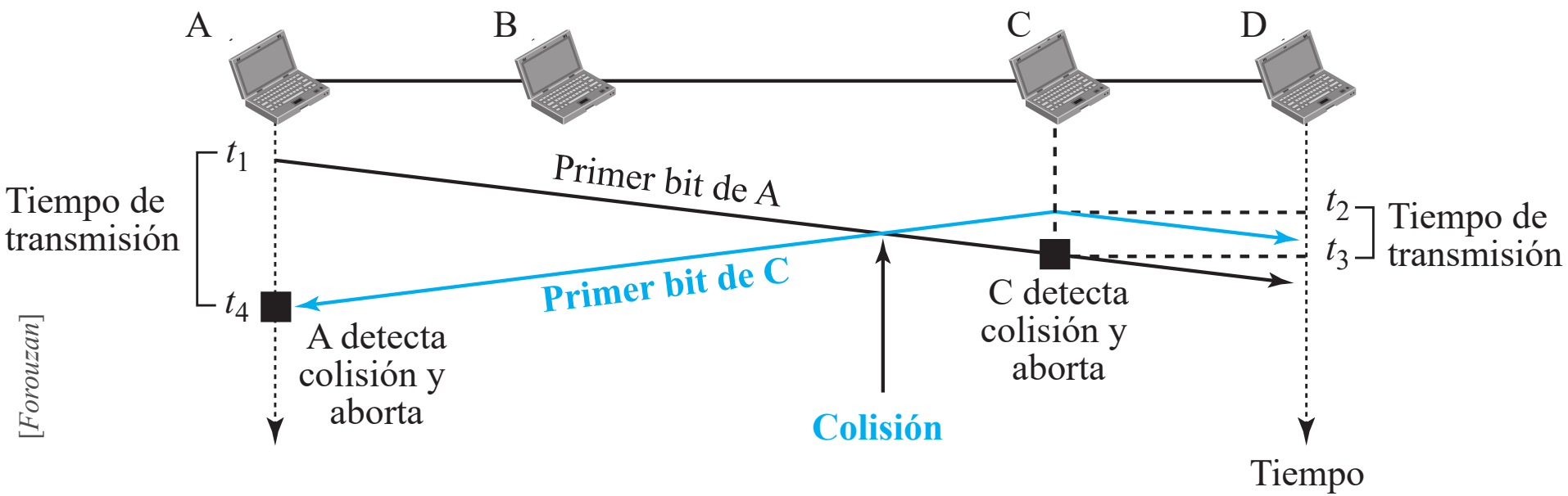
con las siguientes aproximaciones:

$$a \to 0 \Rightarrow S = \frac{G}{1+G}$$

$$G \to \infty \Rightarrow \frac{G}{1+G} = 1$$

CSMA/CD

CSMA/CD



El método CSMA no especifica el procedimiento a seguir una vez producida la colisión.

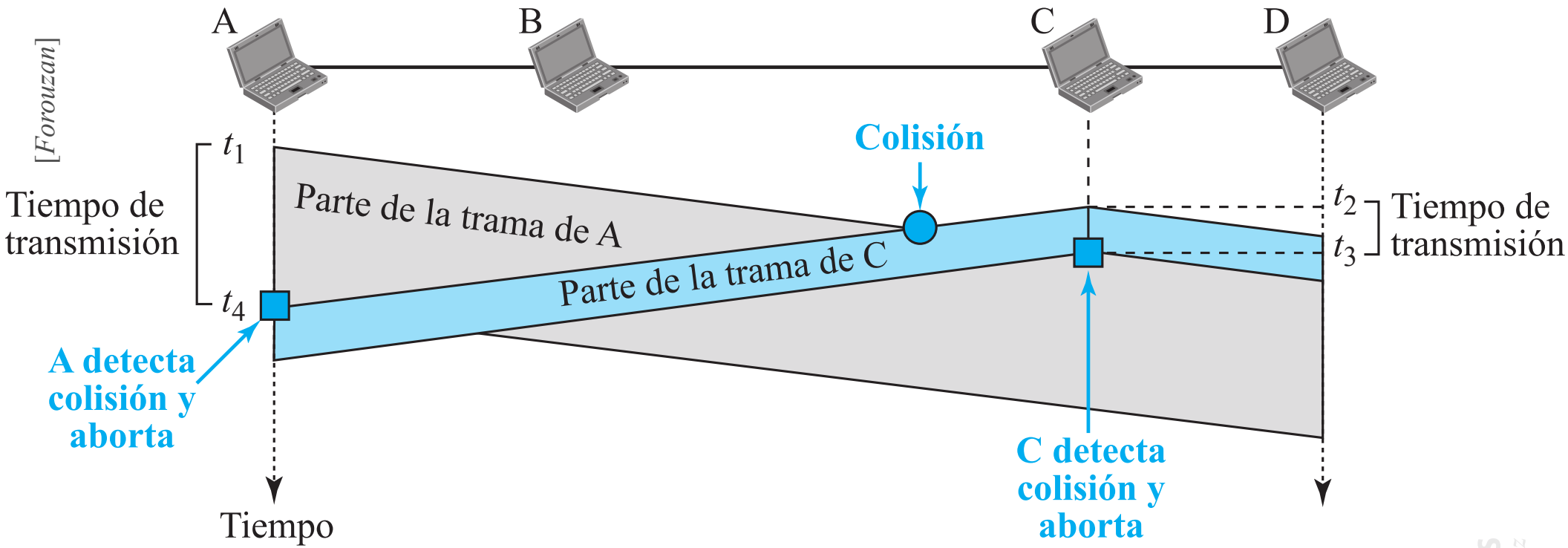
CSMA/CD *(Carrier sense multiple access with collision detection)* enriquece el algoritmo para manejar las **colisiones**.

En CSMA/CD, después de enviar la trama, la estación monitoriza el medio:

- Si lo que escucha es lo mismo que lo transmitido ⇒ transmisión exitosa.
- En caso contrario ⇒ colisión.

Las estaciones continúan transmitiendo bits hasta que detectan la colisión, es decir, hasta que retornan los primeros bits colisionados.

CSMA/CD: colisión e interrupción de transmisión



CSMA/CD: tamaño mínimo de trama

En CSMA/CD hay una **restricción del tamaño de trama**:

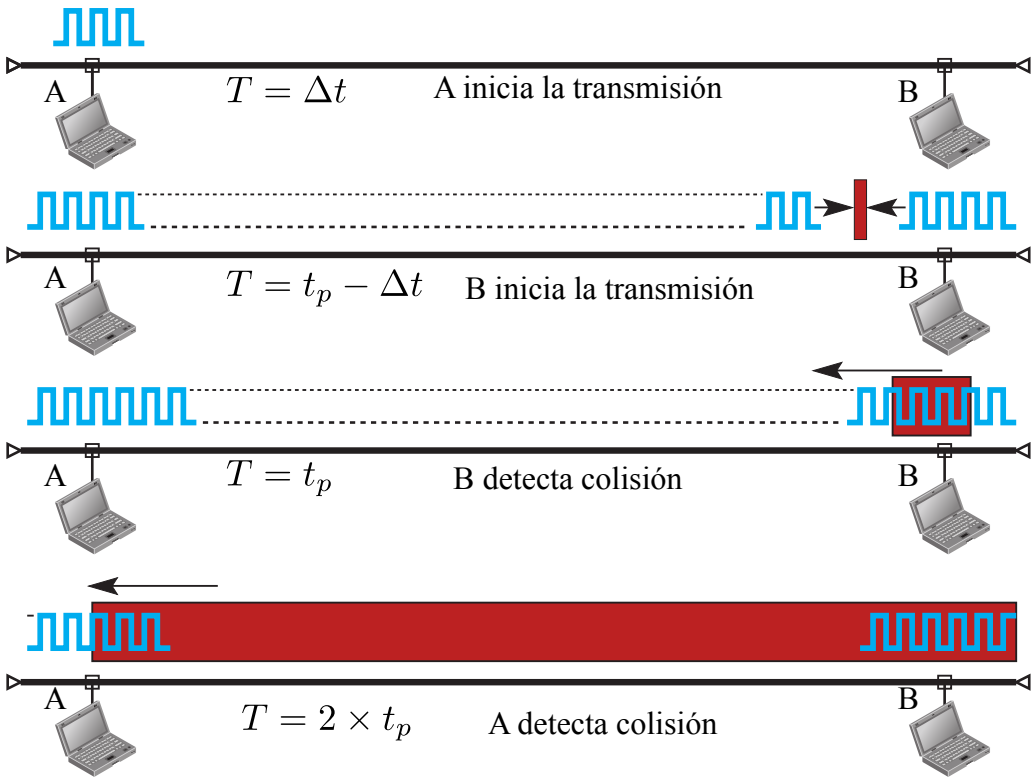
Antes de enviar el último bit de la trama, la estación emisora debe de detectar la colisión (caso de haberse producido), y si se produce, abortar la transmisión.

Una vez que la trama ha sido transmitida, no se guarda copia y por lo tanto, no se puede monitorizar la detección de colisión.

Por lo tanto, el tiempo de transmisión de trama (t_t), debe ser al menos, dos veces el tiempo de propagación (t_p):

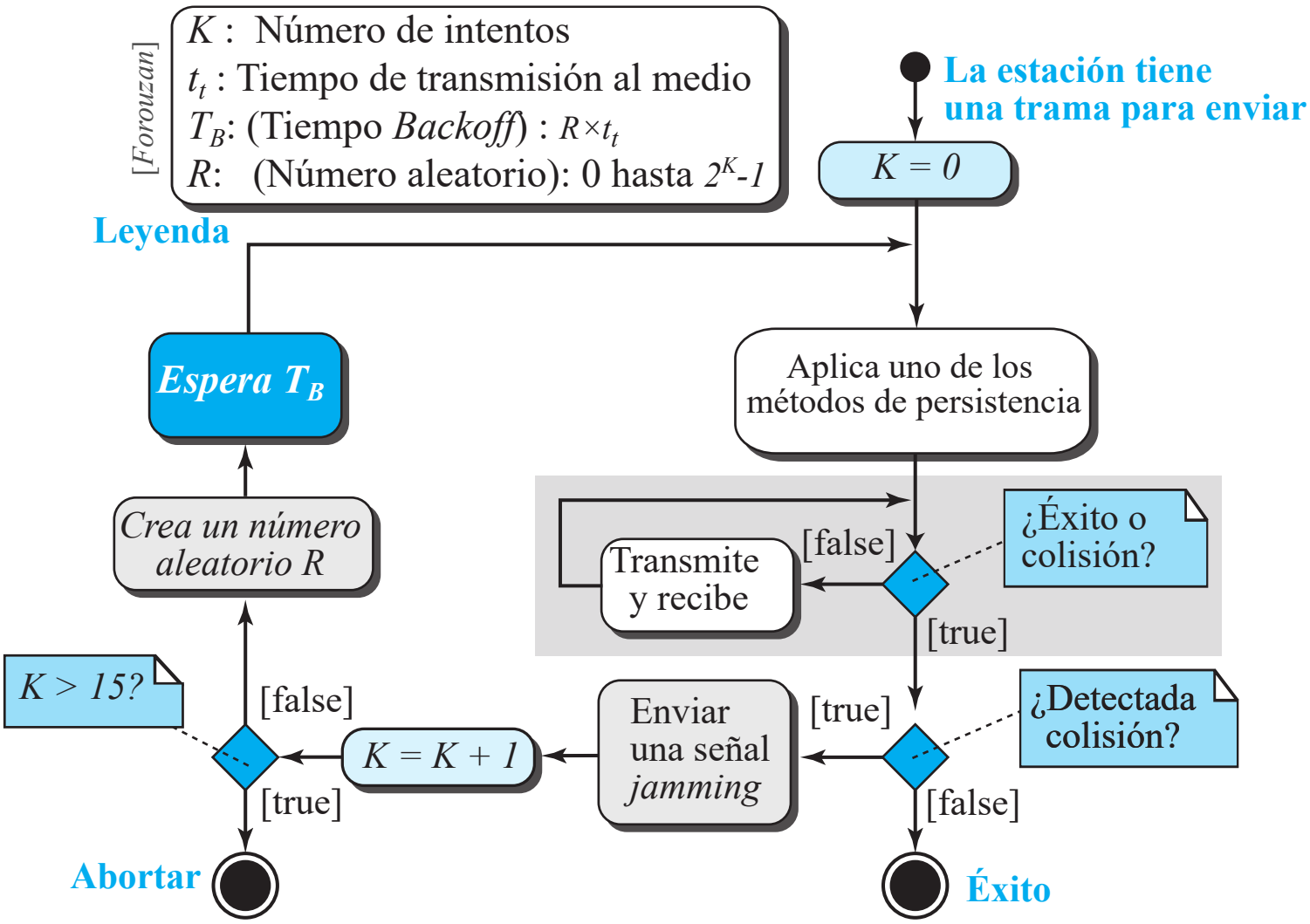
$$t_t = 2 \times t_p$$

CSMA/CD: colisión

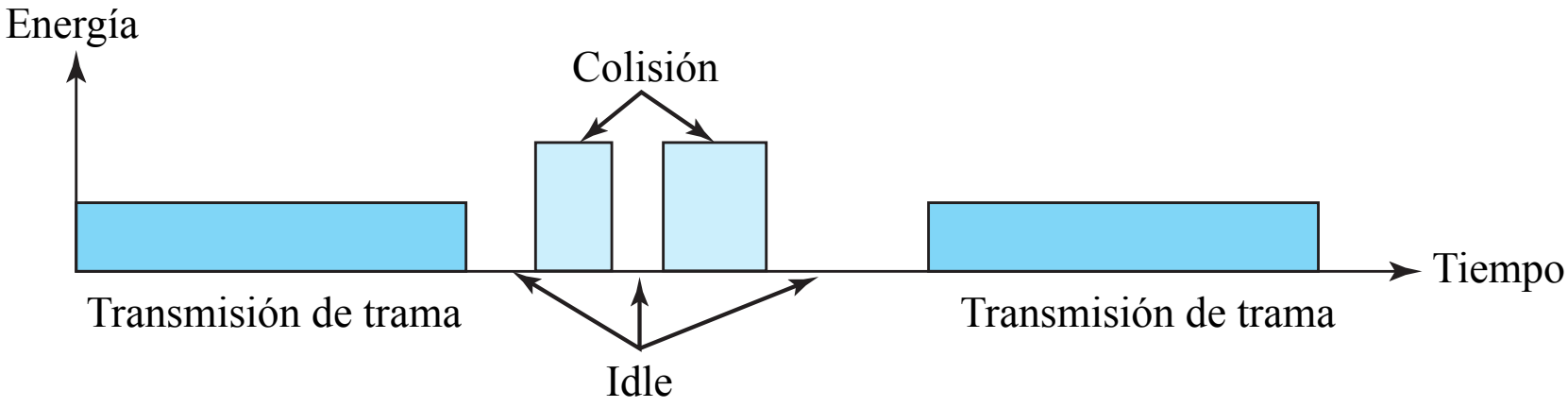


- Dos estaciones involucradas en una colisión están separadas la máxima distancia posible, por lo que el tiempo en recorrer el medio será t_p.
- Supongamos que la colisión se produce en $T = t_p - \Delta t, \Delta t \to 0$, es decir, inmediatamente antes de la estación más alejada, por lo tanto, la colisión necesitará otro t_p para alcanzar la primera estación.
- Por lo tanto, la primera estación debe estar transmitiendo hasta $2 \times t_p$ para que las noticias de la colisión le llegue mientras está transmitiendo.

CSMA/CD: procedimiento



CSMA/CD: nivel de energía del canal



El nivel de energía del canal puede tener tres niveles:

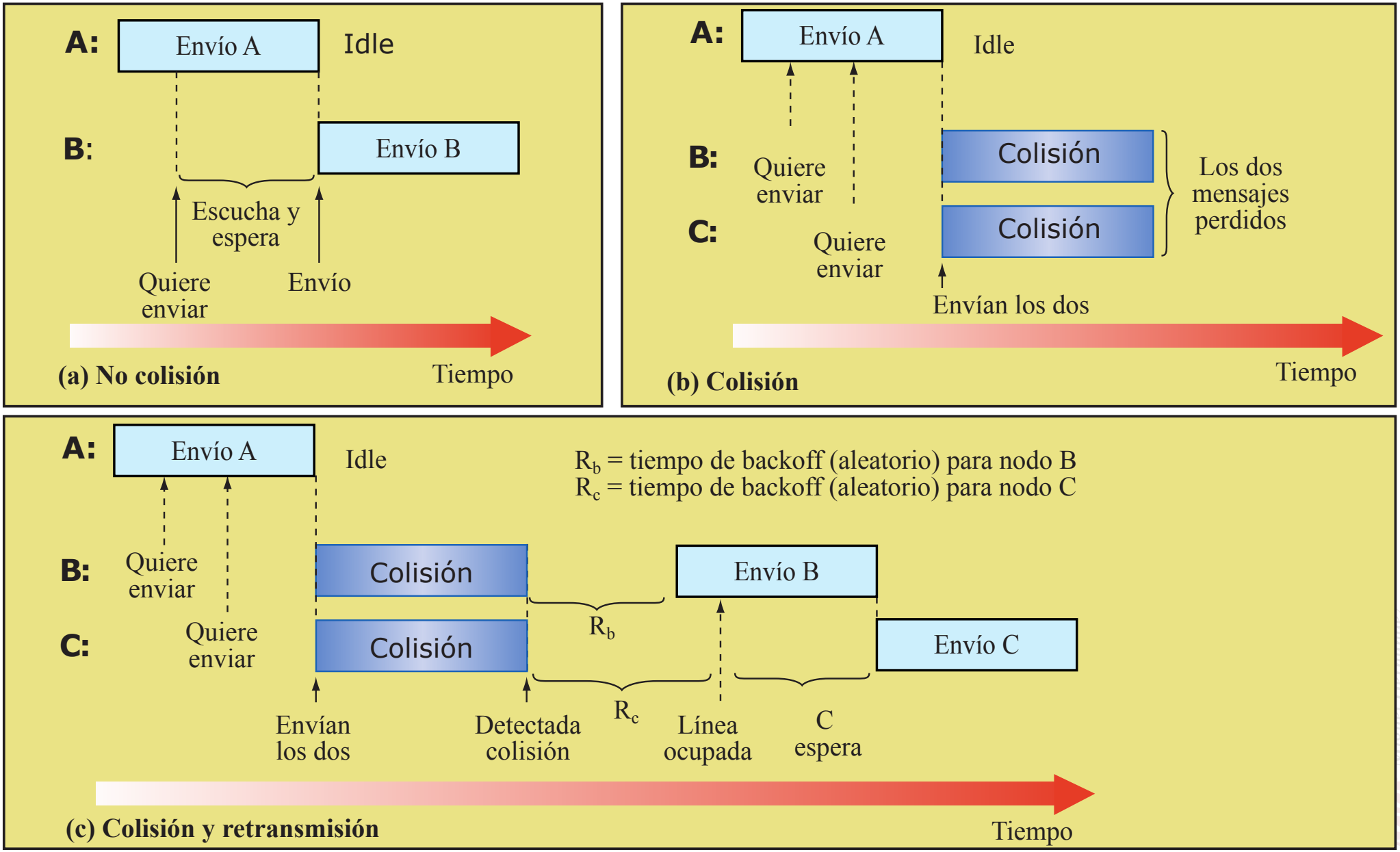
Cero: canal en reposo.

Normal: la estación ha capturado con éxito el canal y está enviando la trama.

Anormal: hay una colisión y el nivel de energía es el doble del nivel normal.

Las estaciones que tienen que enviar o están enviando tramas necesitan monitorizar los niveles de energía para determinar el estado del canal.

CSMA/CD: espera aleatoria



CSMA/CD: rendimiento

La **eficiencia**:

$$S = \frac{aGe^{-aG}}{a + aGe^{-aG} + a(1 - (1 + aG)e^{-aG})}$$

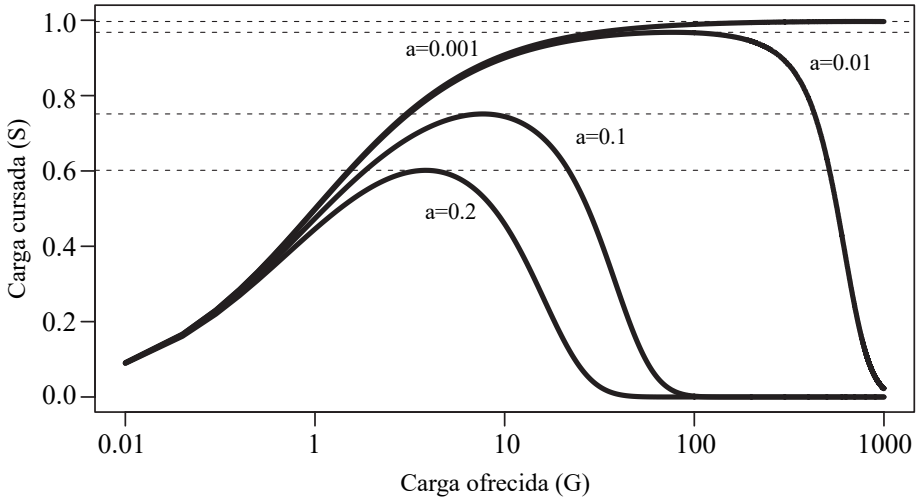
$$S_{\text{máx}} = \frac{1}{1 + 3{,}31a}$$

con las siguientes aproximaciones:

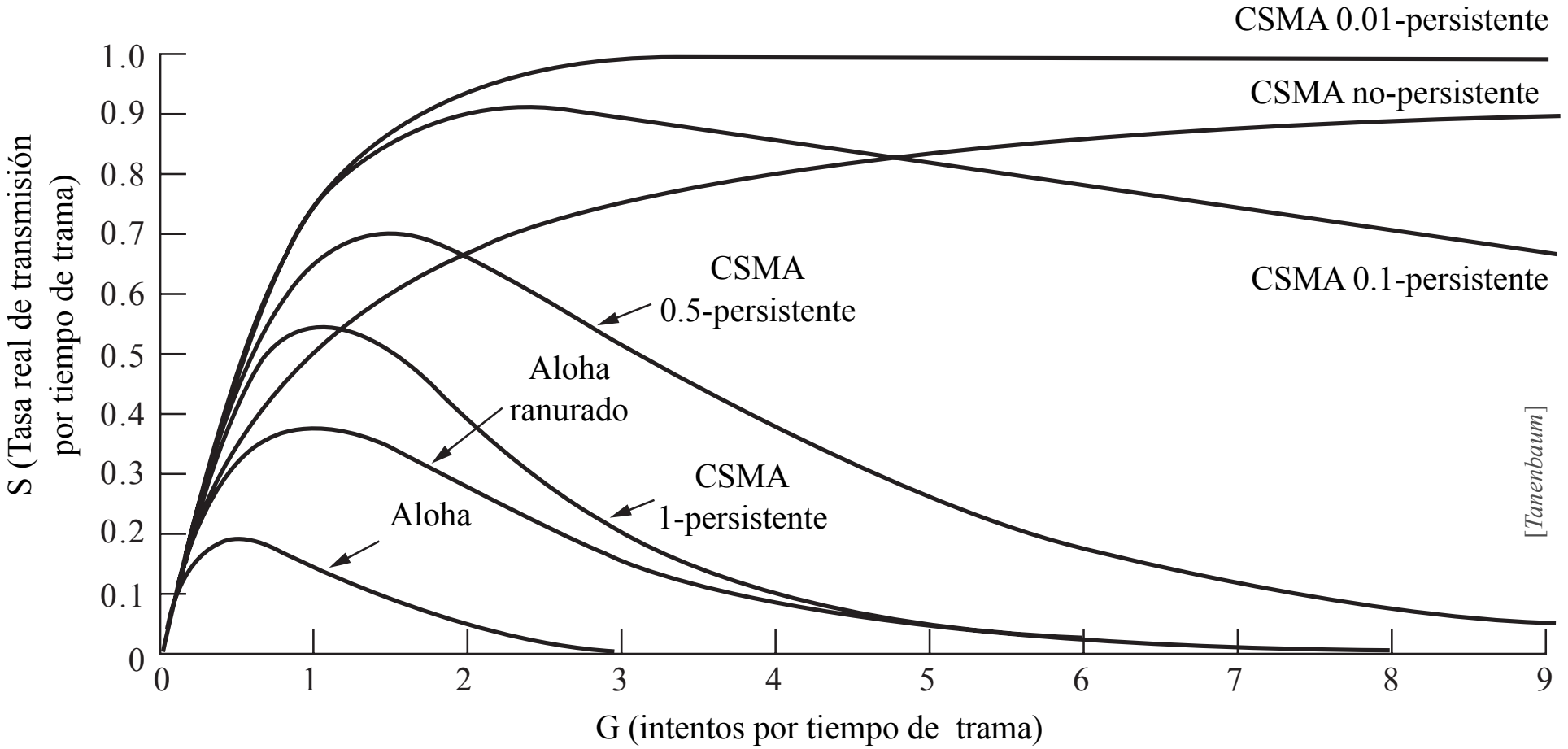
$$a \to 0 \Rightarrow S = \frac{G}{1 + G}$$

$$G \to \infty \Rightarrow \frac{G}{1 + G} = 1$$

$$a \to \infty \Rightarrow S = 0$$



Aloha vs CSMA (I)



Aloha vs CSMA (II)

¿Podríamos afirmar que ALOHA es la variante antigua y CSMA lo ha sustituido ya que es más eficiente?

NO

Simplemente, Aloha surgió antes, pero ambos tienes aplicaciones diferentes.

CSMA es una evolución adaptada para mejorar el caso típico de LANs, con medios de transmisión muy rápidos, por lo tanto:

$$t_p \ll t_t$$

Hemos definido el parámetro:

$$a = \frac{t_p}{t_t}$$

Si se tiene que:

- $a \ll 1$, CSMA es más apropiado y obtiene un rendimiento mejor que Aloha.
- $a > 1$, Aloha es muy sencillo y su eficiencia no depende de a.

Actualmente, encontramos aplicaciones de Aloha:

- Telefonía móvil, para solicitud de recursos
- Comunicación satélite
- Redes de cable, para petición de recursos de subida (ver DOCSIS)

CSMA/CA

CSMA/CA: evitar colisiones

El método **CSMA/CA** (*Carrier sense multiple access with collision avoidance*) fue desarrollado especialmente para **redes inalámbricas**.

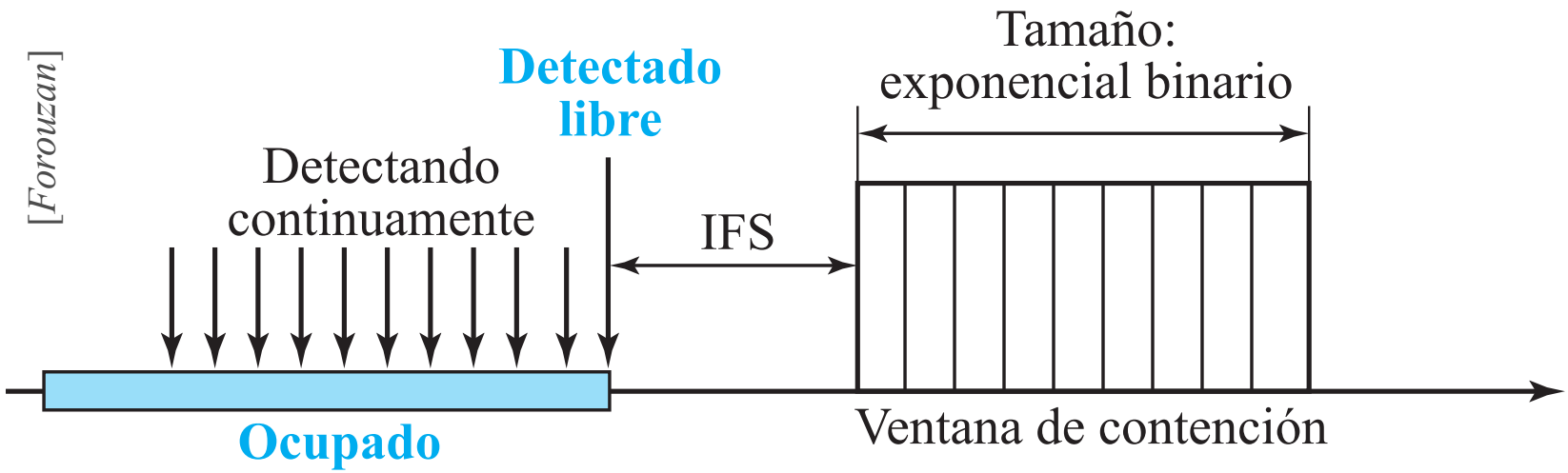
La colisiones se evitan mediante tres estrategias:

Interframe Space (IFS): Incluso cuando el canal está libre, las estaciones no transmiten inmediatamente, sino que se espera el denominado IFS (*Interframe Space*), ya que otra estación alejada, también puede haber iniciado la transmisión, y la señal todavía no haber alcanzado la primera estación.

Ventana de contención: La ventana de contención es una porción de tiempo dividida en ranuras. Una estación preparada para enviar, elige un número aleatorio de slots y se espera para enviar.

Confirmaciones: Si después de todas las precauciones, se produce colisión, se destruyen los datos, además de posibles distorsiones en el medio inalámbrico. Para ayudar a garantizar que el receptor ha recibido la trama, se proporciona **confirmación positiva** y uso de **temporizadores**.

CSMA/CA: ventana de contención



CSMA/CA y NAV

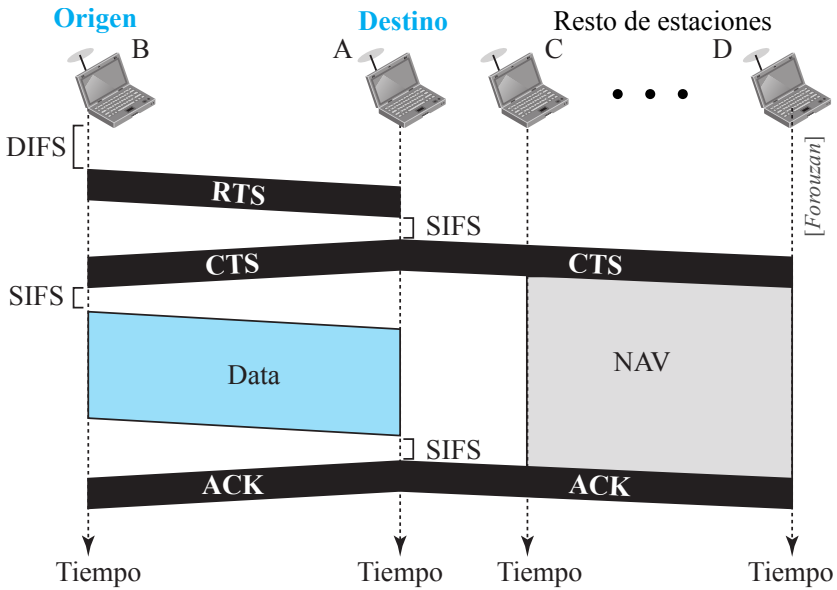
RTS: *Request to send.*

CTS: *Clear to send.*

DIFS: *DCF interframe space.*

SIFS: *Short interframe space.*

ACK: *Acknowledgment.*



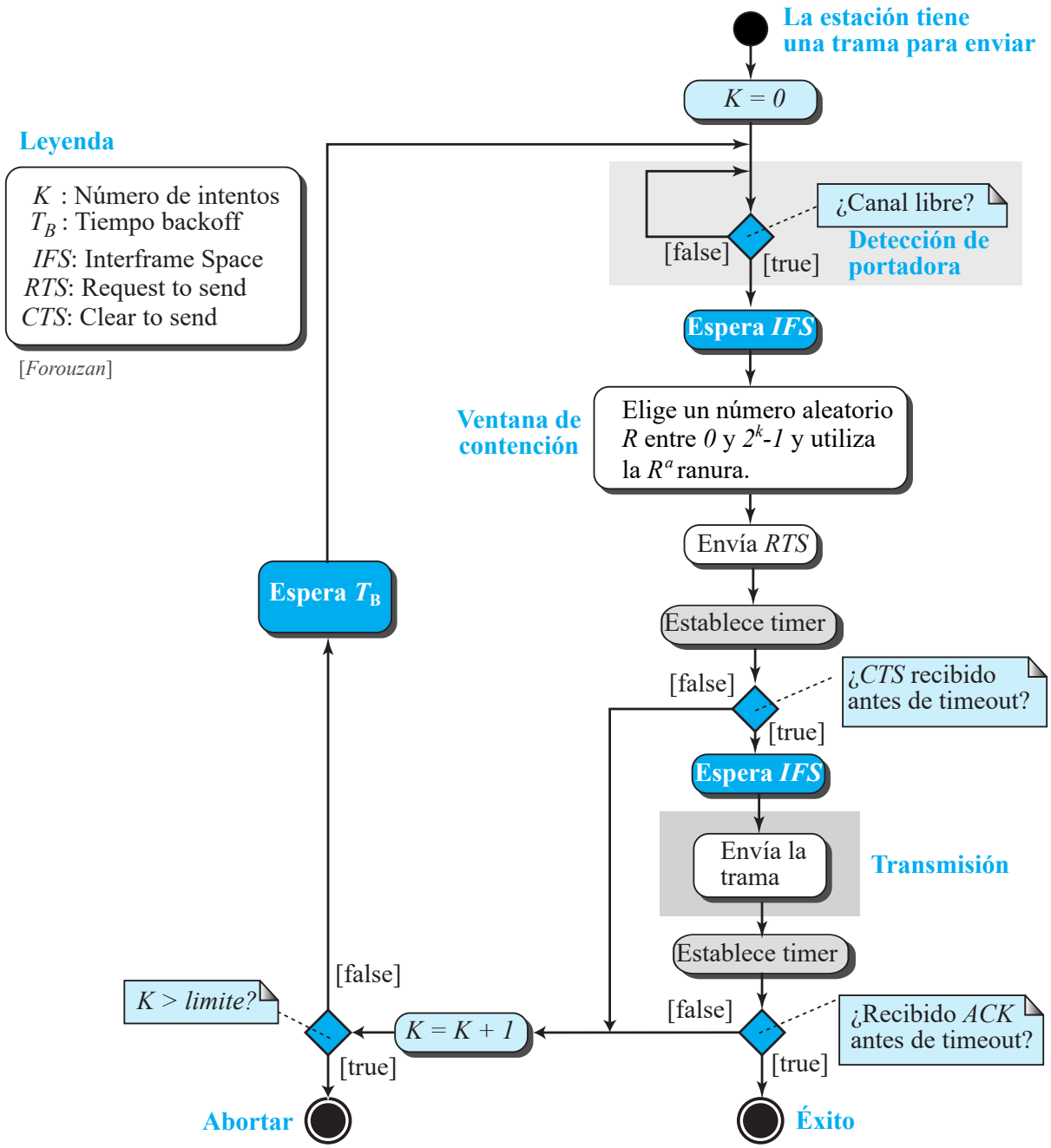
¿Cómo hacen las otras estaciones para retrasar el envío de sus datos si una estación adquire el canal?

Mediante `NAV` (*network allocation vector*), cada vez que una estación emite `CTS`, el resto de estaciones activan el temporizador `NAV`, que les indica cuánto tiempo debe pasar antes de que puedan chequear si el medio está libre.

Las estaciones, antes de chequear el medio físico, inspeccionan si ha expirado `NAV`.

¿Está totalmente libre de colisión el esquema CSMA/CA?

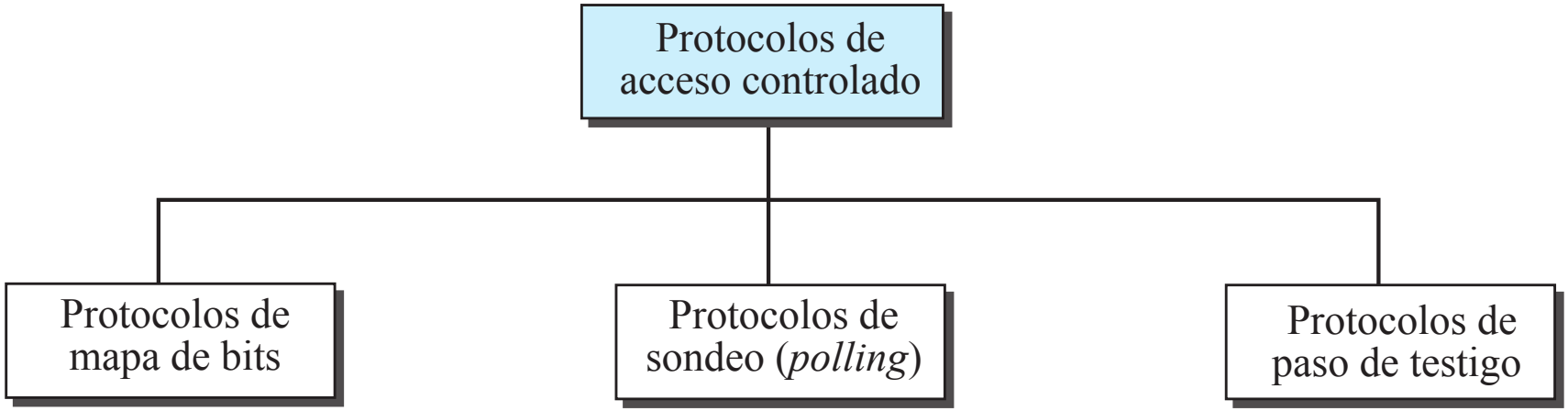
CSMA/CA: procedimiento



Control de acceso al medio

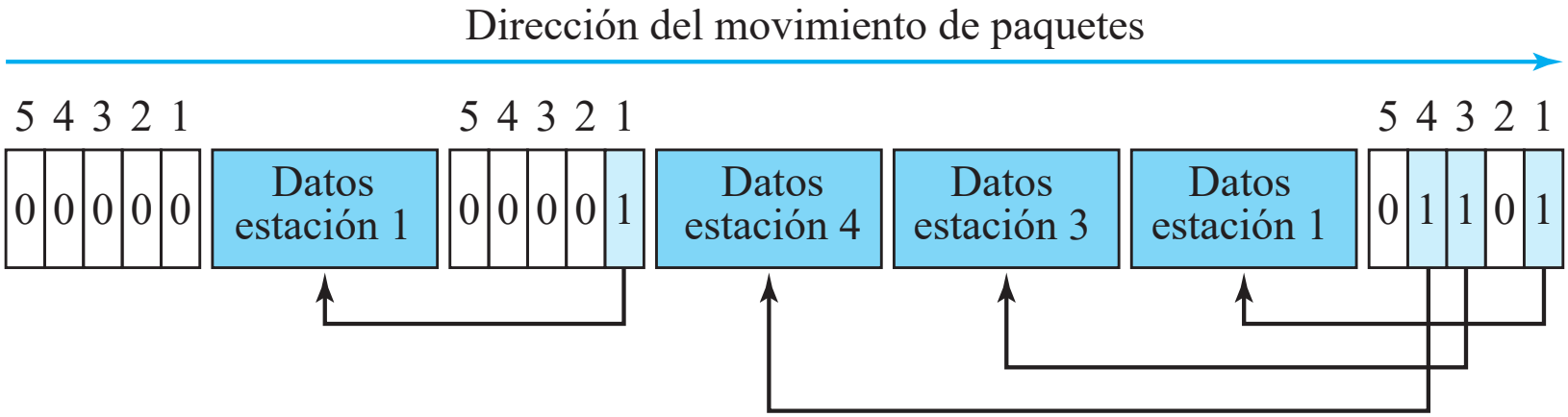
1. Introducción
2. Protocolos de acceso aleatorio
3. ***Protocolos de acceso controlado***
4. Familia Ethernet
5. Redes inalámbricas
6. Dispositivos de interconexión

Protocolos de acceso controlado



Protocolos de mapa de bits

Protocolos de reserva



También se denominan **protocolos de mapa de bits**.

Una estación necesita hacer la **reserva** antes de enviar datos.

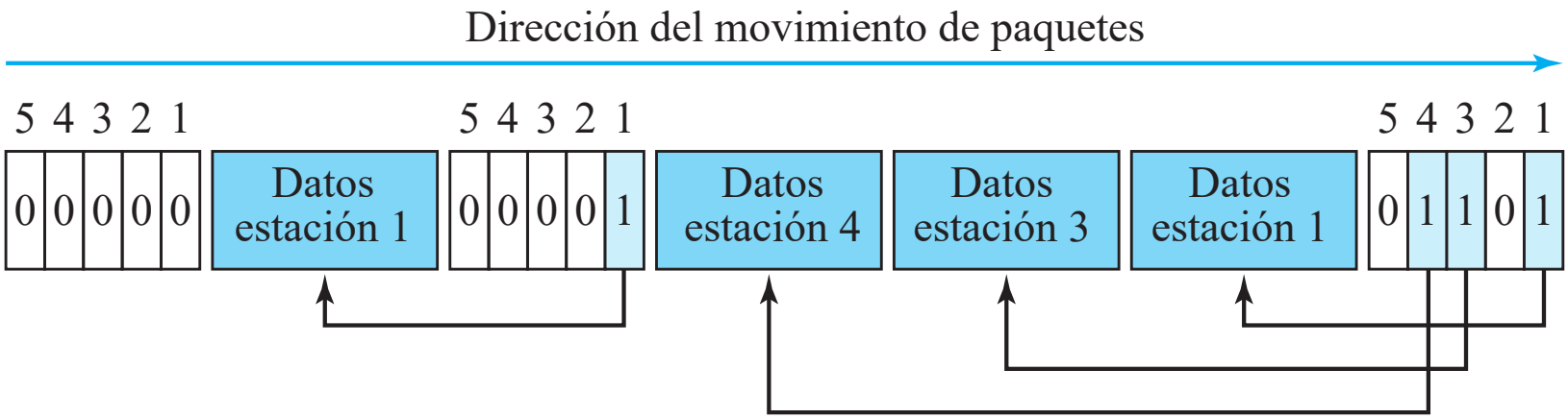
El tiempo se divide en **slots**.

En el periodo de reserva, una trama de reserva precede al envío de la trama de datos en el slot correspondiente.

Si hay N estaciones en el sistema, hay exactamente N minislots en la trama de reserva, donde cada estación hace su reserva en su minislot asignado.

Las estaciones que han realizado reserva, pueden enviar sus tramas de datos después de la trama de reserva.

Protocolos de reserva: rendimiento



Supongamos N estaciones y tramas de datos de longitud d, en situaciones extremas:

- *Baja carga*. Si suponemos que sólo una de las N estaciones existentes en el medio desea transmitir:

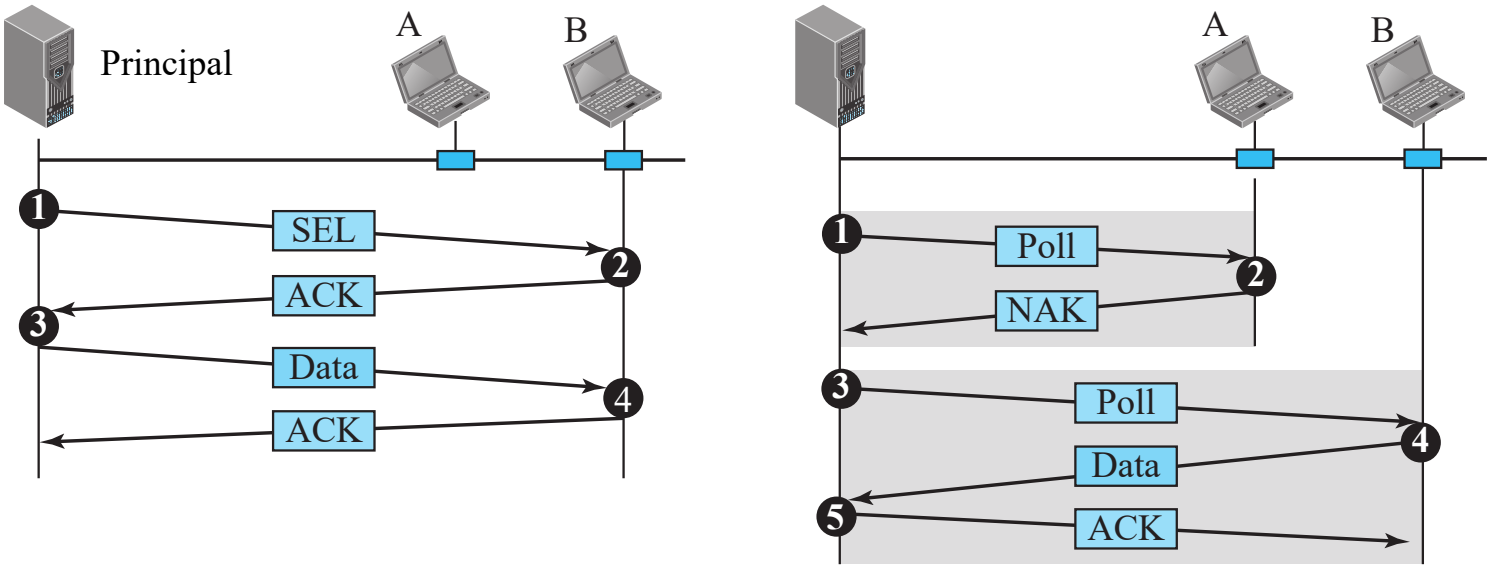
$$U = \frac{d}{d+N}$$

- *Alta carga*. Si suponemos que las N estaciones desean transmitir:

$$U = \frac{dN}{dN+N} = \frac{d}{d+1}$$

Protocolos de sondeo

Protocolos de sondeo



Selección Sondeo

Sondeo (Polling) opera en topologías donde un dispositivo ha sido designado como estación **principal**, y el resto son estaciones **secundarias**.

Todos los intercambios de datos deben pasar a través del dispositivo principal, incluso cuando el destino final sea otra estación secundaria.

El dispositivo principal controla el enlace y las secundarias siguen sus instrucciones.

La principal es la encargada de determinar qué dispositivo tiene permiso para utilizar el canal en cada instante.

Utiliza los métodos de sondeo y selección para prevenir las colisiones.

- **Selección:** cuando un dispositivo principal tiene datos para enviar al dispositivo secundario, que podrá responder con preparado (`ACK`) o no preparado (`NAK`).
- **Sondeo:** cuando el dispositivo principal solicita transmisión desde la secundaria. A partir del sondeo, la secundaria envía sus datos disponibles, en caso contrario, responde `NAK`.

Protocolos de paso de testigo

Protocolos paso de testigo

En el método de **paso de testigo**, las estaciones están organizadas en un anillo lógico, es decir, cada estación tiene un **predecesor** y **sucesor**: estaciones que están, lógicamente, antes y después.

La estación actual es la que está accediendo al medio.

Los derechos de acceso pasan del predecesor a la estación actual, y posteriormente, a la estación sucesora cuando no tenga más datos para enviar.

El derecho de acceso al canal se transfiere mediante una trama especial, denominada, **token**, que circula a lo largo del anillo.

La posesión del token otorga a la estación los derechos de acceso al medio.

Si una estación tiene datos para transmitir, espera hasta recibir el token de su predecesor.

Una vez adquiere el token, envía los datos disponibles.

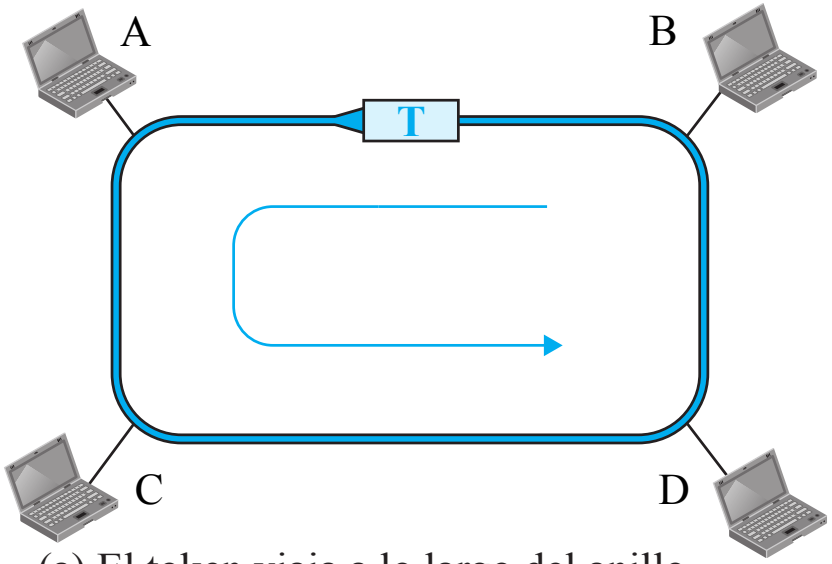
Cuando no tiene más datos, libera el token pasándolo al sucesor.

La estación no puede volver a transmitir datos hasta que vuelva a adquirir el token.

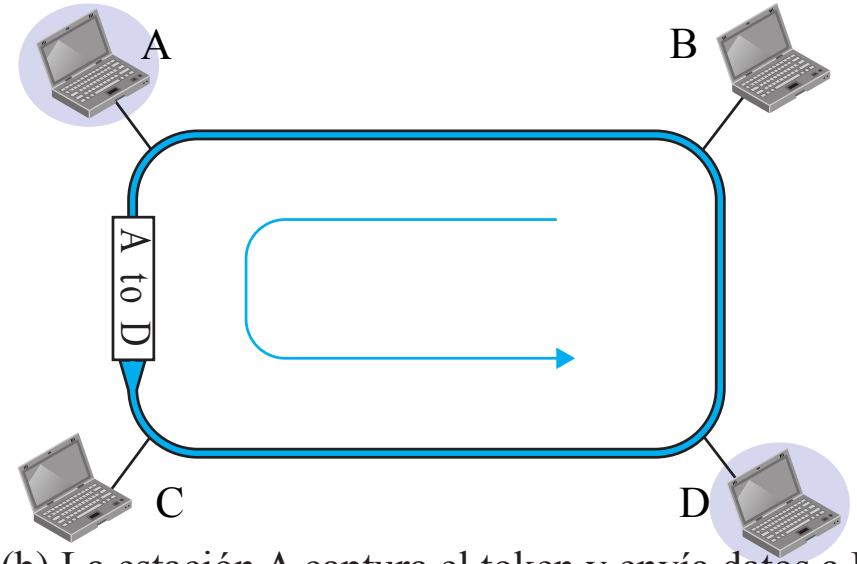
Si una estación adquiere token, y no tiene datos, libera el token inmediatamente.

Es necesario una gestión del token en el método de paso de testigo, para prevenir pérdidas de token, asignación de prioridades, etc.

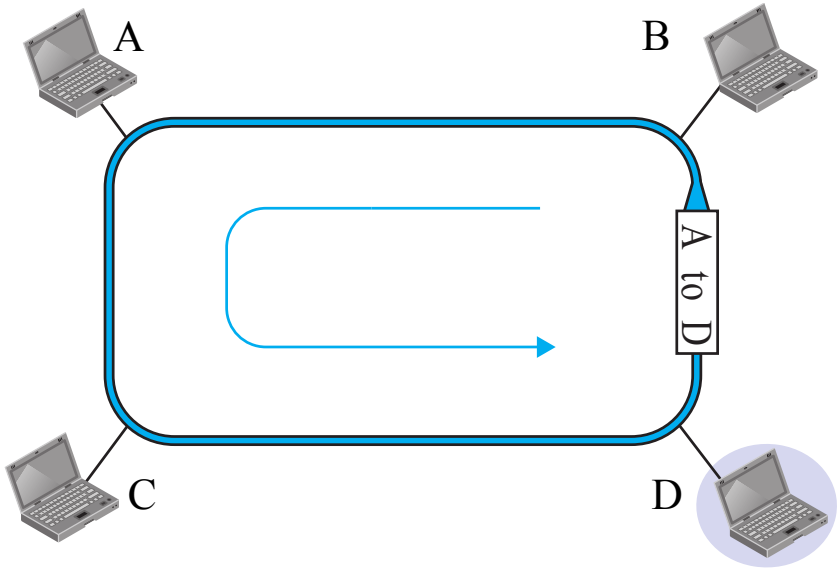
Liberación de token



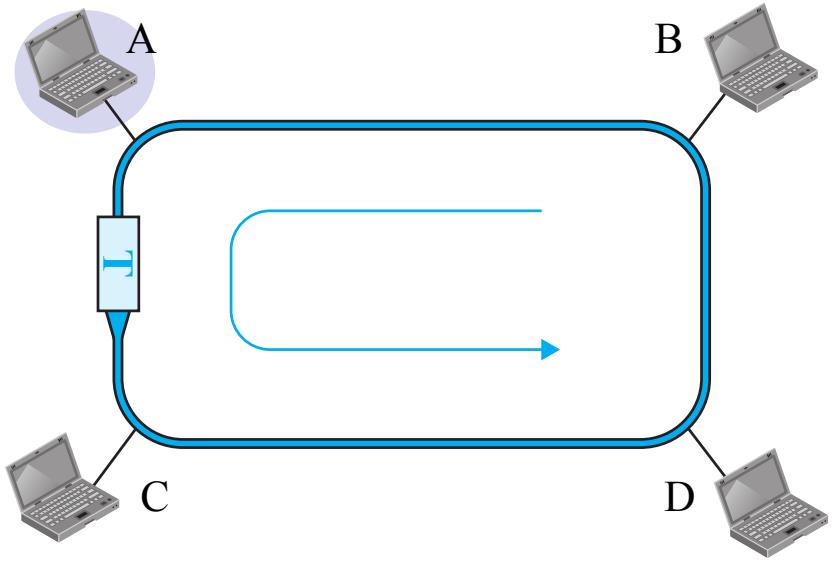
(a) El token viaja a lo largo del anillo.



(b) La estación A captura el token y envía datos a D.



(c) La estación D copia la trama y la envía de vuelta al anillo.

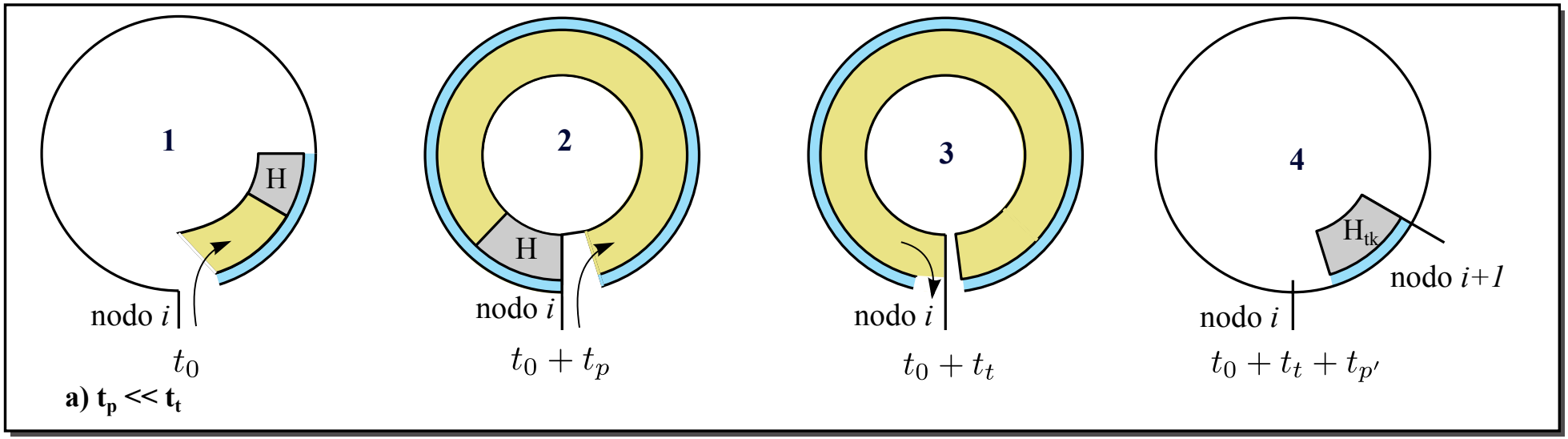


(d) La estación A recibe la trama y libera el token.

Análisis de prestaciones (I)

Leyenda: t_t : tiempo de transmisión de trama datos
t_p : tiempo de propagación ~ longitud temporal del anillo
$t_{p'}$: tiempo de propagación al siguiente nodo

H : Cabecera trama de datos
H_{tk} : Cabecera token



Análisis de prestaciones (II)

Sean:

N estaciones equiespaciadas

Tramas de longitud constante

Se define $a = \frac{t_p}{t_t}$

Tiempo de transmisión de trama normalizado ($t_t = 1$).

Tiempo de propagación (t_p) necesario en recorrer el anillo, incluidos repetidores:

$$a = t_p$$

Diferentes estrategias en la **liberación del testigo**:

- **Con liberación temprana:** se realiza la transmisión inmediatamente después de la anterior, sin esperar la propagación de la trama anterior. Evidentemente, se tiene que cumplir:

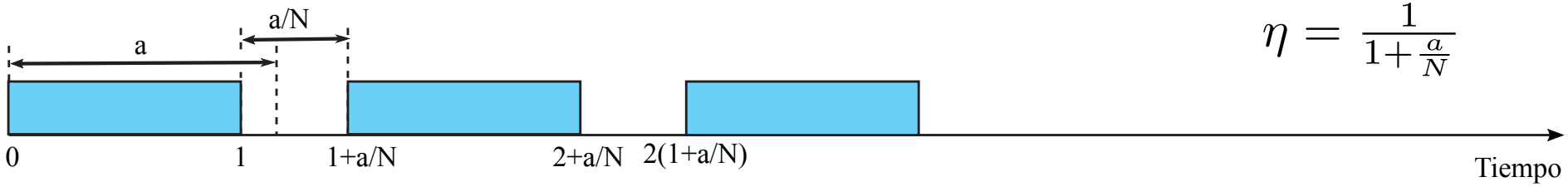
$$t_p > t_t \rightarrow a > 1$$

- **Sin liberación temprana:**
  1. Espera que retornen los primeros bits de la trama al origen.
  2. Espera que retorne la trama entera al origen.

Análisis de prestaciones (III)

Liberación temprana de token (sup. a > 1)

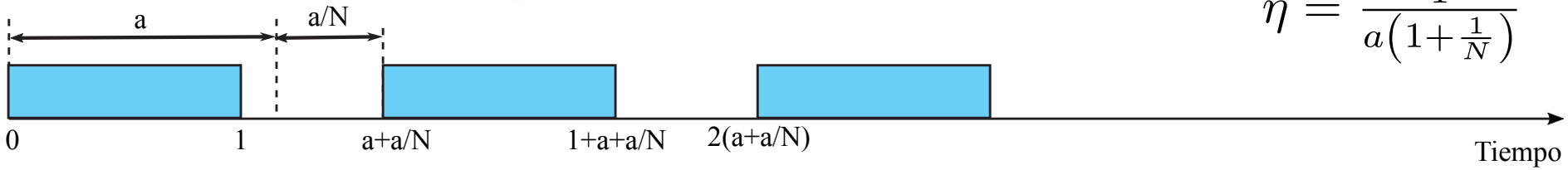
Transmisión de token al finalizar la transmisión de la trama anterior.



$$\eta = \frac{1}{1+\frac{a}{N}}$$

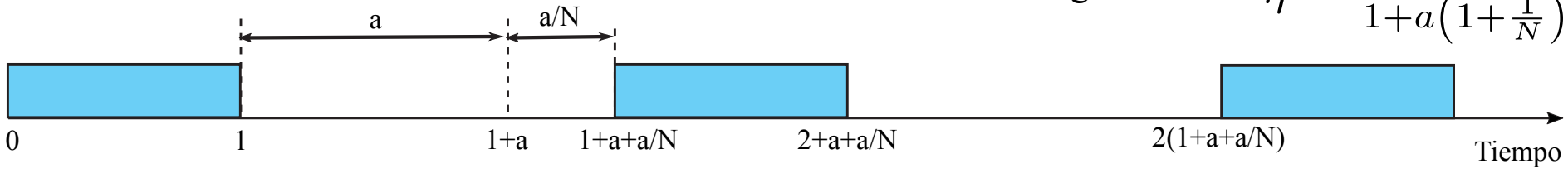
Sin liberación temprana de token (sup. a > 1)

Transmisión de token cuando los **primeros** bits de la trama alcanzan el origen.



$$\eta = \frac{1}{a\left(1+\frac{1}{N}\right)}$$

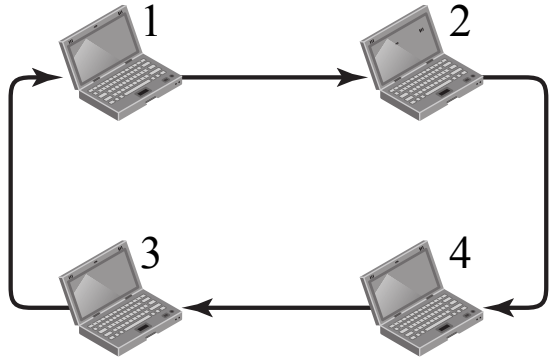
Transmisión de token cuando **todos** los bits de la trama alcanzan el origen.



$$\eta = \frac{1}{1+a\left(1+\frac{1}{N}\right)}$$

Topologías (I)

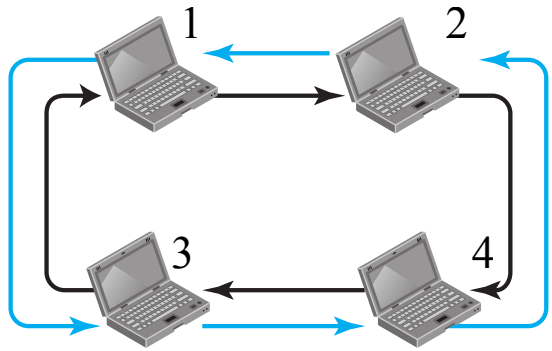
Anillo físico:



- Cuando una estación envía a su sucesor, el token no puede ser visto en otra estación; el sucesor es el siguiente en la línea física, por lo que el token no tiene que tener la dirección del siguiente sucesor.
- El problema con esta topología es que si alguno de los enlaces del medio falla, el sistema entero falla.

Topología dual:

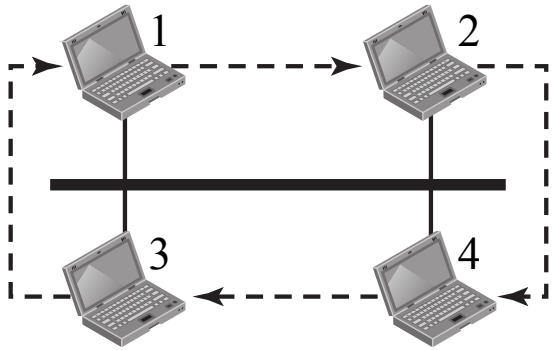
- Utiliza un segundo anillo (auxiliar) que opera en sentido contrario al anillo principal, y sólo para situaciones de emergencias.
- Si alguno de los enlaces de la red principal falla, automáticamente combina los dos anillos de forma temporal.



- Cuando se restablece el enlace, la red auxiliar vuelve a su estado inactivo.
- En esta topología, cada estación necesita dos puertos transmisores y dos puertos receptores.
- FDDI (*Fiber Distributed Data Interface*) y CDDI (*Copper Distributed Data Interface*).

Topologías (II)

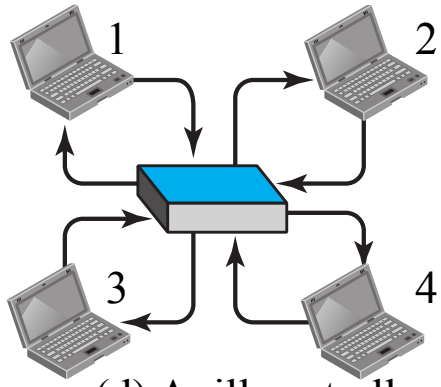
Anillo bus:



(c) Anillo bus

- También denominada, **token bus**.
- Las estaciones se conectan mediante un cable: **bus**.
- Conforman un anillo lógico porque cada estación conoce la dirección del **sucesor** y **predecesor**.
- Cuando una estación finaliza su envío, libera el token e inserta la dirección del sucesor en el token.
  - Sólo la estación que su dirección coincida con la dirección destino del token adquiere el token y consigue acceso al medio.
  - IEEE 802.4 Bus LAN.

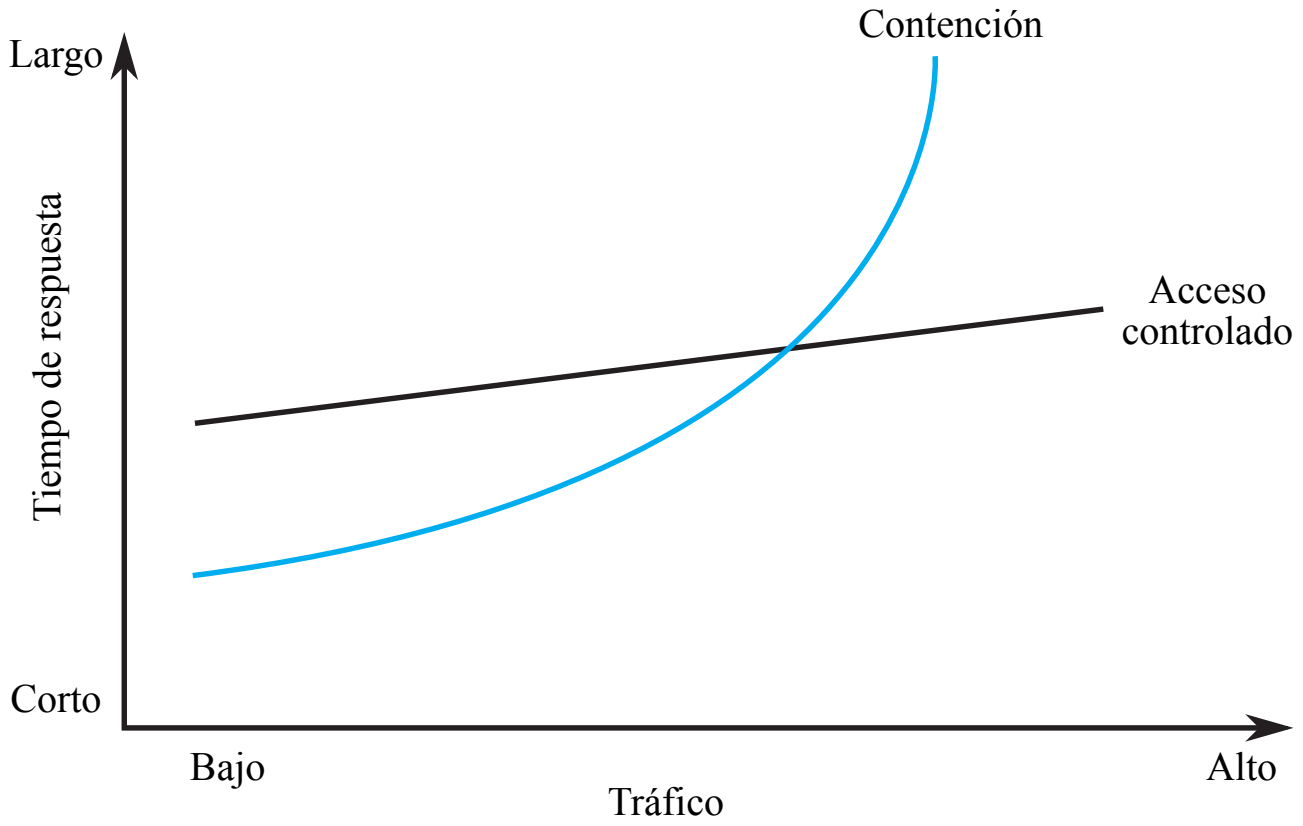
Anillo estrella:



(d) Anillo estrella

- También denominada **token ring**.
- La topología física es una estrella.
- El hub central actúa como conector, al que se conectan las estaciones mediante conexiones dobles.
- Incorporación de estaciones es sencilla.
- Debido al hub, la caída de un enlace no inutiliza toda la red.
  - IEEE 802.5 Ring LAN.

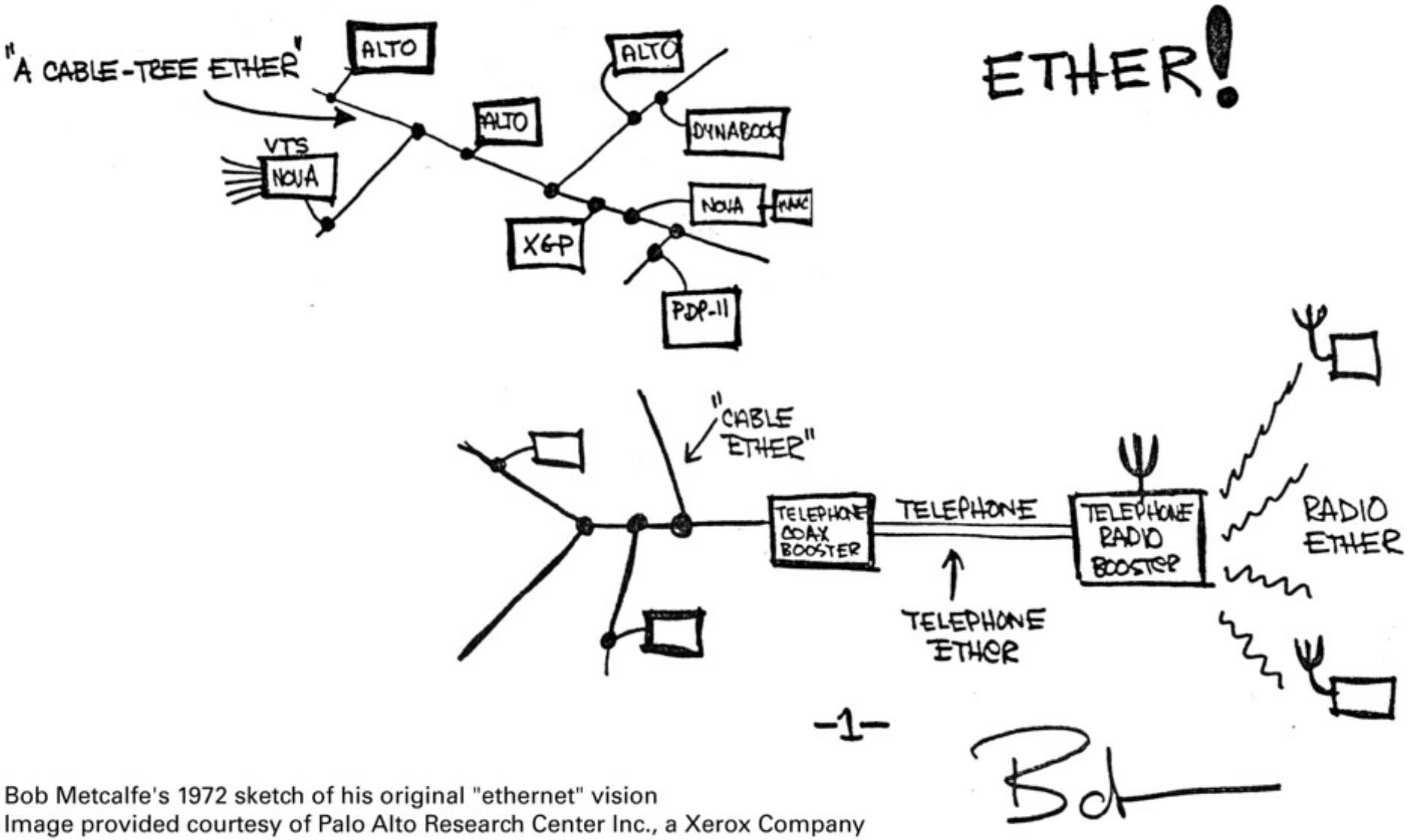
Acceso controlado vs contención



Control de acceso al medio

1. Introducción
2. Protocolos de acceso aleatorio
3. Protocolos de acceso controlado
4. ***Familia Ethernet***
5. Redes inalámbricas
6. Dispositivos de interconexión

Ethernet



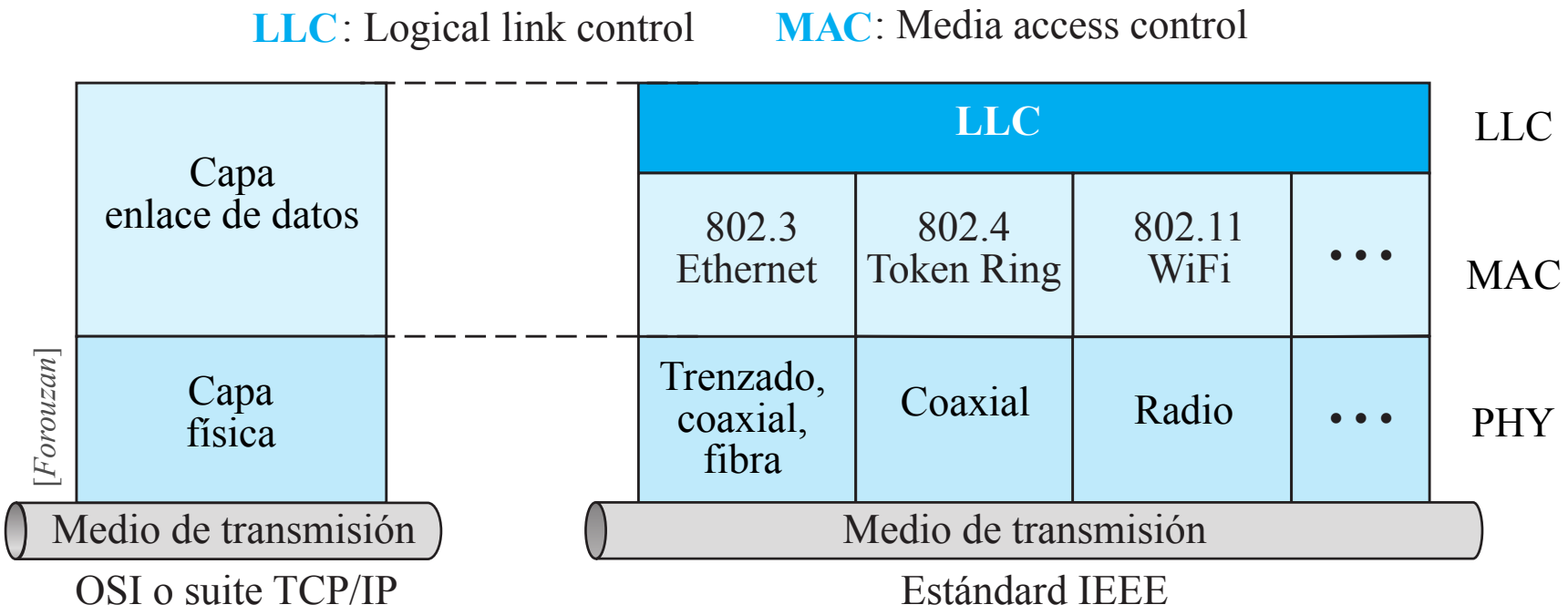
Bob Metcalfe's 1972 sketch of his original "ethernet" vision
Image provided courtesy of Palo Alto Research Center Inc., a Xerox Company

Proyecto IEEE 802

En 1985, IEEE Computer Society inicia el **Proyecto IEEE 802**, para establecer unos estándares de comunicación entre equipos de diferentes fabricantes.

El **Proyecto IEEE 802** no pretende sustituir ninguna parte del modelo OSI o de la suite TCP/IP, sino que, es una forma de especificar y estructurar las funciones de las capas física y enlace de datos en la mayoría de protocolos de LANs.

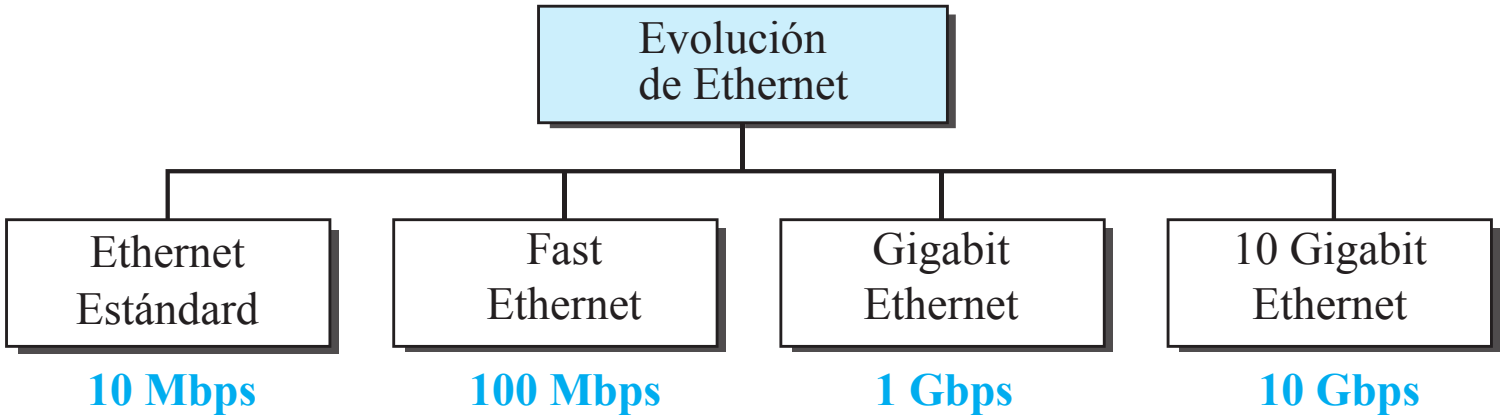
LLC y MAC



IEEE 802.3 divide la capa enlace en dos subcapas:

- **LLC (Logical link control):** maneja parte de las funciones del nivel enlace y proporciona interconectividad entre las diferentes LANS, haciendo transparente el subnivel MAC.
- **MAC (Medium Access Control):** IEEE 802 ha creado una subcapa MAC que define el acceso para cada método LAN: Ethernet, Token Bus, Token Ring, etc.

Evolución de Ethernet



Ethernet LAN fue desarrollada en 1970 por Robert Metcalfe y David Boggs.

Desde entonces, ha evolucionado a través de cuatro generaciones.

Nos referiremos a la Ethernet original de 10 Mbps como **Ethernet Estándard**.

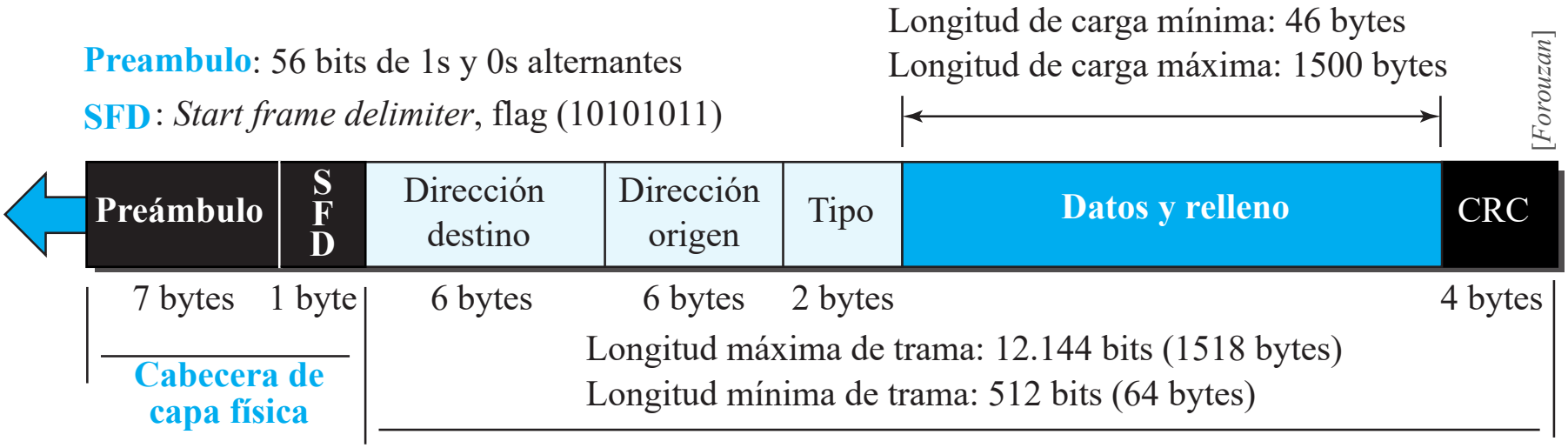
Aunque la mayoría de las implementaciones han evolucionado, hay algunas características de la Ethernet Estándard que aún permanecen.

Sin conexión y servicio no confiable

Algunas características sobre **conexión** y **servicio**:

- Proporciona servicio **sin conexión**: cada trama se envía de forma independiente la trama anterior o de la siguiente.
- Ethernet tampoco establece conexión ni desconexión.
- **Best-effort:** la estación envía una trama en cuanto la tiene disponible, el receptor puede o no estar disponible para recibirla.
  - ✓ Además, el emisor puede saturar a la estación receptora, por lo que se producirán descartes de paquetes.
  - ✓ Los descartes de tramas Ethernet no se informan al emisor.
  - ✓ Igualmente, si una trama se descarta por error en CRC, tampoco se informa al emisor.

Formato de trama Ethernet



Preámbulo: 7 bytes (56 bits) de 0s y 1s alternantes que alertan a la estación receptora de la llegada de una trama. Además permite la sincronización de relojes. Es parte de la capa física y no forma parte de la trama.

Start frame delimiter (SFD): 1 byte: 10101011. Informa a la estación receptora de la última oportunidad para sincronizarse. Los dos últimos bits (11) alertan que la dirección destino viene a continuación. El campo SFD también forma parte de la capa física.

Destination address (DA): 6 bytes (48 bits). Contiene la dirección física (también denominada hardware) del dispositivo al que va dirigida la trama.

Source address (SA): 6 bytes (48 bits). Contiene la dirección física del dispositivo del que procede la trama.

Type: Define el protocolo de nivel superior del paquete encapsulado en la trama Ethernet: IP, ARP, OSPF, etc.

Data: Datos encapsulados de nivel superior. Mínimo 46 bytes y máximo de 1500 bytes. Si el mensaje de nivel superior es superior a 1500 bytes, habrá sido segmentado en más de una trama. Por el contrario, si es inferior a 46 bytes, habrá sido rellenado (padding) con 0s.

CRC: Contiene información para detección de error, CRC-32, sobre los campos dirección, tipo y datos.

Longitud de trama

Ethernet impone restricciones a los tamaños mínimos y máximos de trama:

El tamaño **mínimo** de trama es necesario para la detección de colisiones en CSMA/CD:

- La trama Ethernet necesita una **longitud mínima de 512 bits (64 bytes)**, y parte de esta longitud es la cabecera y la cola.
- Si la cabecera son 18 bytes (6 bytes de dirección destino, 6 bytes de dirección origen, 2 bytes de del campo tipo y 4 bytes de CRC), entonces, la longitud mínima de datos de nivel superior deben ser $64 - 18 = 46$ bytes.
- Si los datos de nivel superior es menor a 46 bytes, se realiza el relleno (*padding*).

El estándard define un tamaño **máximo de 1518 bytes** (sin preámbulo y SFD).

- Por tanto, si restamos la cabecera y la cola, tenemos que la longitud máxima de carga es $1518 - 18 = 1500$ bytes.
- Si el mensaje de nivel superior es mayor de esta longitud, se produce **segmentación**.

La restricción de longitud máxima procede de dos **razones históricas**:

1. Cuando Ethernet fue desarrollado, la memoria era muy cara, por lo que la restricción de la longitud máxima ayudaba a reducir el tamaño del buffer.
2. Para prevenir que una estación monopolizara el medio compartido, bloqueando otras estaciones que tuvieran datos para enviar.

Direccionamiento

Cada estación Ethernet tiene su propia NIC (*network interface card*), localizada en su interior y con una dirección de nivel de enlace.

La dirección Ethernet se conoce como **dirección física**.

La dirección Ethernet son 6 bytes (48 bits), normalmente escritos en hexadecimal, separados por guión. Por ejemplo:

`4A:30:10:21:10:1A`

La forma en la que la dirección se envía es diferente a como se escribe: *la transmisión es de izquierda a derecha, byte a byte; pero, para cada byte, primero se envía el bit menos significativo, y al más significativo se envía la final.*

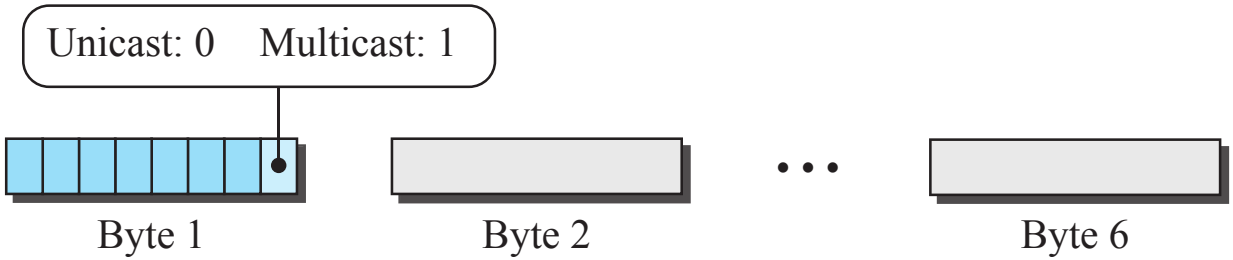
Sea la dirección `47:20:1B:2E:08:EE`, entonces:

Hexadecimal		47	20	1B	2E	08	EE
Binario		01000111	00100000	00011011	00101110	00001000	11101110
Transmitido	←	11100010	00000100	11011000	01110100	00010000	01110111

La forma en transmitir los bits dirección ayuda a detectar inmediatamente si el paquete es unicast o multicast.

Dirección: *unicast*, *multicast* y *broadcast*

La dirección **origen** es siempre unicast: *una trama sólo puede proceder de una estación.*



- Si el bit menos significativo del primer byte es 0, la dirección es **unicast**:

```
                    4A:30:10:21:10:1A
0100 1010:0011 0000:0001 0000:0010 0001:0001 0000:0001 1010
```

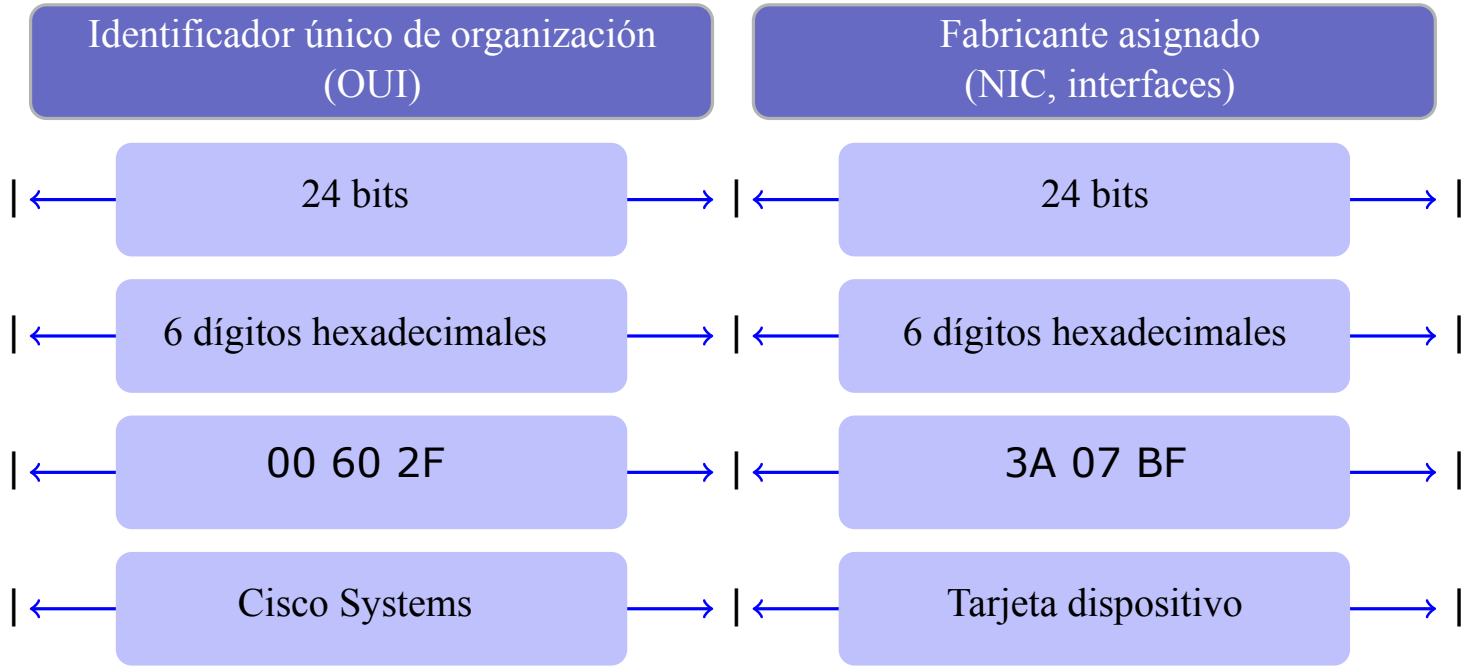
- De otro modo, es **multicast**:

```
                    47:20:1B:2E:08:EE
0100 0111:0010 0000:0001 1011:0010 1110:0000 1000:1110 1110
```

- La dirección **broadcast**:

```
                    FF:FF:FF:FF:FF:FF
1111 1111:1111 1111:1111 1111:1111 1111
```

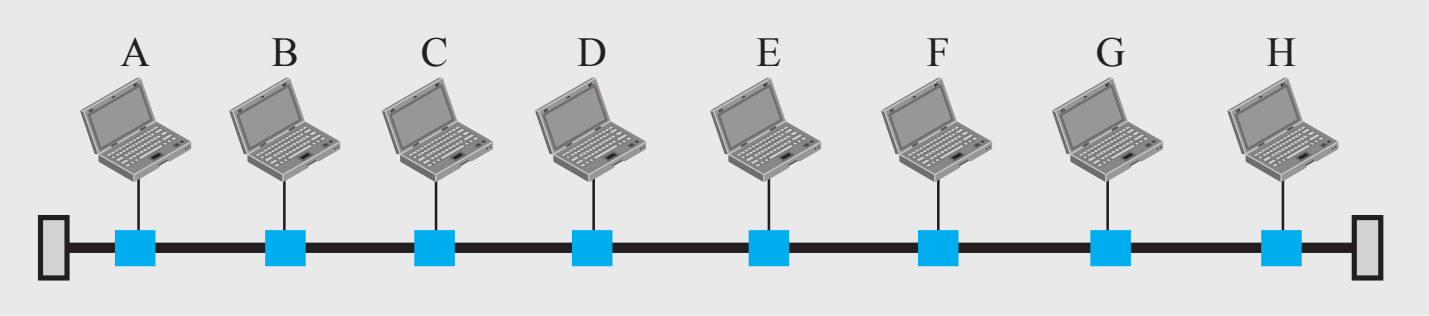
Ethernet: dirección MAC (*Media access control*)



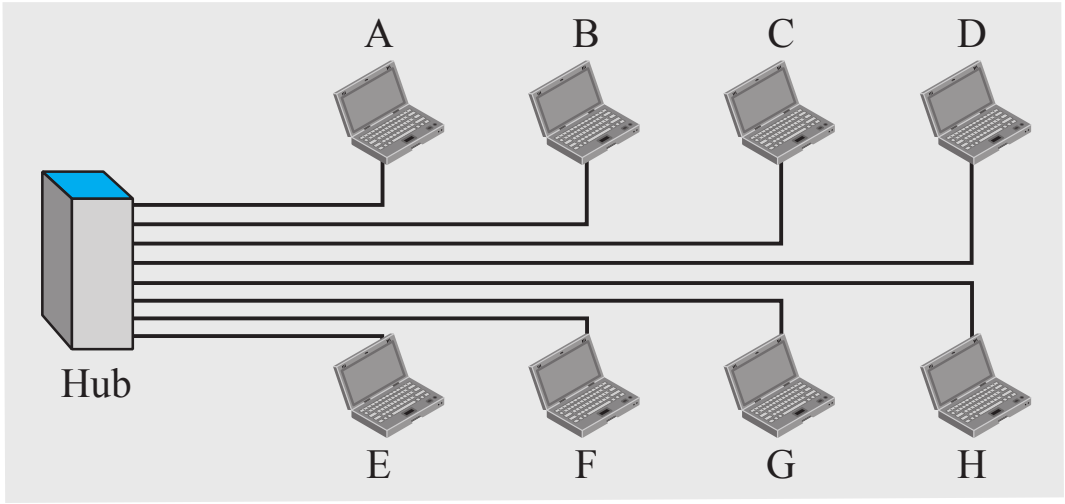
Algunas representaciones MAC:

```
00-60-27-3A-07-BF
00:60:27:3A:07:BF
0060.273A.07BF
```

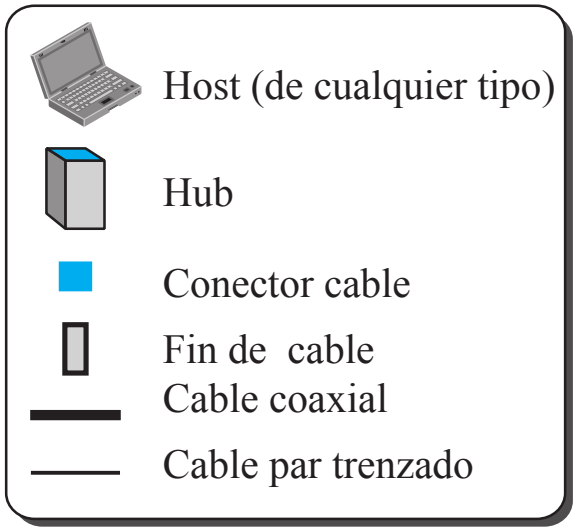
Implementación de Ethernet estándard



(a) LAN con topología bus utilizando cable coaxial



(b) LAN con topología estrella utilizando hub



[*Forouzan*]

Unicasting, multicasting y broadcasting

Ethernet standard utiliza cable coaxial (**topología bus**) o cable par trenzado con un hub (**topología estrella**).

Independientemente que el destino de las tramas sea una dirección unicast, multicast o broadcast, en la Ethernet standard, **la transmisión de las tramas siempre es broadcasting**. En la topología anterior, si la estación A envía una trama a B, entonces:

- En topología **bus**, la trama viaja por todo el bus, y todas las estaciones reciben la trama.
- En topología **estrella**, el hub recibe la trama, y como es un dispositivo pasivo, no chequea la dirección destino, regenera los bits y los envía por todos los puertos, excepto por el que ha llegado (inundación de la red).

¿Cómo se distinguen las tramas unicast, multicast y broadcast?

Todas las estaciones reciben todas las tramas, pero según la forma en que las estaciones guardan o descartan las tramas:

- **Unicast:** sólo la estación prevista guardará y gestionará la trama; el resto las descartarán.
- **Multicast:** sólo aquellas miembros del grupo las guardarán, el resto las descartarán.
- **Brodcast:** todas las estaciones (excepto el emisor) las guardarán y manejarán.

Método de acceso: *A* inicia la transmisión

1. Ethernet es una red **broadcast**, con acceso al medio **CSMA/CD 1-persistente**.
2. Supongamos que el dispositivo *A* envía una trama al dispositivo *D*.
3. En primer lugar, *A* debe chequear si el medio está libre (CSMA, detección de portadora), para ello, mide el nivel de energía del medio, durante un corto periodo de tiempo, normalmente menor que $100\ \mu s$. Si no hay señal en el medio, significa que no hay ninguna otra estación transmitiendo (o que la señal no ha llegado todavía hasta *A*). El dispositivo *A* interpreta como medio libre, por lo que inicia el envío de la trama.
4. Si el nivel señal fuera superior a cero, significa que el medio está ocupado, y quedaría monitorizando de forma continua hasta que el medio quedara libre durante $100\,\mu$s, y entonces, iniciaría la transmisión.
5. La estación *A* mantiene copia en el buffer de la trama hasta asegurarse que no hay colisión.
6. El chequeo del medio continua después de que *A* ha iniciado las transmisión de la trama. Estación *A* necesita enviar y recibir contínuamente. Pueden ocurrir dos casos: transmitir con **éxito** (adquisición del medio) o **colisión**.

Método de acceso: captura del medio

Si la estación A envia 512 bits y no ha detectado colisión, entonces está segura que la trama ha recorrido todo el medio sin colisión, y por lo tanto, detiene la detección del medio.

¿De dónde procede la cantidad de 512 bits?

Si suponemos una tasa de transmisión de Ethernet de 10 Mbps, entonces para transmitir al medio 512 bits tardará:

$$\frac{512\,\text{bits}}{10\,\text{Mbps}} = 51{,}2\,\mu\text{s}$$

Si la velocidad del cable es $2 \times 10^8\,\text{ms}^{-1}$, entonces, en ese tiempo, el primer bit habrá recorrido $10240\,\text{m}$ (o sólo $5120\,\text{m}$ con ida y vuelta), habrá colisionado con un bit de la estación más alejada y habrá vuelto.

En otras palabras, si la colisión hubiera ocurrido lo habría hecho en el tiempo de enviar 512 bits (peor caso) y el primer bit habría recorrido $5120\,\text{m}$.

Si la colisión se hubiera producido en medio del cable, la colisión se habría detectado antes.

Se supone que la longitud del cable es $5120\,\text{m}$. Actualmente, el estándard reduce la distancia a la mitad, $2500\,\text{m}$, para ampliar el margen de seguridad.

Método de acceso: colisión

Estación A **ha detectado una colisión** antes del envío de 512 bits: alguno de los bits previos ha colisionado con algún bit de otra estación.

Hay que detener inmediatamente el envío de datos y mantener la trama en el buffer para reenviar cuando el medio esté disponible. Además, se informa de la colisión al resto de estaciones mediante el envío de una **señal de colisión** (*jam*) de 48 bits.

Después de enviar la señal de colisión, las estaciones incrementan el valor de K (número de intentos). Si después del incremento, $K = 15$, el medio está demasiado ocupado, la estación aborta la transmisión y comienza de nuevo.

Si $K < 15$, la estación tiene que esperar un tiempo de backoff (T_B), para ello, la estación crea un número aleatorio entre 0 y $2^K - 1$, por lo tanto, cada vez que se produce una colisión, el número aleatorio se incrementa exponencialmente:

- Después de la 1ª colisión ($K = 1$), el número aleatorio está en el rango $[0, 1]$.
- Después de la 2ª colisión ($K = 2$), el número aleatorio está en el rango $[0, 1, 2, 3]$.
- Después de la 3ª colisión ($K = 3$), el número aleatorio está en el rango $[0, 1, 2, 3, 4, 5, 6, 7]$.

por lo tanto, después de cada colisión, la probabilidad de aumentar el tiempo de backoff se incrementa. Es lógico, ya que después de la 3ª, 4ª y sucesivos intentos sigue produciéndose colisión, significa que la red está realmente congestionada y necesita más tiempo de backoff.

Eficiencia de la Ethernet estándard

Eficiencia de la Ethernet estándard (I)

Supongamos una Ethernet en condiciones de carga pesada y constante:

- k estaciones siempre listas para transmitir,
- probabilidad p constante de transmisión en cada ranura, y,
- tiempo de propagación en el medio t_p.

Sea el suceso $S_1 = \{$*Adquirir canal durante una ranura*$\}$, entonces, la probabilidad de S_1:

$$A = P(S_1) = \binom{k}{1} p(1-p)^{k-1} = kp(1-p)^{k-1}$$

donde, A es máximo cuando $p = 1/k$, sabiendo que:

$$\lim_{k\to\infty} A = \frac{1}{e} \tag{1}$$

Sea el suceso $S_2 = \{$*Intervalo de contención tenga exactamente j ranuras*$\}$, entonces, la probabilidad de S_2:

$$B = P(S_2) = A(1-A)^{j-1}$$

Si el número medio de ranuras por contención:

$$\mu = E[B] = \sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{A}{1-A}\sum_{j=0}^{\infty} jA(1-A)^{j} = \frac{A}{1-A} \times \frac{1-A}{A^2} = \frac{1}{A} \tag{2}$$

si cada ranura tiene una duración de $2t_p$, entonces, el intervalo medio de contención:

$$\omega = 2t_p\mu = \frac{2t_p}{A} \tag{3}$$

A partir de (1) y (2) se deduce que $\mu \leq e$, y sustiyendo en (3), se obtiene el intervalo de contención óptimo:

$$\omega \leq 2et_p \approx 5{,}42t_p \tag{4}$$

Eficiencia de la Ethernet estándard (II)

Sea t_t el tiempo de transmisión en condiciones de tráfico elevado, es decir, con intervalo de contención, definido en (4). Entonces, el rendimiento de Ethernet estándar:

$$\eta_{Ethernet} = \frac{t_t}{t_t + \omega} = \frac{t_t}{t_t + \frac{2t_p}{A}}$$

Si suponemos:

- Tiempo de transmisión de trama normalizado ($t_t = 1$).
- Tiempo de propagación normalizado al tiempo de transmisión ($a = t_p/t_t$).
- Y caso óptimo ($A = \frac{1}{e}$).

entonces[1]:

$$\boxed{\eta_{Ethernet} = \frac{1}{1 + 5{,}42a}}$$

[2] Otros modelos expresan la eficiencia de Ethernet como $\eta = {}^{1}/_{(1+6{,}4a)}$, el resultado es, prácticamente, similar.

Eficiencia de la Ethernet estándard (III)

Si definimos a en función de los parámetros de red:

F : longitud de trama,

B : ancho de banda,

L : longitud del cable,

C : velocidad de propagación

entonces:

$$t_t = \frac{F}{B} \qquad t_p = \frac{L}{C}$$

y considerando $\omega = 2et_p$, podemos redefinir la eficiencia de Ethernet:

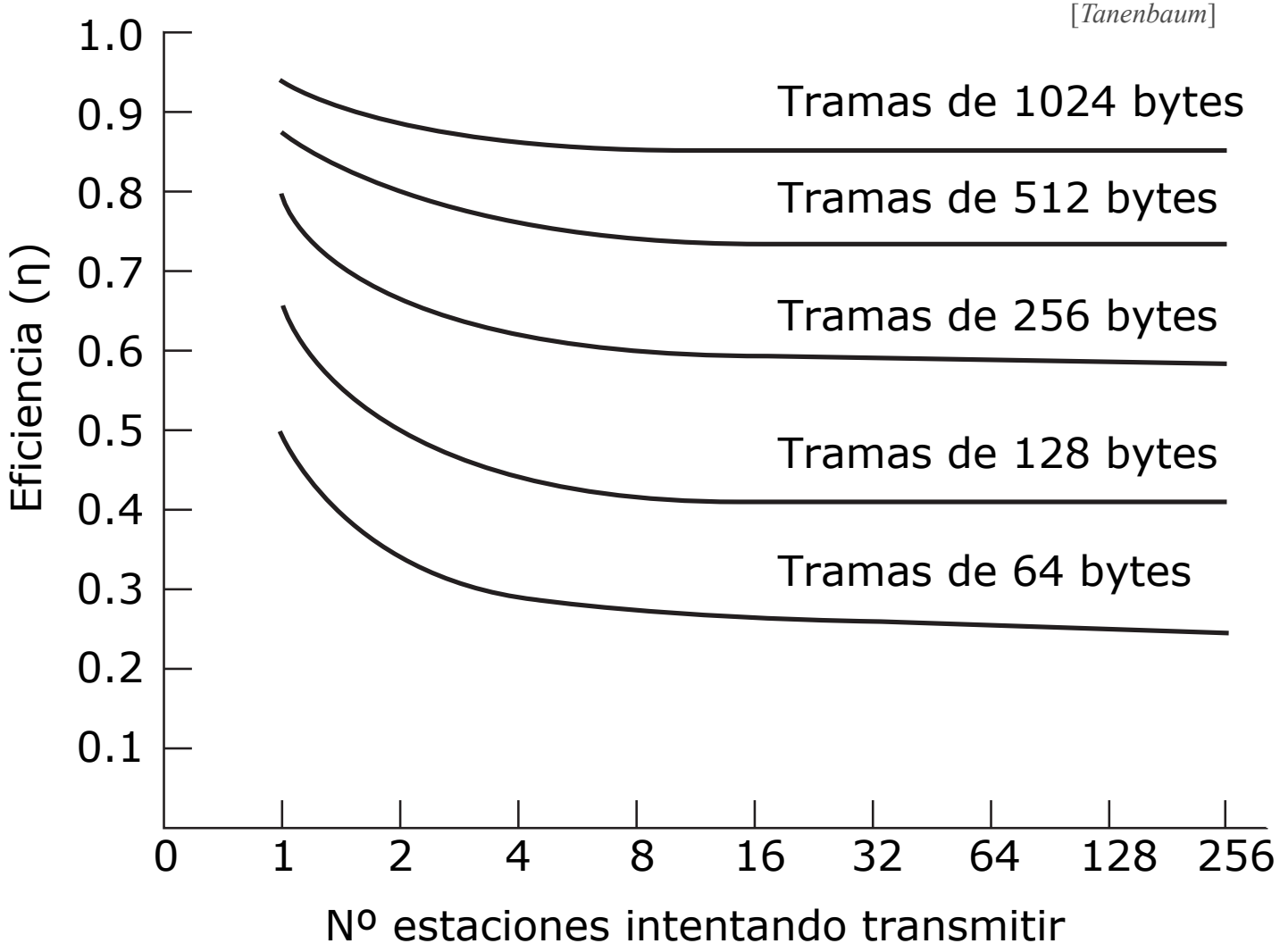
$$\eta_{Ethernet} = \frac{1}{1 + \frac{2BLe}{CF}}$$

De donde se obtienen las siguientes conclusiones:

- Debido a que la longitud del cable (L) influye mucho en el rendimiento (*a mayor longitud de cable, mayor intervalo de contención*) ⇒ Ethernet stándard especifica una longitud máxima de cable.
- Con el aumento del ancho de banda (B) o la distancia (L), disminuye la eficiencia ⇒ Ethernet estándard **NO** es la tecnología más apropiada para gran ancho de banda a grandes distancias (por ejemplo, redes MAN de fibra óptica).

Eficiencia de la Ethernet estandard (IV)

[*Tanenbaum*]



Implementaciones Ethernet estándard

Implementaciones Ethernet estándard

Fueron definidas varias implementaciones de Ethernet estándard, pero sólo cuatro de ellas tuvieron éxito durante la década de los 80.

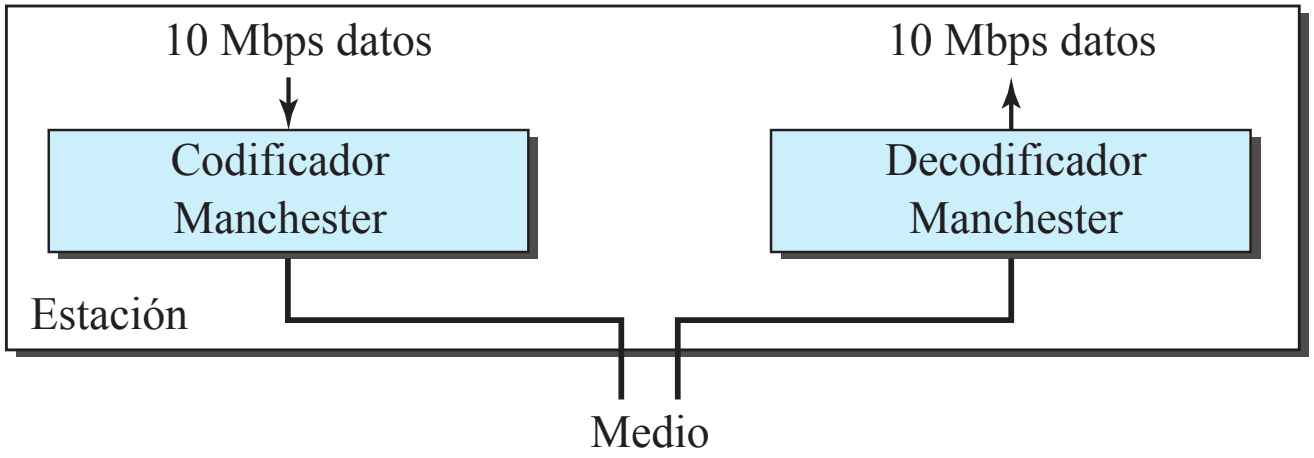
Implementación	*Medio*	*Longitud del medio*	*Codificación*
10Base5	Coaxial grueso	500 m	Manchester
10Base2	Coaxial fino	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fibra	2000 m	Manchester

La terminología **10BaseX** es la siguiente:

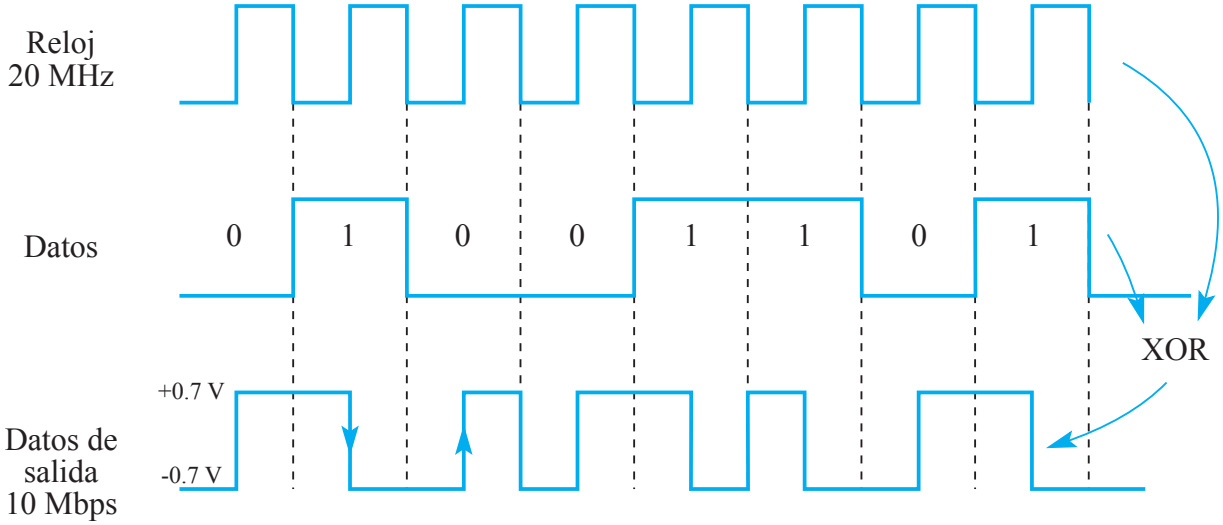
- *Base*, indica señal banda base (digital).
- *X*, define, aproximadamente, la longitud máxima del cable, expresado en 100 m, o el tipo de cable:
  - ✓ *T* para cable par trenzado no apantallado (UTP).
  - ✓ *F* para fibra óptica.

Ethernet estándard utiliza señal banda base, lo que significa que los bits se convierten a señal digital y transmitidos al medio.

Codificación Ethernet estándard

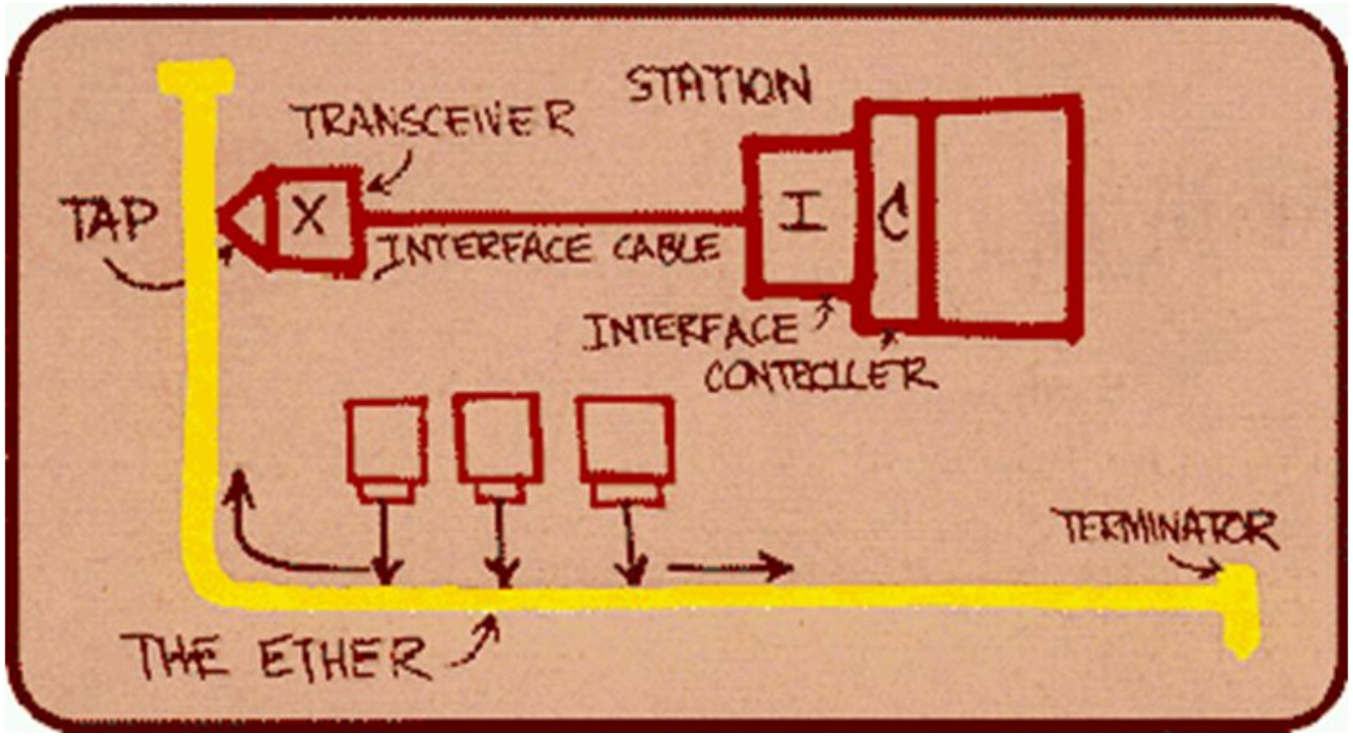


Los datos se convierten a señal digital mediante codificación **Manchester**.



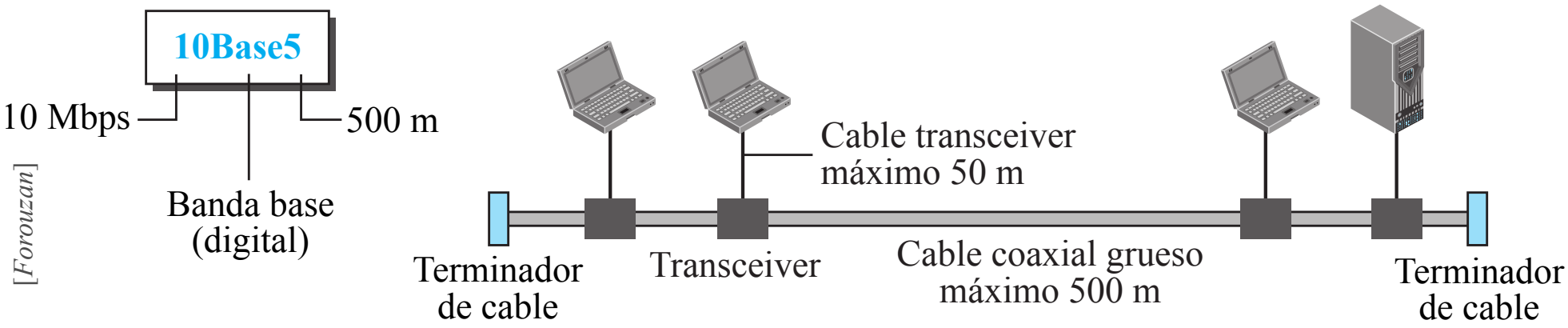
Manchester es **autosincronizada**: proporciona una transición en cada intervalo.

Ethernet estándard: origen



©Robert Metcalfe

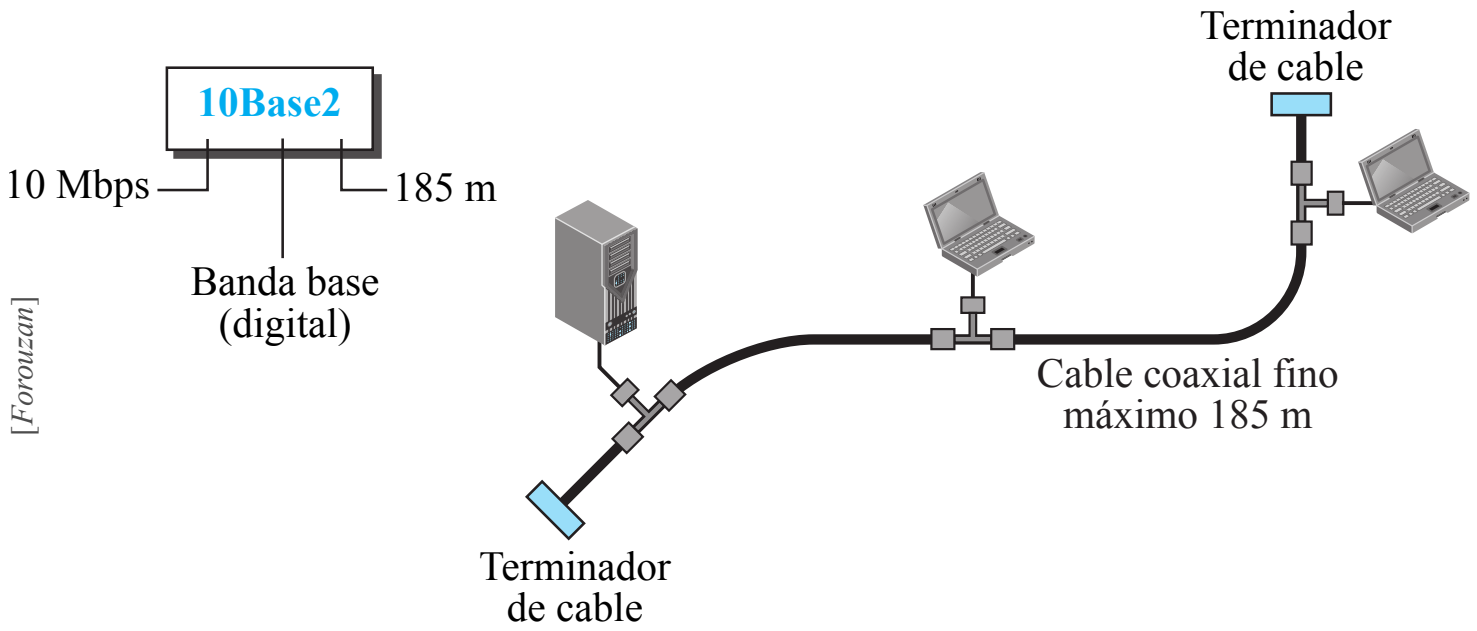
10Base5: Ethernet grueso (*Thick Ethernet*)



La **10Base5** o **Thick Ethernet**, fue la primera implementación de Ethernet Estándard:

- Su nombre procede del cable utilizado: coaxial grueso.
- Topología bus.
- El transceiver es el responsable de la transmisión, recepción y detección de colisiones.
- Las colisiones sólo pueden ser detectadas en el cable coaxial.
- Longítud máxima de segmento es 500 m.
- Distancias superiores, hasta 5 segmentos máximo, conectados mediante repetidores.

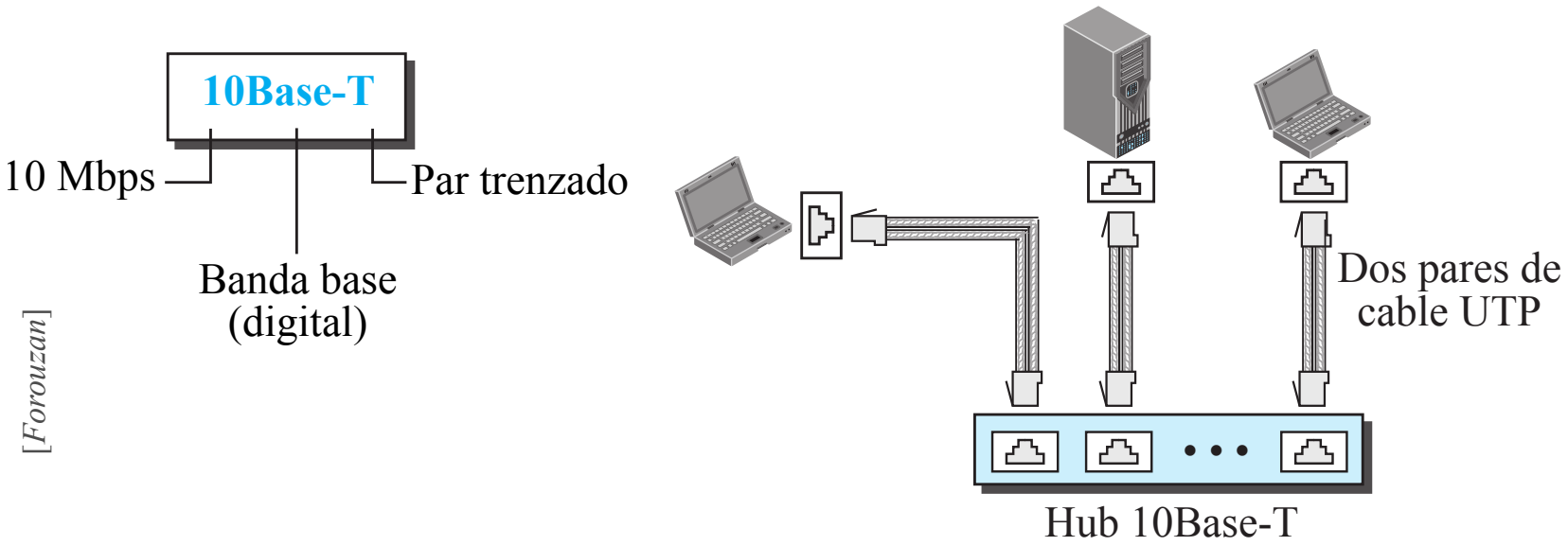
10Base2: Ethernet fino (*Thin Ethernet*)



La segunda implementación, **10Base2**, **Thin Ethernet** o **Cheapernet**:

- También utiliza topología bus, pero con cable mucho más fino y flexible.
- El cable puede ser doblado, pudiendo pasar muy cerca de las estaciones.
- El transceiver es parte de la tarjeta de red (NIC) e integrado en la estación.
- Es más económica que la 10Base5 debido a que el cable y los conectores BNC son más baratos que los taps.
- Instalación más fácil.
- Los segmentos no pueden exceder de 185 m. (cerca de 200 m) debido a la atenuación alta del cable coaxial fino.

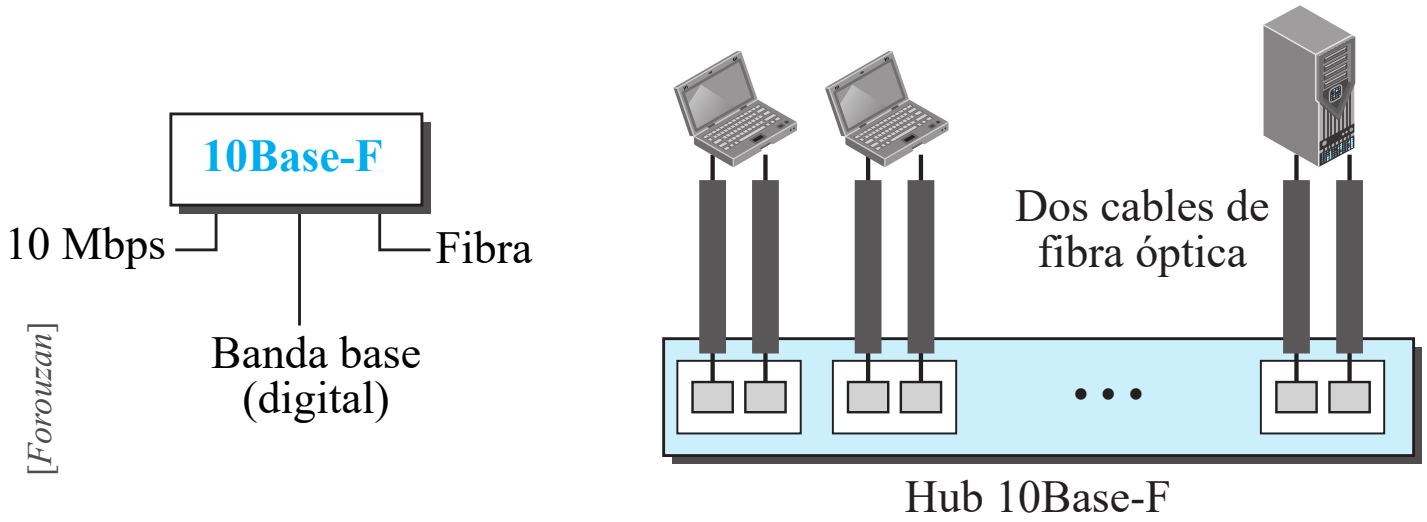
10BaseT: Ethernet par trenzado



La tercera implementación, **10BaseT**, **Ethernet par trenzado**:

- Utiliza topología física en estrella.
- Las estaciones se conectan al **hub** mediante par trenzado de dos pares.
- Mediante los dos pares UTP se crean dos caminos entre las estaciones y el hub (emitir y recibir), por lo que las colisiones se producen en el hub.
- Longitud máxima de segmento de cable de 100 m, para minimizar la atenuación del cable trenzado.
- El hub forma una estrella física y una topología lógica en bus.

10BaseF: Ethernet fibra óptica



Aunque hay varias implementaciones de Ethernet 10-Mbps fibra óptica, la más común se denomina **10BaseF**.

- Utiliza una topología estrella mediante un hub de fibra óptica.
- Las estaciones se conectan al hub mediante dos cables de fibra óptica (emisión y recepción).

Cambios en Ethernet Estándard

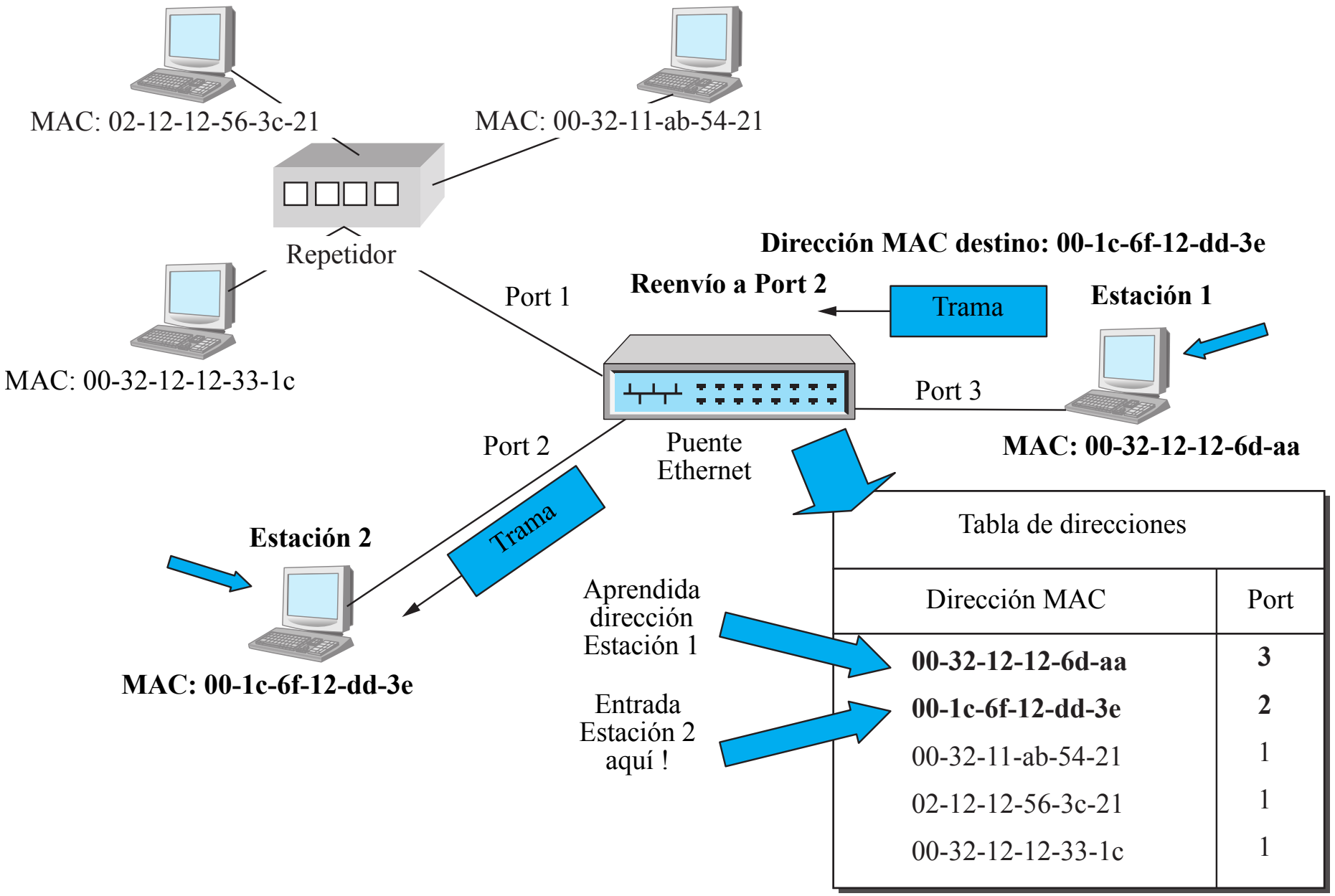
Ethernet con puentes

El primer paso en la evolución de Ethernet fue la división de LAN mediante **puentes** (bridges), que provoca dos efectos principales:

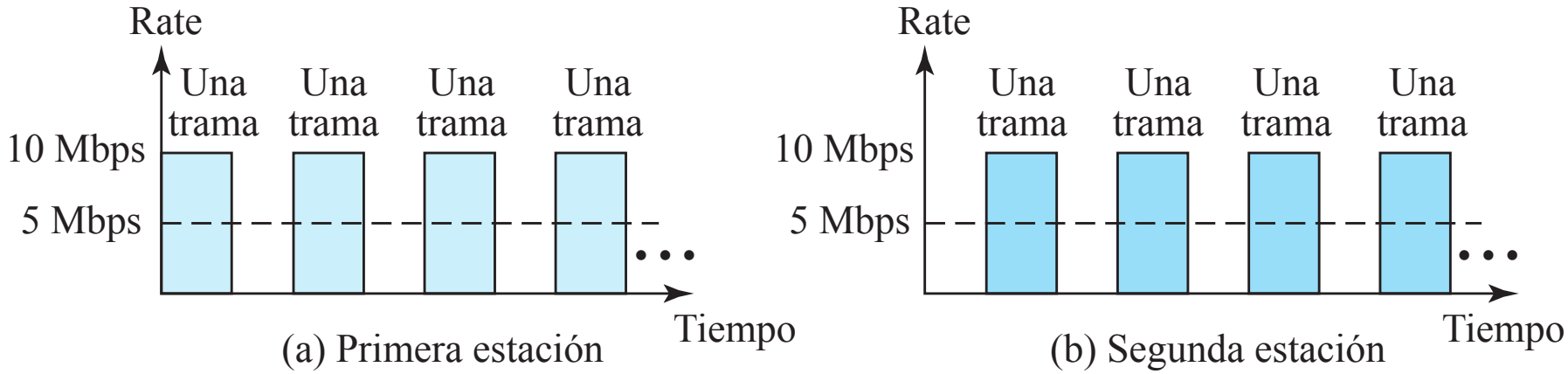
- El incremento de ancho de banda disponible.
- La separación de los dominios de colisión.

Puente transparente: aprenden de forma transparente de los dispositivos conectados a cada lado del puente.

Tablas MAC y aprendizaje en puentes transparentes



Medio compartido



En una Ethernet sin puentes, el total de la capacidad (10 Mbps) se reparte entre todas las estaciones con tramas para enviar.

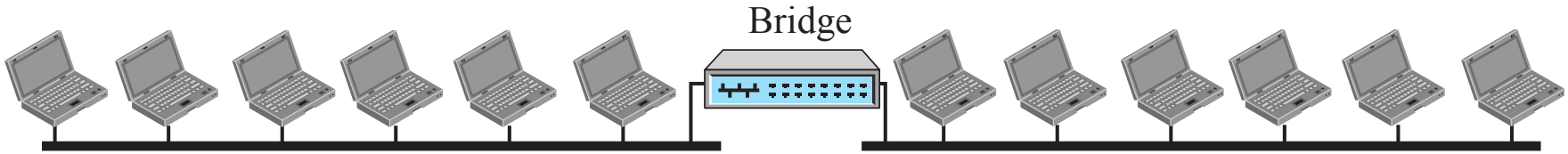
Si sólo hay una estación tiene tramas para enviar, se beneficia del total de la capacidad.

Pero si hay más de una estación, necesitan compartir el medio.

Por ejemplo, si hay dos estaciones con tramas para enviar, probablemente tendrán que hacer la transmisión de forma alternativa, por lo que, aproximadamente, podrán transmitir a una media de 5 Mbps.

Incremento de ancho de banda

(a) Sin bridging



(b) Con bridging

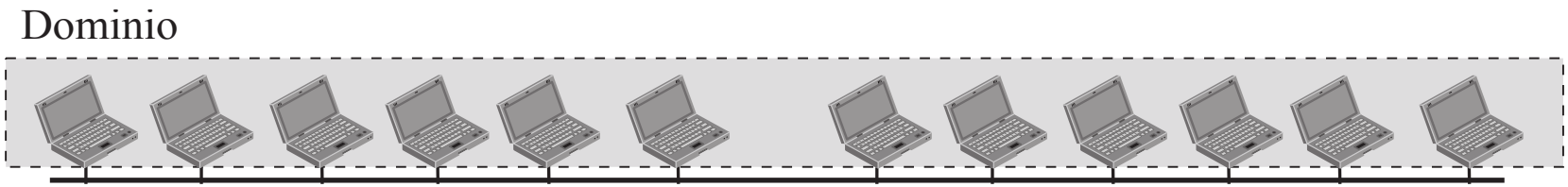
El **bridge** divide la red en dos o más segmentos.

El ancho de banda de cada segmento es independiente del resto.

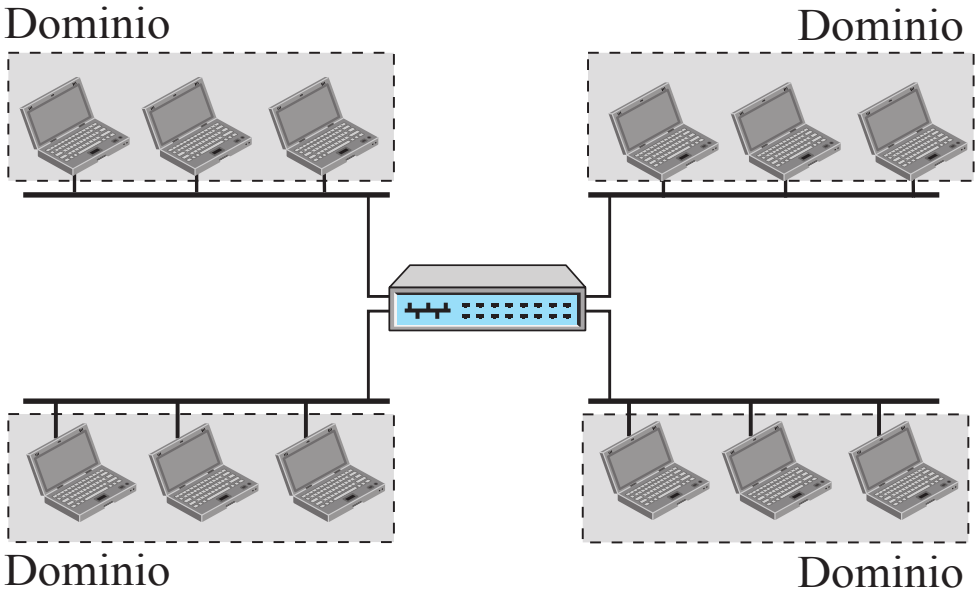
Por ejemplo, una red de 12 dispositivos dividida por un bridge en dos redes de 6 dispositivos. Ahora, cada segmento de red, dispone de 10 Mbps, por lo que la capacidad de cada segmento (10 Mbps) es compartida por las 6 estaciones (realmente 7, ya que el bridge es otro dispositivo).

Evidentemente, aumentando la división de la red, se puede ganar más ancho de banda para cada segmento.

Separación de dominios de colisión



(a) Sin bridging

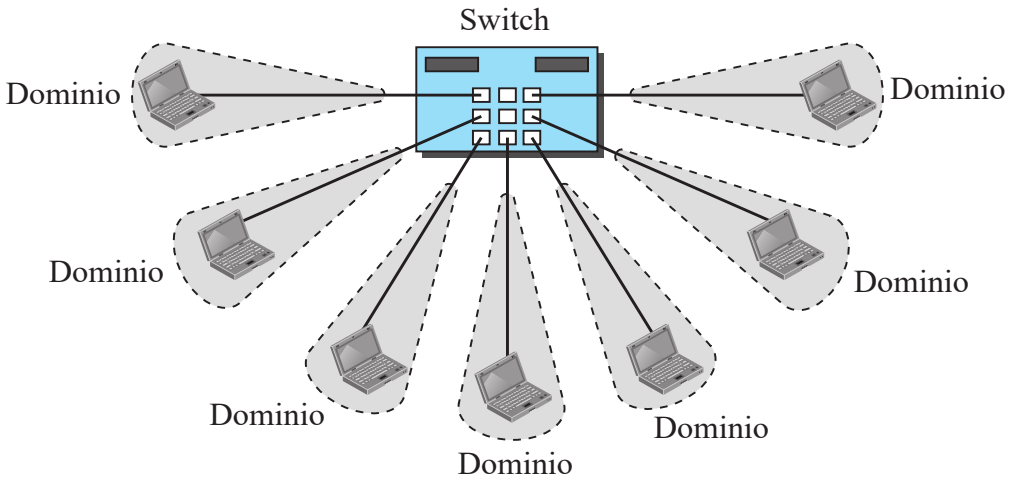


(b) Con bridging

Otra ventaja del uso de bridge es la **separación de los dominios de colisión**.

En dominios de colisión más pequeños, la probabilidad de colisión se reduce drásticamente: en una red sin bridge, 12 estaciones compiten por el medio; con bridging, sólo 3 estaciones compiten por el acceso al medio.

Ethernet conmutada (*switched*)



La idea de la LAN con puentes se puede extender a LAN conmutada: en lugar de tener dos o cuatro redes, etc...

¿Por qué no tener N redes donde N es el número de estaciones de la LAN?

La idea es disponer de un switch con N puertos, donde el ancho de banda sea compartido entre el switch y la estación (5 Mbps cada uno).

Además, el dominio de colisión es dividido en N dominios.

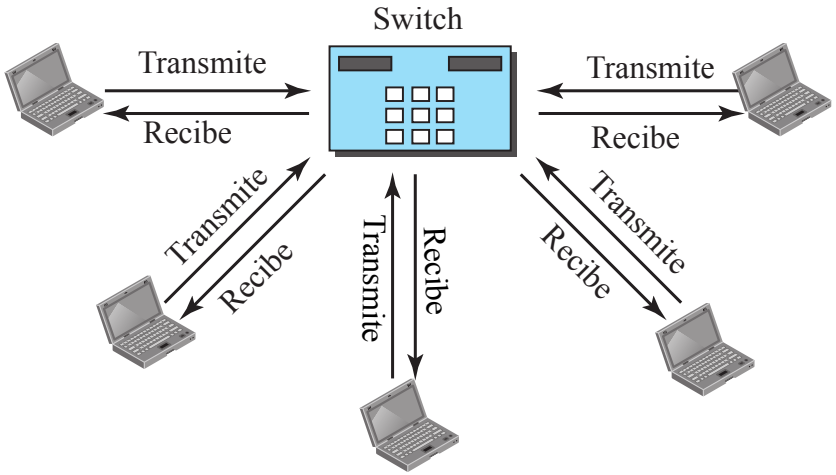
Un switch de capa-2 es un bridge de N–puertos con electrónica adicional que permite la conmutación rápida de paquetes.

La evolución de la Ethernet con puentes a **Ethernet conmutada** ha sido la clave para obtener una Ethernet mucho más rápida.

Ethernet full-duplex

Una de las limitaciones de 10Base5 y 10Base2 es que la comunicación es half-duplex (10Base-T es full-duplex), ya que una estación puede enviar o recibir, pero no pueden hacer las dos operaciones de forma simultánea.

El siguiente paso en la evolución es convertir Ethernet conmutada en **Ethernet conmutada full-duplex**, con lo que cada dominio de colisión pasa de 10 Mbps a 20 Mbps, utilizando dos enlaces, uno para enviar y otro para recibir.



En Ethernet conmutada full-duplex **ya no es necesario CSMA/CD**, ya que cada estación está conectada al switch por dos enlaces separados, y puede enviar/recibir, sin necesidad de detectar el medio, ni colisiones.

En este punto, **la subcapa MAC es deshabilitada**.

Y se dota a la Ethernet de la **Capa Control MAC**, localizada entre LLC y subcapa MAC, proporcionando control de flujo y error a la Ethernet conmutada full-duplex.

Fast Ethernet

En 1990, algunas tecnologías LAN con tasas de transmisión superiores a 10 Mbps, aparecieron en el mercado (FDDI y canal de fibra).

Para sobrevivir, Ethernet debía de llegar a tasas de 100 Mbps, y la nueva generación se le llamó **Fast Ethernet**.

Uno de los requisitos determinantes es que la nueva tecnología fuera compatible con Ethernet Estándard, motivo por el que la subcapa MAC permaneció sin cambios, lo que implica que el formato de trama y los tamaños máximos y mínimos se mantuvieron.

Los objetivos principales de Fast Ethernet fueron:

1. Actualizar la tasa de transmisión de datos a 100 Mbps.
2. Mantener la compatibilidad con Ethernet Estándard.
3. Mantener la dirección de 48 bits.
4. Mantener el formato de trama.

Fast Ethernet: autonegociación

Incorpora la **autonegociación**, que permite a las estaciones y hubs operar en un rango de capacidades, negociando el modo y tasa de transmisión:

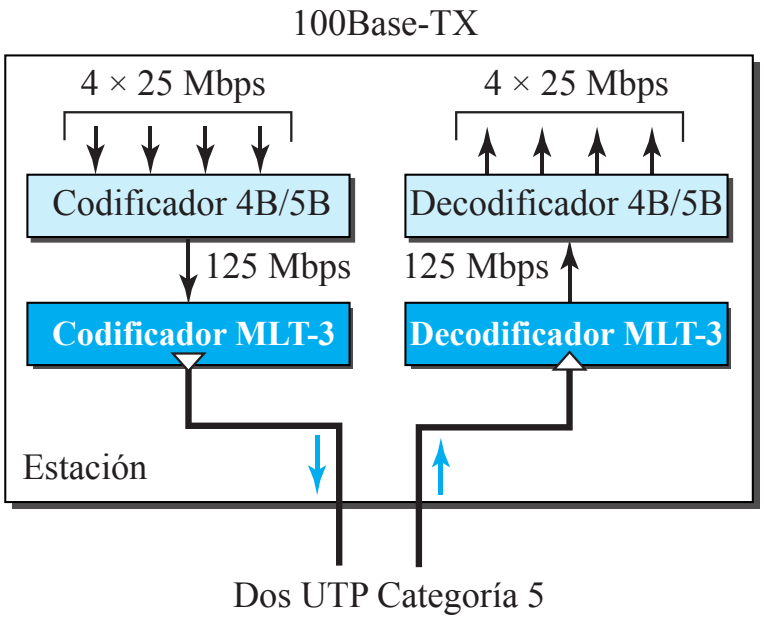
- Permitir la compatibilidad entre dispositivos.
- Permite la conexión de dispositivos de 10 Mbps y 100 Mbps, evidentemente, operando ambos a la menor tasa de transmisión.
- Permitir a un dispositivo disponer de múltiples capacidades.
- Permitir a un estación chequear la capacidad de un hub.

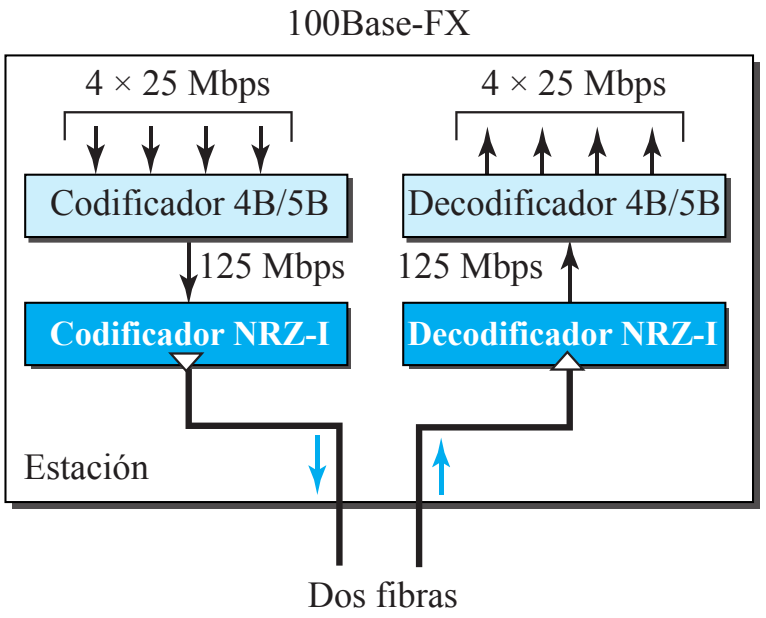
Fast Ethernet: Capa física (I)

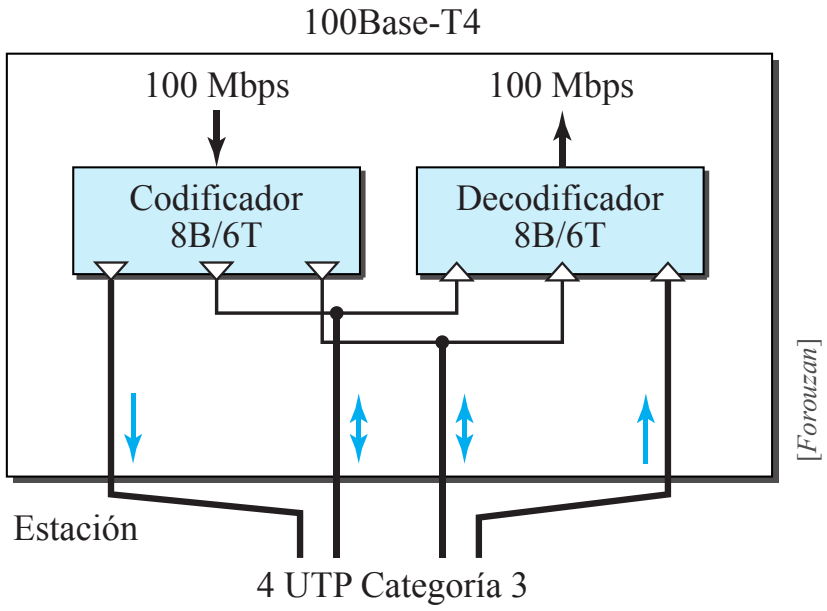
Para alcanzar los 100 Mbps, algunas cambios fueron necesarios a nivel físico:

- Fast Ethernet ha sido diseñado para conectar dos o más estaciones.
- Para dos estaciones, es suficiente con un cable punto a punto.
- Para más de dos estaciones, se necesita una topología estrella con un hub o switch en el centro.
- Puesto que la codificación Manchester necesita 200 MBaudios para tasas de transmsisión de 100 Mbps, no es lo más apropiado para un cable de par trenzado.
- Para las diferentes implementaciones se utilizaron diferentes esquema de codificación.

Fast Ethernet: Capa física (II)







Fast Ethernet: codificación

Implementación	*Medio*	*Longitud del medio*	*Hilos*	*Codificación*
100Base-TX	UTP o STP	100 m	2	4B/5B + MLT-3
100Base-FX	Fibra	185 m	2	4B/5B + NRZ-I
100Base-T4	UTP	100 m	4	Dos 8B/6T

100Base-TX:

- 2 pares de par trenzado (UTP o STP).
- Codificación MLT-3, y como no es auto-sincronizado, 4B/5B para prevenir errores de sincronización en largas cadenas de 0s ó 1s.

100Base-FX:

- 2 pares de fibra óptica.
- La fibra óptica puede manejar elevado ancho de banda, por lo que se utiliza NRZ-I.
- Para solventar los problemas de sincronización, a continuación se utiliza codificación 4B/5B, a tasas de 125 Mbps, aptas para fibra óptica.

100Base-T4:

- 100Base-TX proporciona 100 Mbps, pero requiere el uso de cable UTP Cat 5 o STP.
- 100 Base-T4, utiliza 4 pares de UTP Cat 3 a 100 Mbps.

  En este esquema, un par conmuta entre envío y recepción.

  Los otros 3 pares de UTP, sólo pueden manejar 75 Mbaud (25 Mbaud cada uno), por lo que se necesita un esquema que convierta 100 Mbaud a 75 Mbaud.

  Con 8B/6T, ocho elementos de dato son codificados en seis elementos de señal, lo que significa que 100 Mbps utiliza sólo $(6/8) \times 100\ Mbps = 75\ Mbaud$.

Gigabit Ethernet

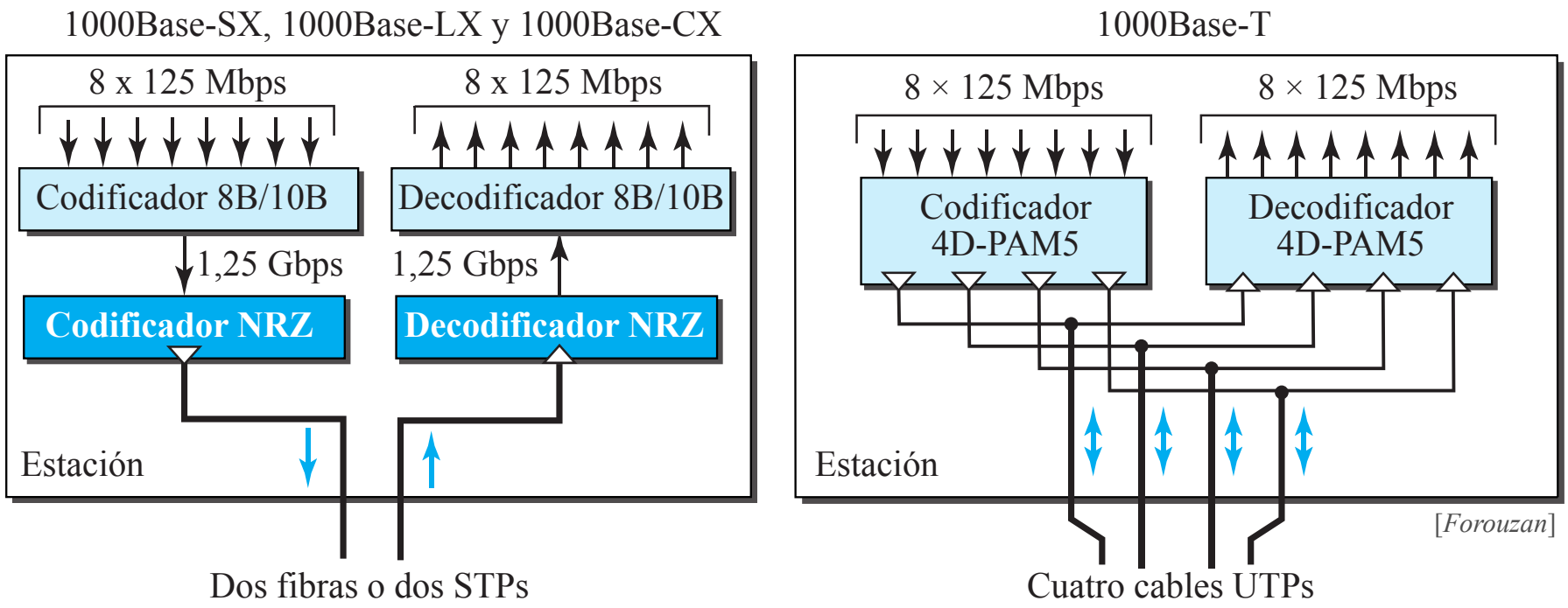
La necesidad del aumento de las tasas de transmisión resultó en el diseño del **Protocolo Gigabit Ethernet** (1000 Mbps).

Denominado IEEE 802.3z.

Los objetivos de Gigabit fueron:

1. Actualizar la tasa de transmisión de datos a 1 Gbps.
2. Mantener la compatibilidad con Fast Ethernet.
3. Mantener la misma dirección de 48 bits.
4. Mantener el mismo formato de trama.
5. Mantener la misma longitud mínima y máxima de trama.
6. Soportar la autonegociación definida en Fast Ethernet.

Gigabit Ethernet: medio físico y codificación



Gigabit Ethernet no puede utilizar Manchester porque es inviable para un ancho de banda tan elevado (2 GBaud).

Dos-hilos:

- Codificación NRZ.
- Para sincronización codificación en bloque 8B/10B, que previene la falta de sincronización en cadenas largas de 0s ó 1s, pero obtiene una tasa de 1,25 Gbps.
- Utiliza un hilo para enviar y otro para recibir.

4-hilos:

- No es posible tener 2 hilos para entrada y 2 hilos para salida, porque cada hilo necesitaría 500 Mbps, y excede la capacidad del UTP Cat 5.
- Solución: codificación 4D-PAMS, utilizado para reducir el ancho de banda, de forma que los cuatro cables que intervienen en el envío y recepción necesitan 250 Mbps, que es un rango apto para UTP Cat 5.

Gigabit Ethernet: resumen

Implementación	*Medio*	*Longitud del medio*	*Hilos*	*Codificación*
1000Base-SX	Fibra S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fibra L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

10 Gigabit Ethernet

Recientemente ha sido propuesto Ethernet para su uso en redes metropolitanas, extendiendo la tecnología, tasa de transmisión y distancia de cobertura de forma que Ethernet pueda ser utilizada como LAN y MAN.

IEEE ha creado la **10 Gigabit Ethernet**, denominada IEEE 802.3ae.

En resumen, los objetivos que del diseño de 10 Gigabit Ethernet son:

1. Actualizar la tasa de transmisión de datos a 10 Gbps.
2. Mantener el formato y tamaño de trama.
3. Permitir la interconexión entre LANs, MANs y WANs.

Implementación	*Medio*	*Longitud medio*	*Hilos*	*Codificación*
10GBase-SR	Fibra 850 nm	300 m	2	64B/66B
10GBase-LR	Fibra 1310 nm	10 Km	2	64B/66B
10GBase-EW	Fibra 1350 nm	40 kM	2	SONET
10GBase-X4	Fibra 1310 nm	300 m hasta10 Km	2	8B/10B

Las tasas de transmisión de 10 Gigabit sólo son posible con fibra óptica.

Evolución histórica de Ethernet (I)

Tecnología Ethernet	Fecha	⇒	Otras tecnologías LAN	Fecha
Ethernet	1985	⇒	Token Ring (IBM)	1989
Fast Ethernet	1995	⇒	FDDI (ISO)	1990
Gigabit Ethernet	1998	⇒	ATM (622 Mbps)	1997
10 Gigabit Ethernet	2002	⇒		
40 Gigabit Ethernet	2007	⇒		
100 Gigabit Ethernet	2016	⇒		
...	...	⇒		

Control de acceso al medio

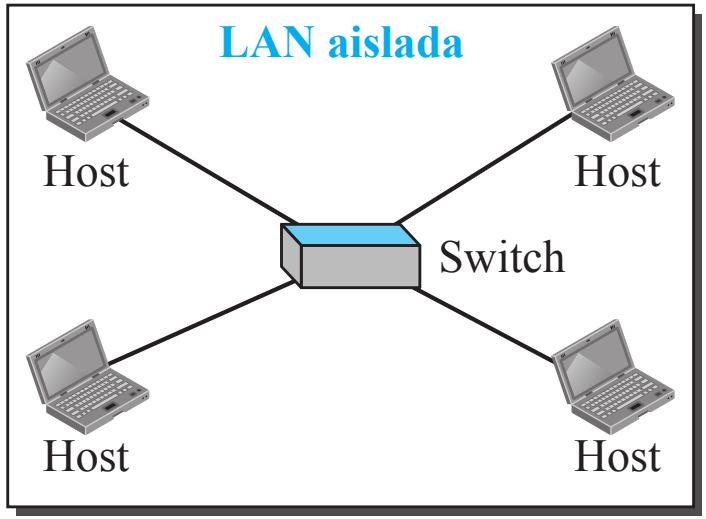
1. Introducción
2. Protocolos de acceso aleatorio
3. Protocolos de acceso controlado
4. Familia Ethernet
5. ***Redes inalámbricas***
6. Dispositivos de interconexión

Introducción a las LANs inalámbricas

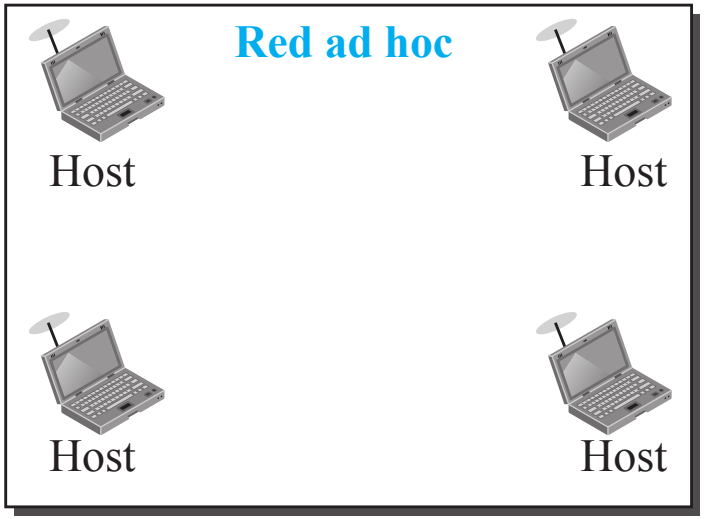
Elemento	**Cableada**	⇒	**Inalámbrica**
Medio	Cable, fibra óptica. Comunicación punto a punto. Full-duplex.	⇒	Aire. Señal broadcast, medio compartido
Hosts	Hosts siempre conectados. Mantiene dirección física y cambia dirección red.	⇒	Host no está conectado físicamente a la red, se puede mover líbremente.
Aislamiento LAN	En redes cableadas Ethernet, la LANs aislada se consigue mediante el switch de capa 2.	⇒	El equivalente es la red ad hoc, que es un conjunto de hosts que comunican libremente entre ellos. El concepto de switch de capa 2 no existe.
Conexionado	Se conectan con otras redes mediante routers	⇒	Con redes cableadas u otras redes inalámbricas

LANS cableadas vs inalámbricas

Aislamiento LANS:



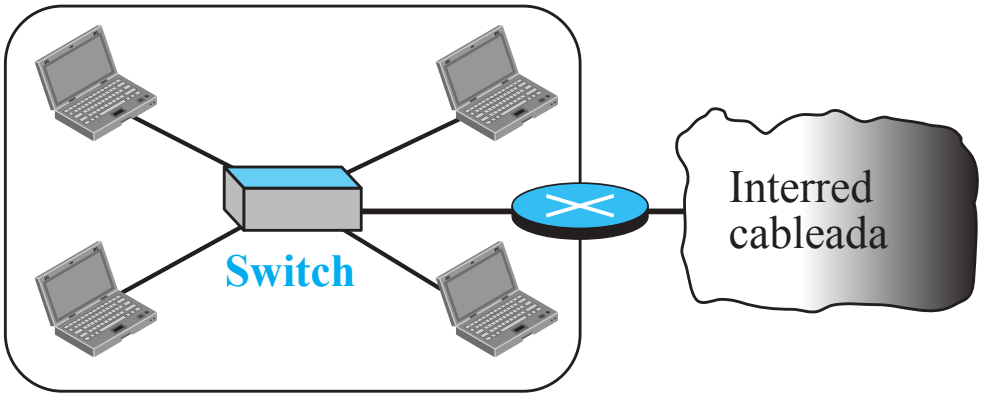
(a) Cableada



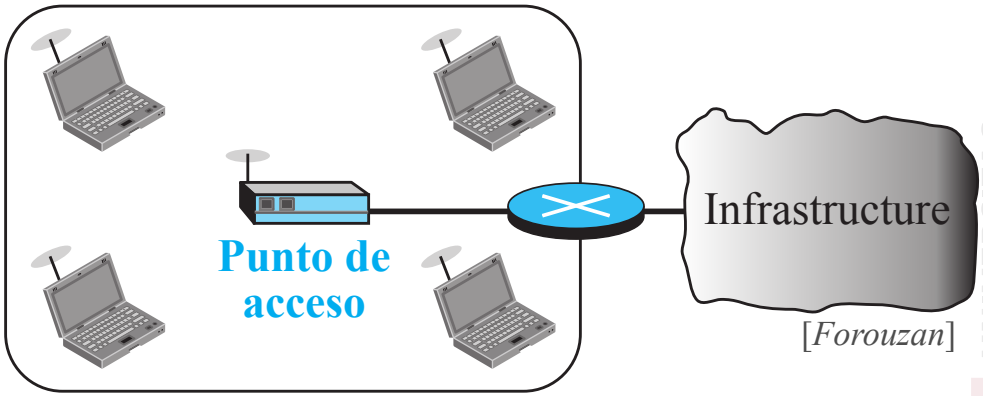
[Forouzan]

(b) Inalámbrica

Interconexión LANS:



LAN cableada



[Forouzan]

Infraestructura de red

Características de las redes inalámbricas

Hay algunas características específicas de las redes inalámbricas:

Atenuación: La potencia de la señal electromagéntica decrece rápidamente debido a que la señal se dispersa en todas las direcciones; sólo una pequeña porción alcanza el receptor.

La situación es más crítica en dispositivos móviles que operan con baterías y pequeñas fuentes de alimentación.

Interferencias: El receptor puede recibir señales de diferentes emisores que utilicen las mismas bandas de frecuencias.

Propagación multicamino: El receptor puede recibir más de una señal procedente del mismo emisor, debido a las reflexiones de la señal electromagnética en los obstáculos tales como vallas, paredes, suelo u objetos. El resultado puede ser una señal irreconocible.

Error: El control y detección de errores es un aspecto más crítico en redes inalámbricas que en cableadas.

Control de acceso

El método de acceso CSMA/CD, utilizado en redes cableadas, **no puede ser utilizado en redes inalámbricas**, por las siguientes razones:

1. Para detectar una colisión, los host necesitan enviar y recibir simultáneamente (enviar la trama y recibir la señal de colisión), lo que supone operar en modo full-duplex.

   Los host inalámbricos, alimentados con baterías, no tienen suficiente potencia, en general, para transmisión full-duplex.

   Sólo pueden emitir o recibir en cada instante.

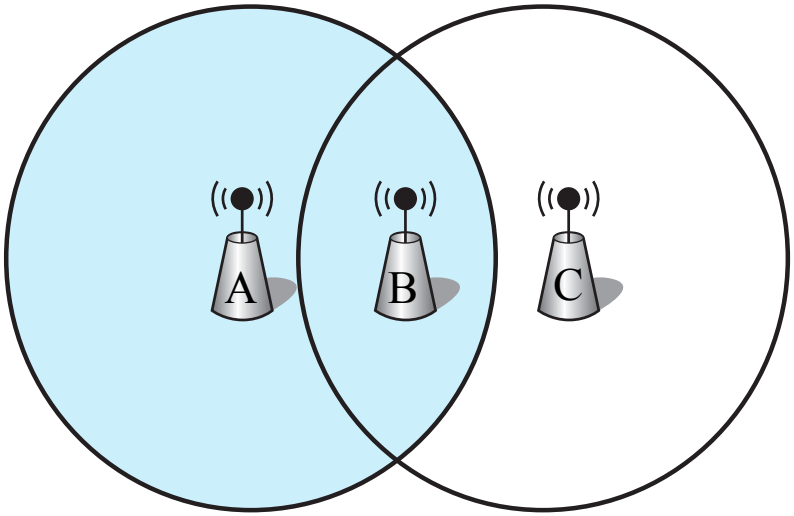
2. **Problema de la estación oculta**.

3. **Problema del nodo expuesto**.

4. La distancia entre estaciones puede ser considerable. La pérdida de señal puede impedir que una estación detectara una colisión producida en el otro extremo.

El problema de la estación oculta

Aunque las estaciones A y C están ocultas entre ellas, sus señales pueden colisionar en B.

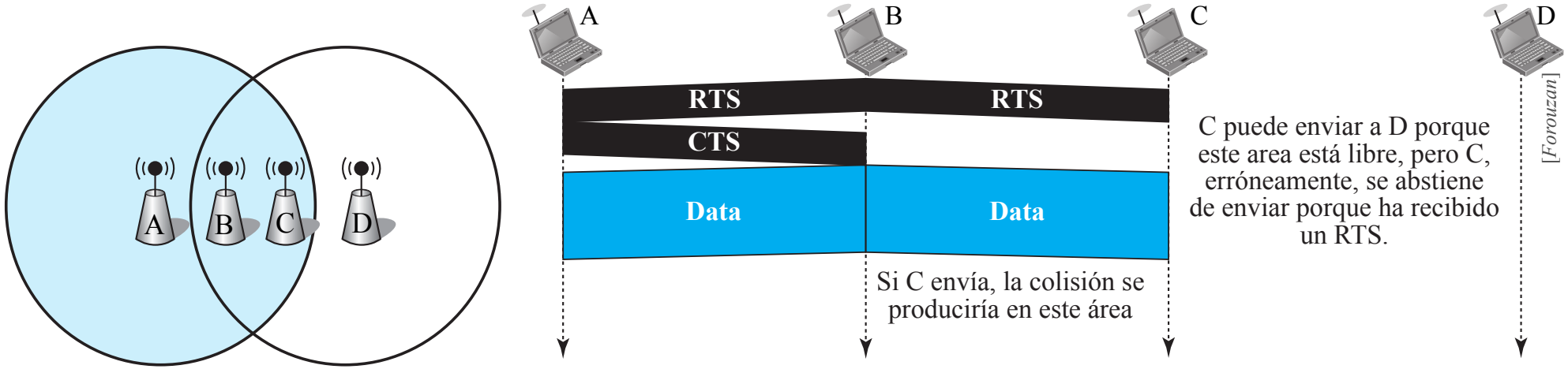


Supongamos:

- A y C, ambas en el rango de B, pero no entre ellas.
- A y C quieren comunicar con B y ambas envían una trama.
- Tanto A como C no son conscientes de la existencia de la otra, ya que sus señales no llegan tan lejos.
- Las tramas colisionarán en B.
- Los nodos A y C están **ocultos** entre sí.

El problema del nodo expuesto (I)

Aunque B y C están expuestas entre ellas a sus señales, no hay interferencia si B transmite a A mientras C transmite a D.



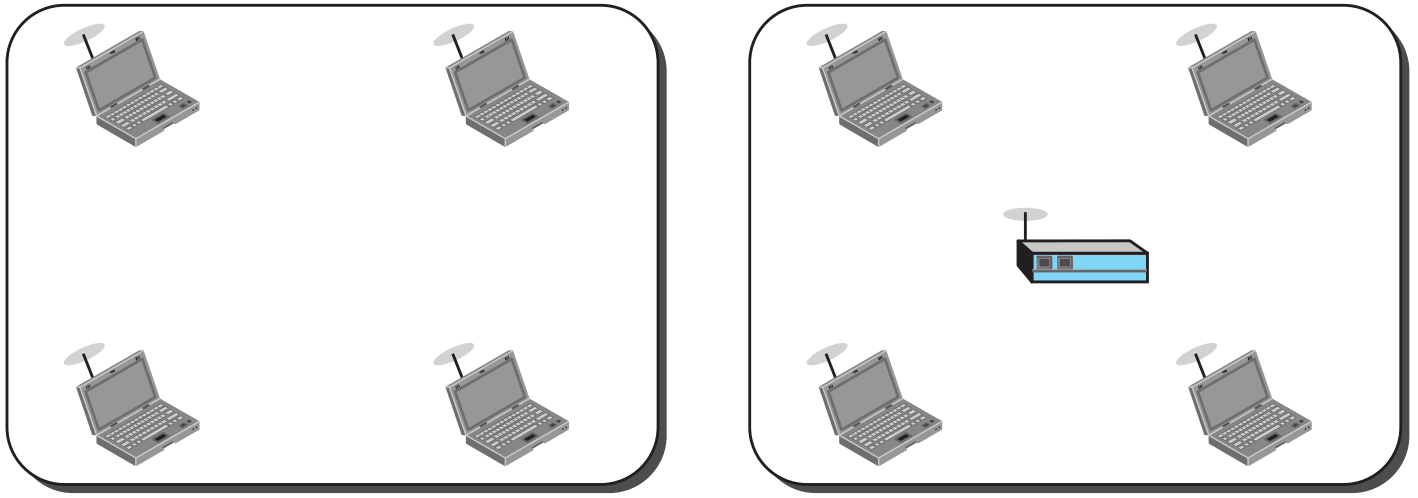
Supongamos:

- B está en el rango de A y C, pero no en el de D.
- C está en el rango de B y D, pero no en el de A.
- Suponga B envía una señal al nodo A.
- C es consciente de esta comunicación ya que escucha la comunicación de B.
- C determina que no puede transmitir porque el medio está ocupado (transmisión B).
- Pero es incorrecto porque la transmisión C-D no interferiría la comunicación A-B.
- El nodo C está **expuesto**.

IEEE 802.11

Arquitectura: Basic Service Set (BSS)

[*Forouzan*]



(a) ad hoc BSS (b) Infrastructure BSS

IEEE 802.11 define el **Basic Service Set (BSS)**, por ejemplo, bloques de edificios de una red wireless.

Está formada por estaciones fijas o móviles y una estación base central, conocida como Punto de Acceso (AP, Access point).

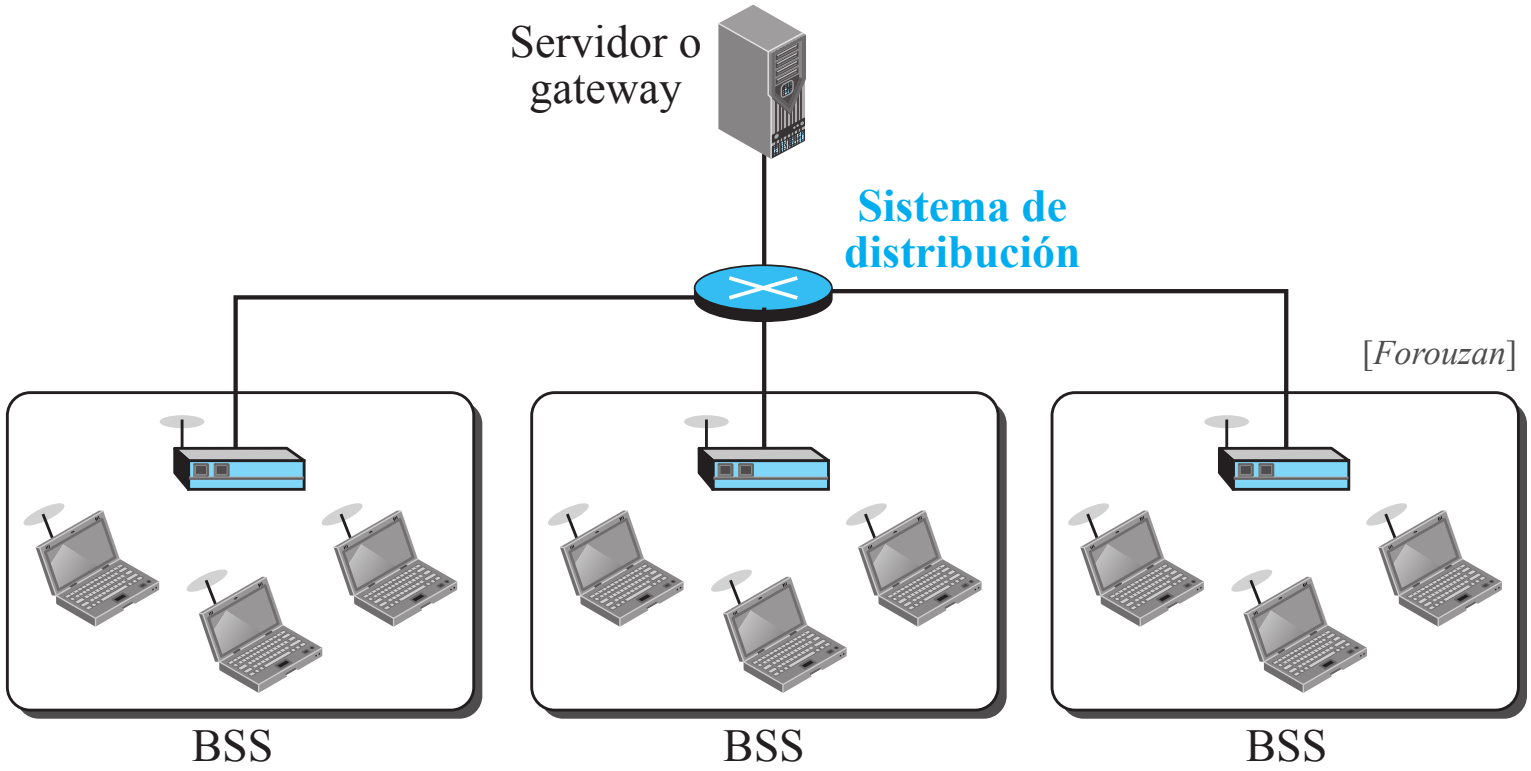
La BSS sin un AP es una red autónoma y no puede conectar con otras BSS.

Se denomina **Arquitectura ad hoc**.

En esta arquitectura, las estaciones pueden formar una red sin necesidad de AP.

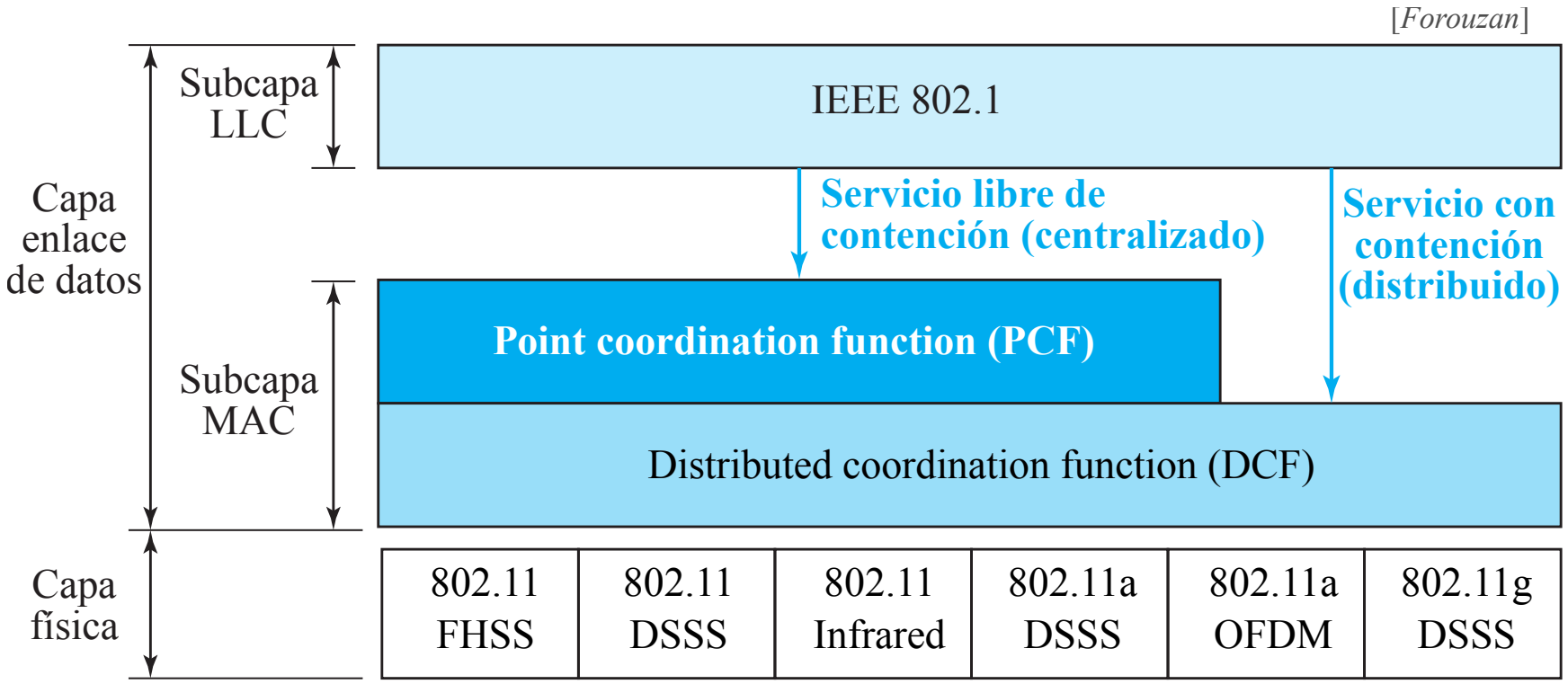
Una BSS con un AP se denomina **Infrastructure BSS (IBSS)**.

Arquitectura: Extended Service Set (ESS)



Subcapa MAC

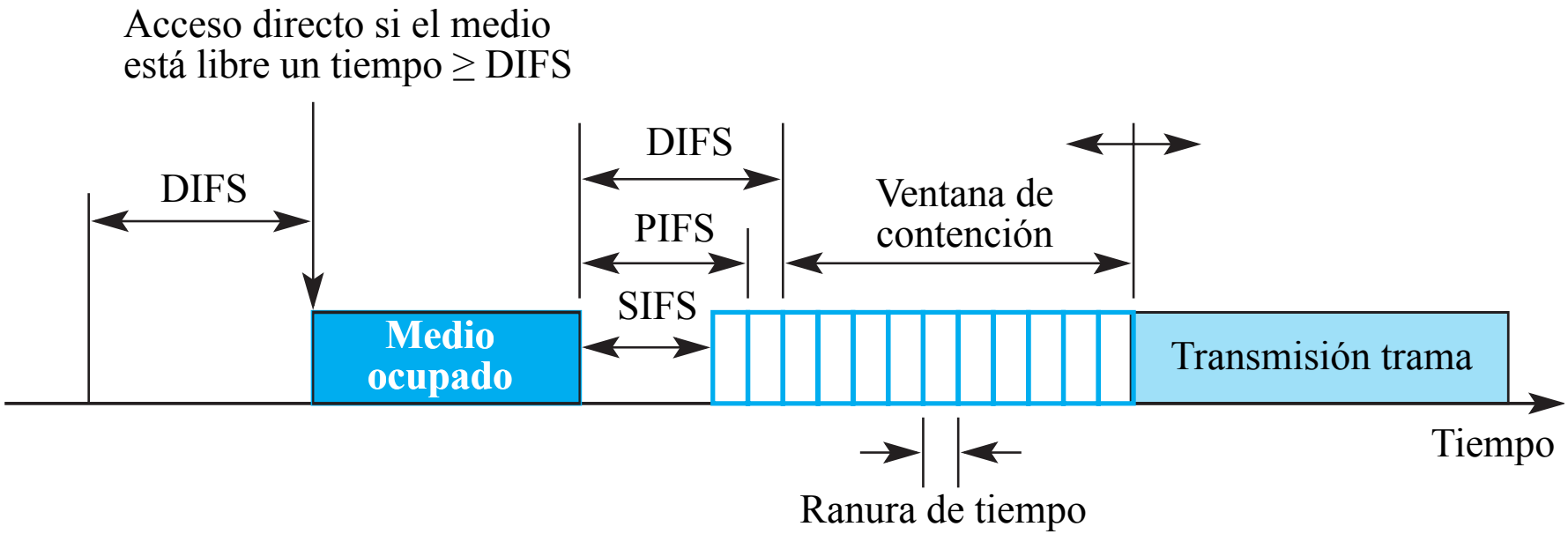
[*Forouzan*]



IEEE 802.11 define dos subcapas MAC:

- *Distributed coordination function (DCF).*
  1. DCF con CSMA/CA.
  2. DCF con RTS/CTS.
- *Point coordination function (PCF).*

Temporización en subcapa MAC 802.11



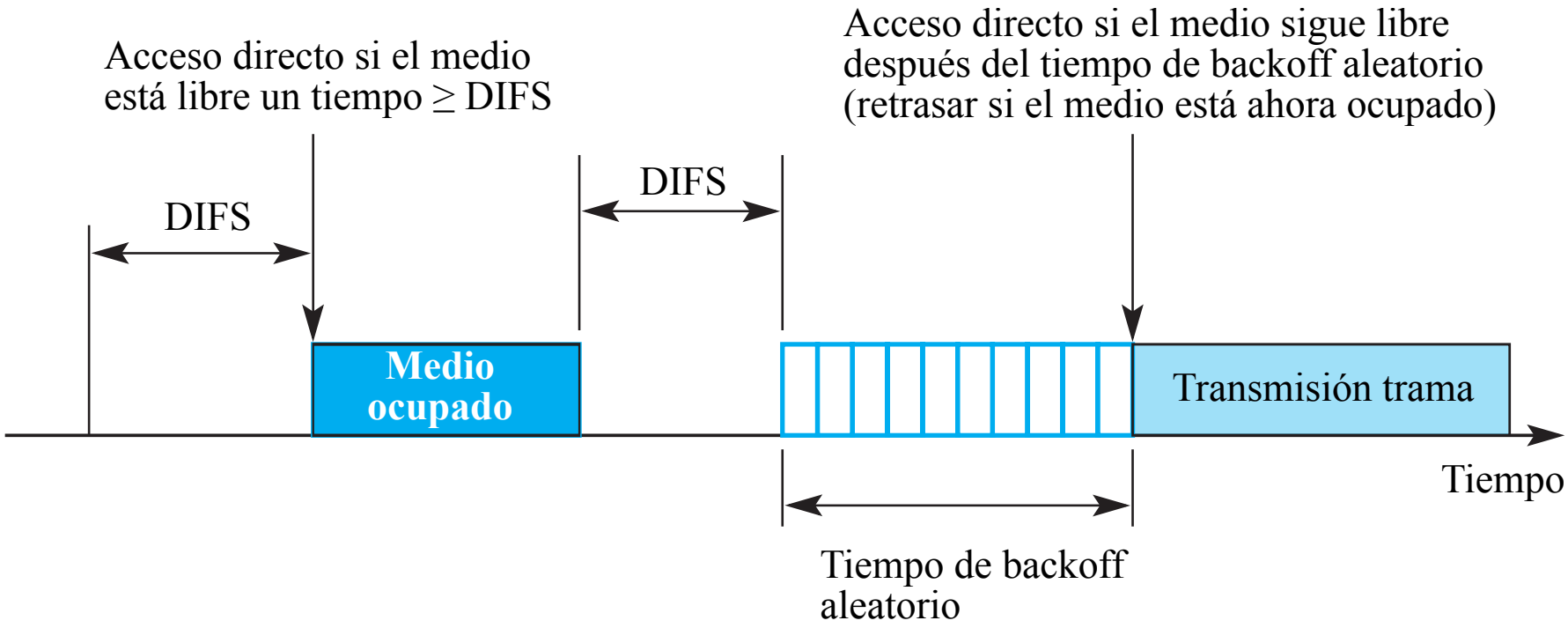
Se utilizan los siguientes InterFrame Space (IFS), para definir las prioridades de acceso:

SIFS: tiempo de espera inter-trama corto (**prioridad alta**)

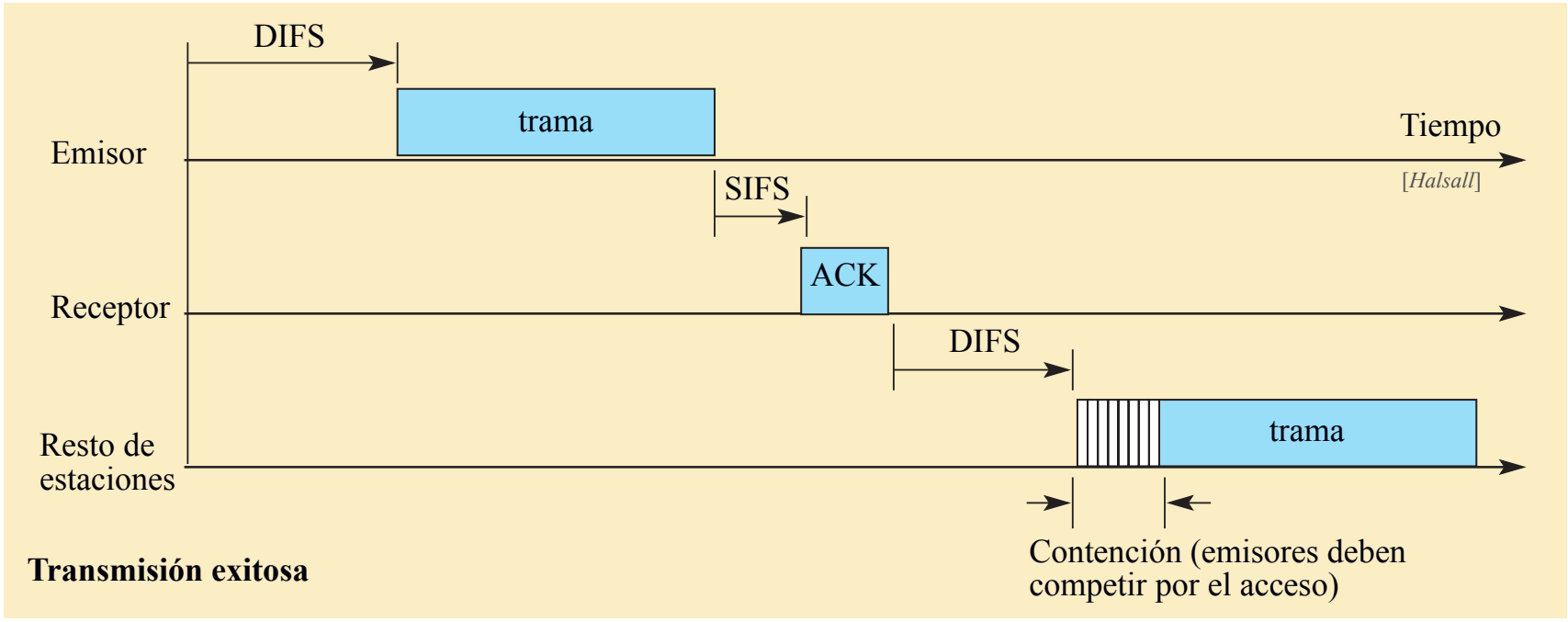
PIFS: tiempo de espera entre SIFS y DIFS (**prioridad media**)

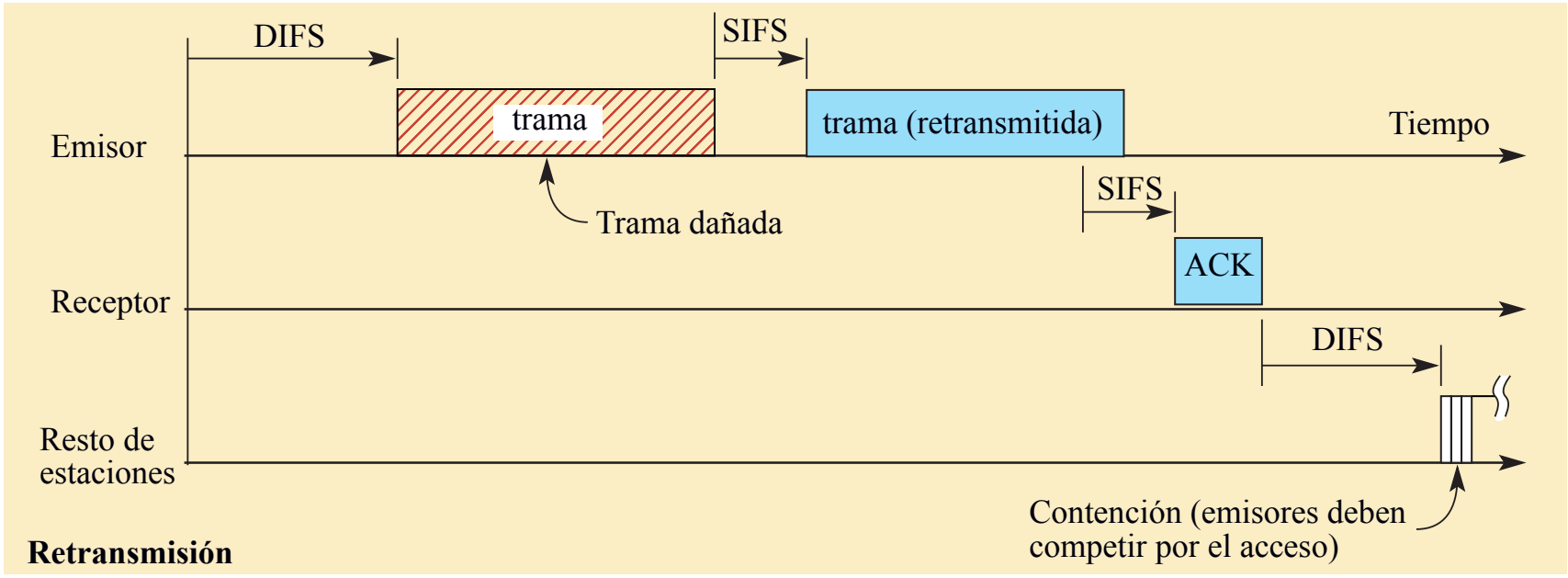
DIFS: tiempo de espera inter-trama más alto (**prioridad más baja**)

Acceso aleatorio



DCF con CSMA/CA (acceso aleatorio)



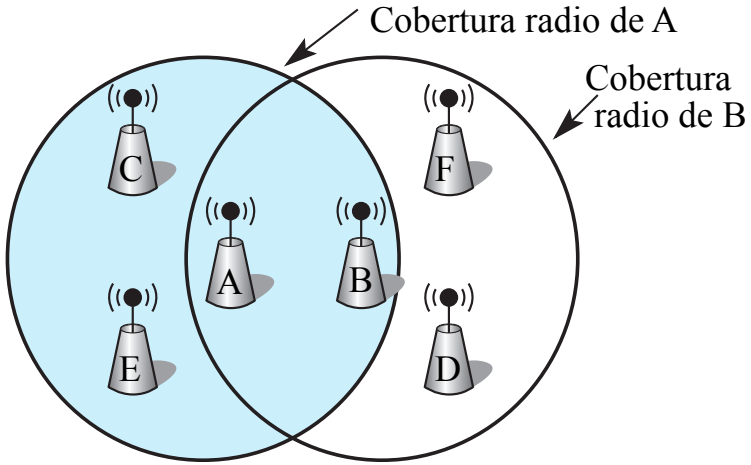


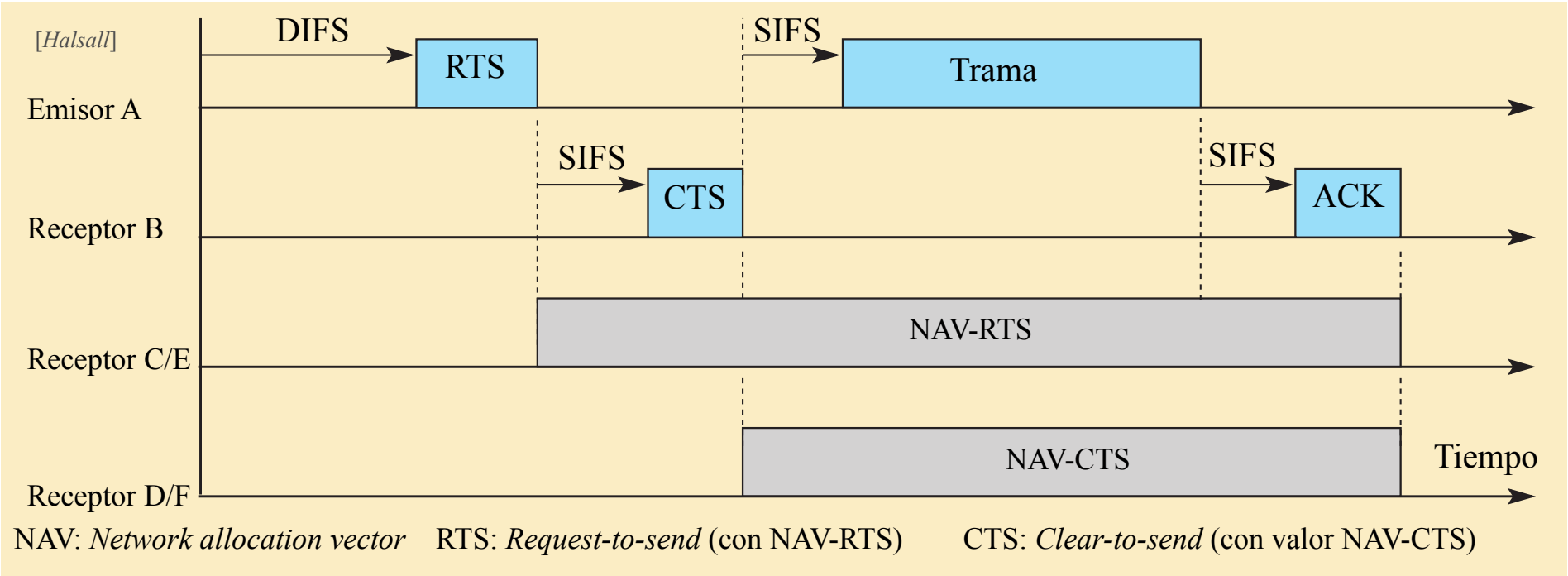
DCF con RTS/CTS

RTS/CTS se utiliza para resolver el problema de la estación oculta.
Supongamos la siguiente distribución de coberturas:

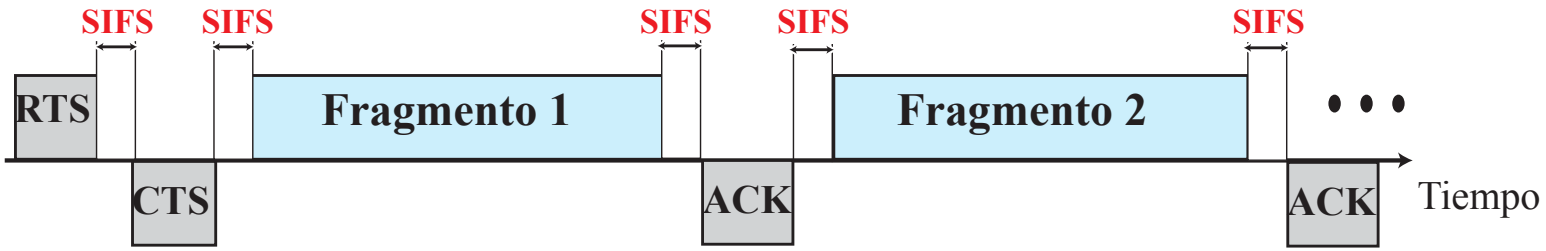
- C y E están dentro de la cobertura radio de A.
- D y F están dentro de la cobertura de B.

A envía una trama a B.





DCF con RTS/CTS: fragmentación (I)

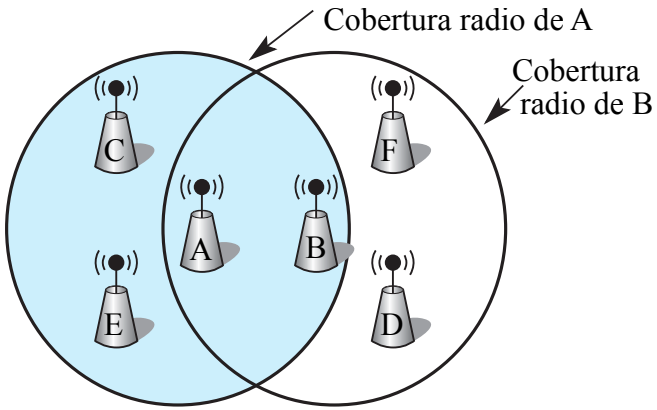


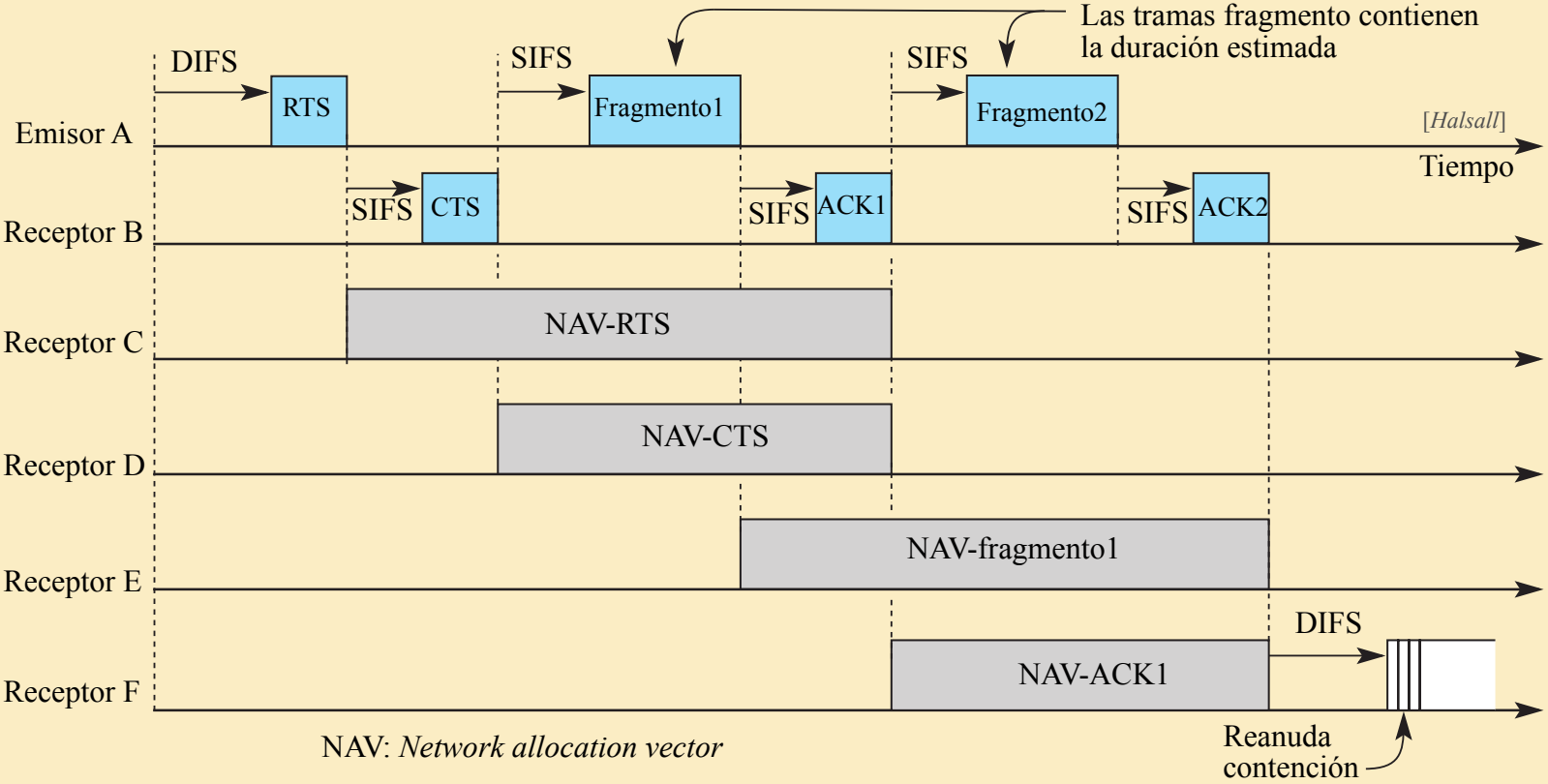
El entorno inalámbrico es muy ruidoso por lo que las tramas son susceptibles de corromperse.

Los protocolos wireless recomiendan la **fragmentación**: división de la trama total en tramas más pequeñas.

Es más eficiente enviar una trama pequeña que una grande.

DCF con RTS/CTS: fragmentación (II)





Función de coordinación puntual (PCF) (I)

La **función de coordinación puntual (PCF)** es un método de acceso puntual que se puede implementar en una red de infraestructura (no en una red ad hoc).

Se implementa encima de la función DCF y se utiliza, fundamentalmente, en transmisión sensible al tiempo.

PCF es un método de acceso por sondeo **libre de contención** y **centralizado**.

El AP ejecuta un sondeo a las estaciones que sean capaces de ser sondeadas, de forma secuencial, respondiendo al AP con cualquier dato que tengan.

Para dar prioridad a PCF sobre DCF, se utiliza otro espacio entre tramas denominado **PIFS** (PCF IFS), de forma que PIFS es más corto que DIFS.

Función de coordinación puntual (PCF) (II)

Si una estación quiere utilizar sólo DCF y, al mismo tiempo, un AP quiere utilizar PCF, el AP tiene prioridad.

Debido a la prioridad de PCF sobre DCF, las estaciones que sólo utilicen DCF pueden no tener acceso al medio.

Para prevenir este problema, se ha diseñado un **mecanismo de repetición** para cubrir el tráfico PCF libre de contención y DCF basado en contención.

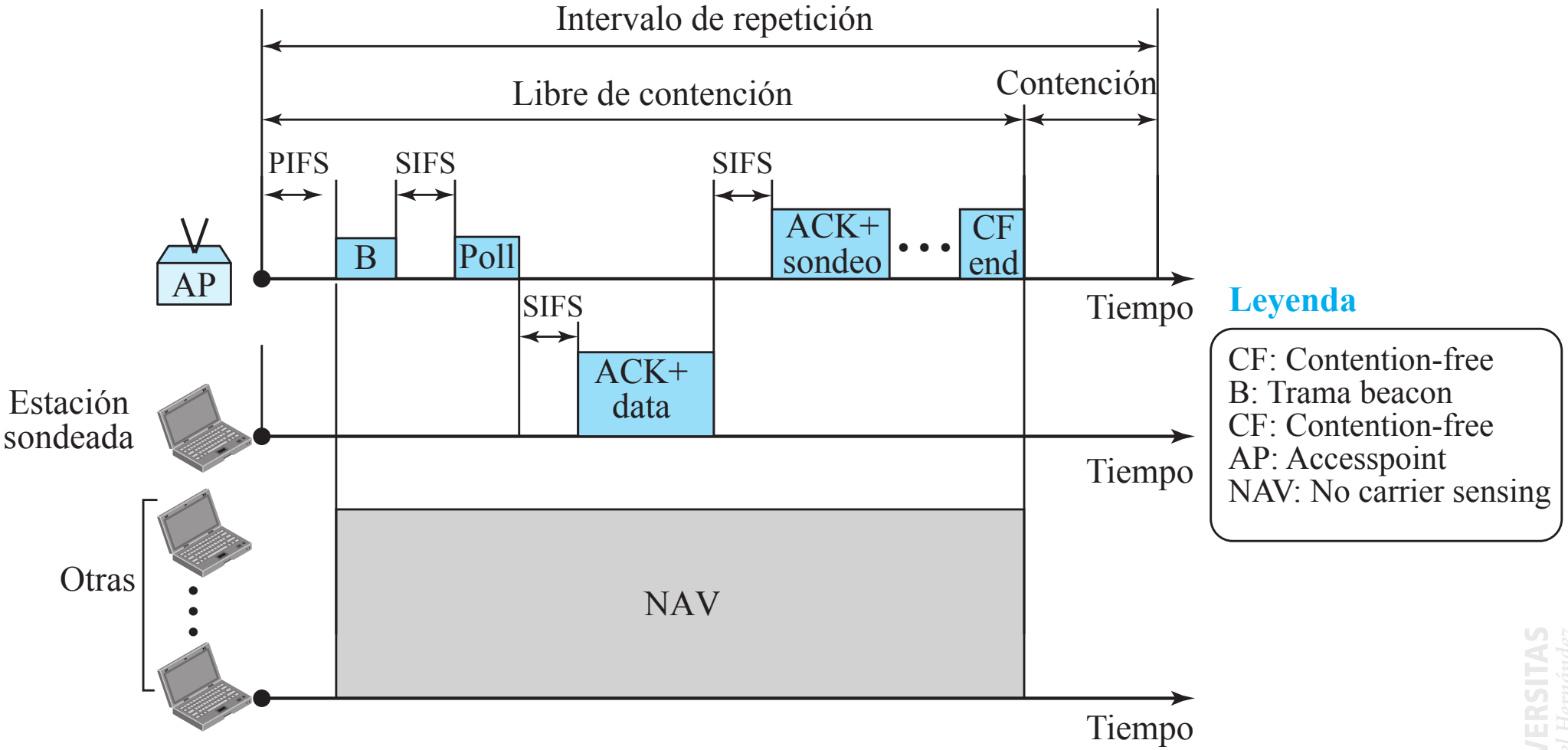
El **intervalo de repetición**, que se repite continuamente, se inicia con una trama especial denominada *beacon (B)*.

Cuando las estaciones escuchan la trama *beacon*, arrancan sus NAV por una duración igual al periodo libre de contención del intervalo de repetición.

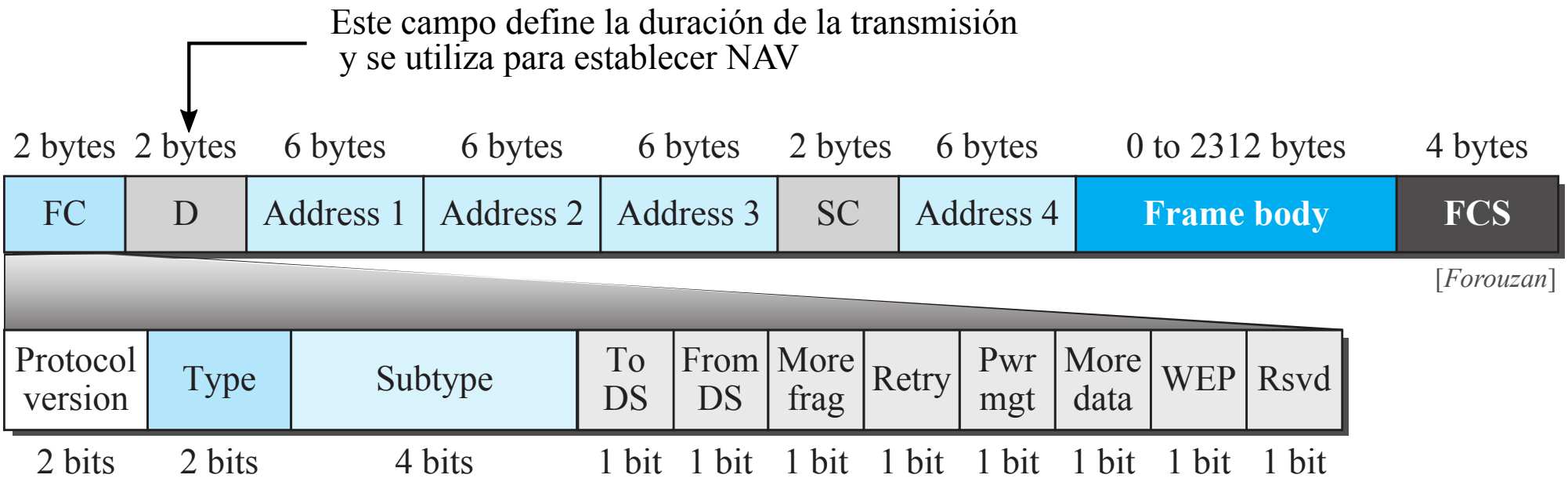
Durante el periodo de repetición, el PC (*Point controller*) puede enviar una trama de sondeo, recibir datos, enviar y recibir ACK o hacer cualquier combinación de estas.

Al final del periodo libre de contención, el PC envía una trama CF end (*Contention-free end*) para permitir utiliza el medio a las estaciones basadas en contención.

PCF con sondeo: ejemplo



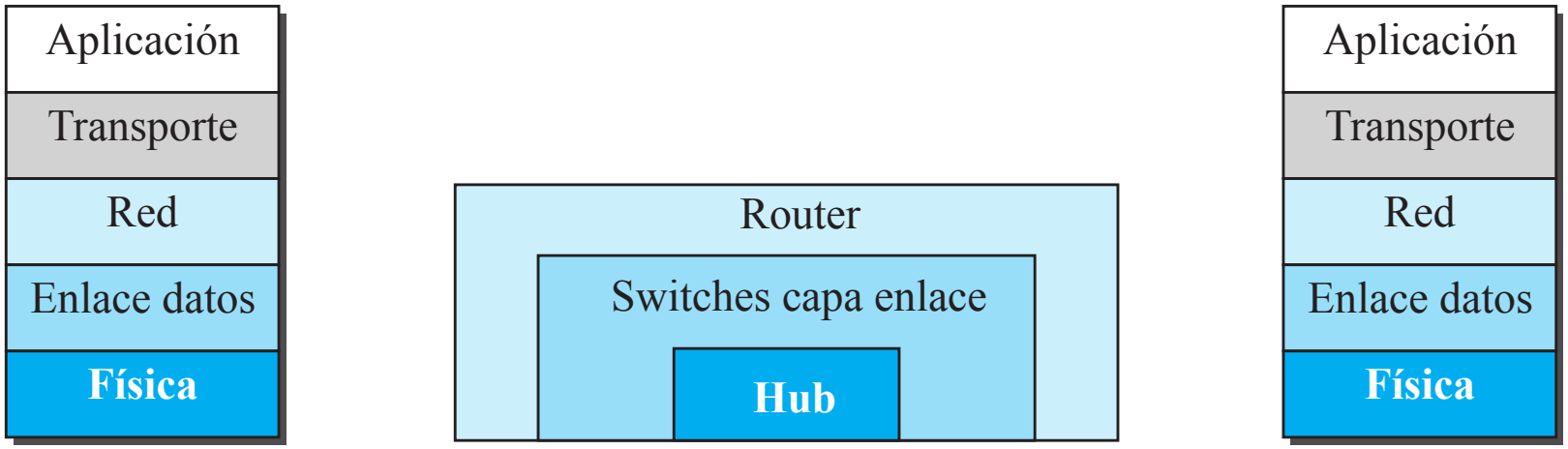
Formato de trama



Control de acceso al medio

1. Introducción
2. Protocolos de acceso aleatorio
3. Protocolos de acceso controlado
4. Familia Ethernet
5. Redes inalámbricas
6. ***Dispositivos de interconexión***

Dispositivos de interconexión

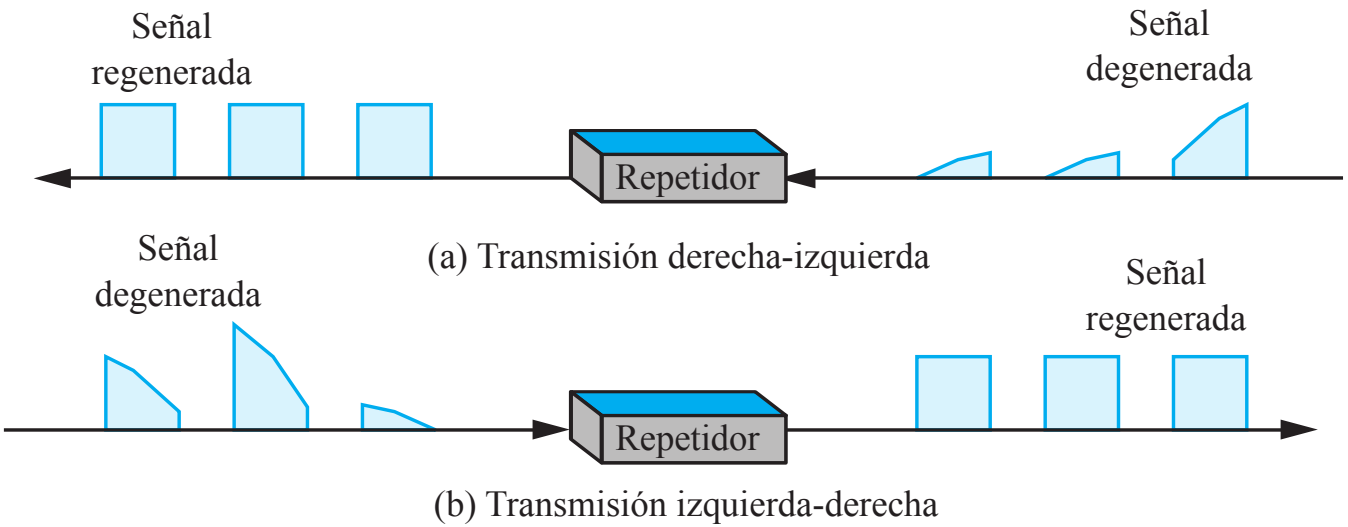


Los host y redes no operan de forma aislada.

Los dispositivos de interconexión se utilizan para interconectar hosts entre sí y formar una red, o conectar redes entre ellas y formar una interred.

Los dispositivos de interconexión operan en diferentes capas del modelo TCP/IP.

Hub

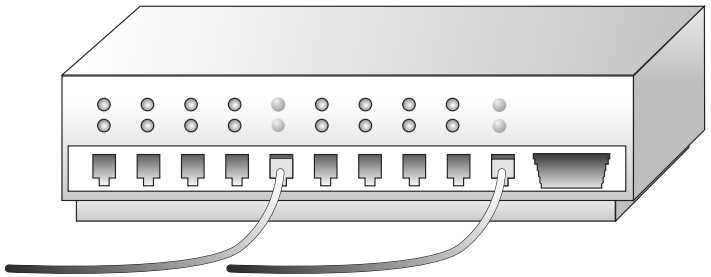


El **hub** es un dispositivo que opera sólo en **capa física**.

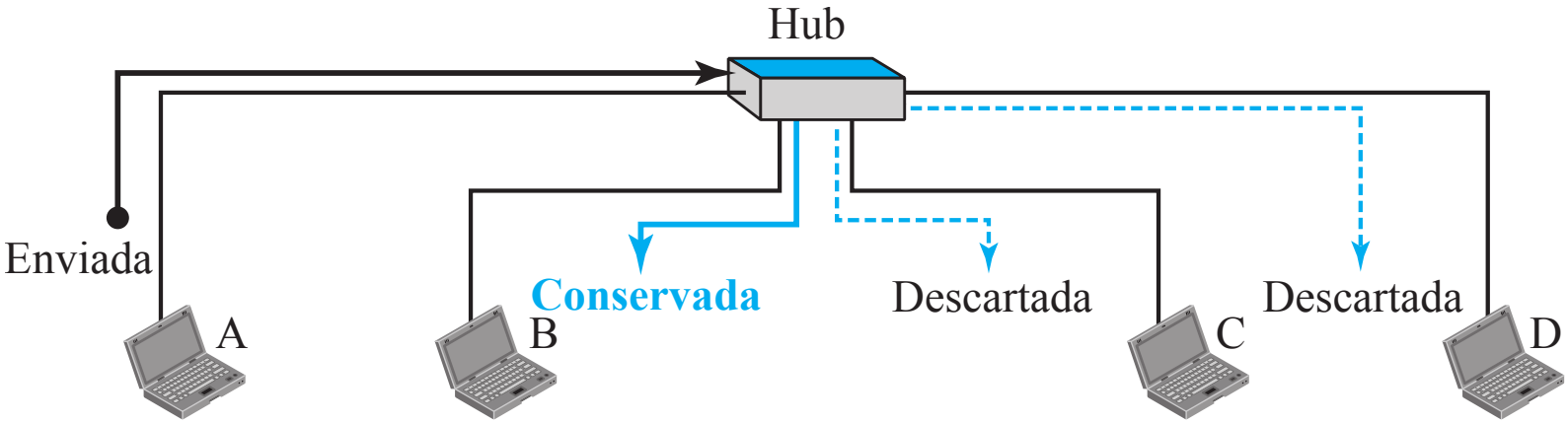
La señal que viaja a lo largo de los medios sufre de atenuación.

El repetidor recibe la señal y antes de que sea demasiado débil o corrupta, regenera y retemporiza el patrón de bits original, y la devuelve al medio.

Actualmente, en la Ethernet LAN con topología estrella, el hub es un dispositivo multipuerto, que además de ser un dispositivo de interconexión realiza la función de **repetidor multipuerto**.



Hub: operación



- Un paquete procedente del dispositivo A destinado al dispositivo B llega al hub.
- La señal eléctrica que representa la trama se regenera para eliminar el ruido.
- El hub reenvía la trama por todos los puertos de salida, excepto por el que ha sido recibida (**broadcast**).
- Todas las estaciones reciben la trama, pero sólamente la estación B la guardará, y el resto la descartarán.
- El hub no hace ningún tipo de filtrado a nivel de señal, ni selección de puerto, sólamente, regenera la señal.

Switch: filtrado

El dispositivo **switch** de capa enlace (switch) opera en los niveles **físico** y **enlace**:

- A nivel físico regenera la señal que recibe.
- A nivel enlace, el switch inspecciona la dirección MAC (origen y destino).

Realiza **filtrado de tramas**: chequea la dirección destino y decide el puerto de reenvío.

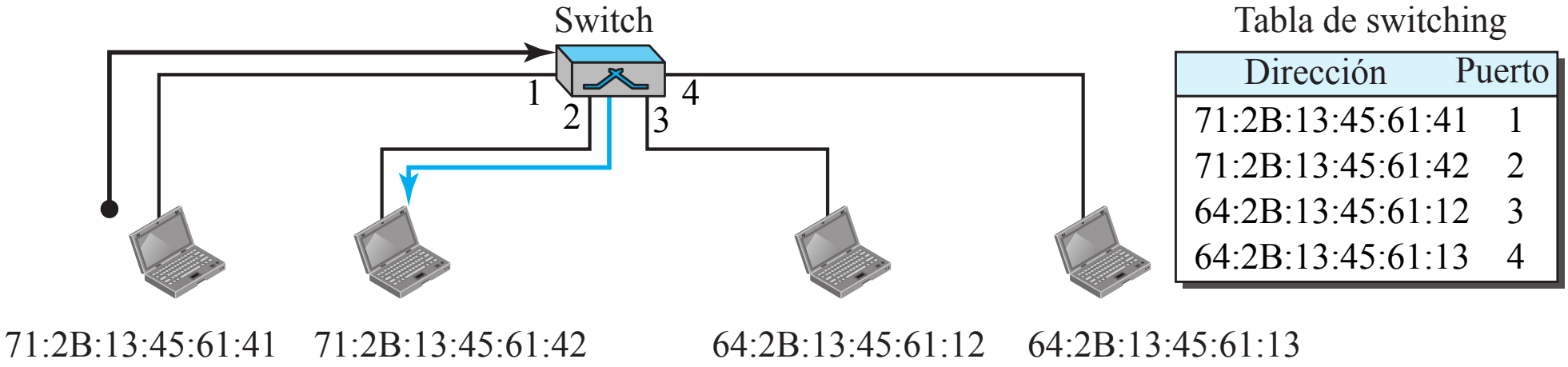


Tabla de switching

Dirección	Puerto
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

Si la trama destinada a la estación `71:2B:13:45:61:42` llega al puerto 1, el switch consulta su tabla para encontrar el puerto de reenvío, y decide que la trama debe ser enviada sólo por el puerto 2, por lo tanto, no es necesario hacer reenvío por todos los puertos.

Un switch no cambia la dirección de enlace (MAC) en la trama.

Switches transparentes

El switch es **transparente** porque las estaciones son completamente inconscientes de su existencia.

La incorporación o eliminación de un switch en una red no necesita ningún reconfiguración.

Según la especificación IEEE 802.1d, un sistema equipado con switches transparentes debe cumplir los siguientes criterios:

- Las tramas deben reenviarse de una estación a otra.
- La tabla de reenvío debe construirse de forma automática a partir de los envíos de tramas en la red.
- Debe prevenir los bucles.

También se denominan **bridges** (en el caso de disponer de sólo 2 puertos).

Switches: aprendizaje

Construcción gradual de la tabla

[*Forouzan*]

Dirección	Puerto

(a) Original

Dirección	Puerto
71:2B:13:45:61:41	1

(b) Después de A enviar trama a D

Dirección	Puerto
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

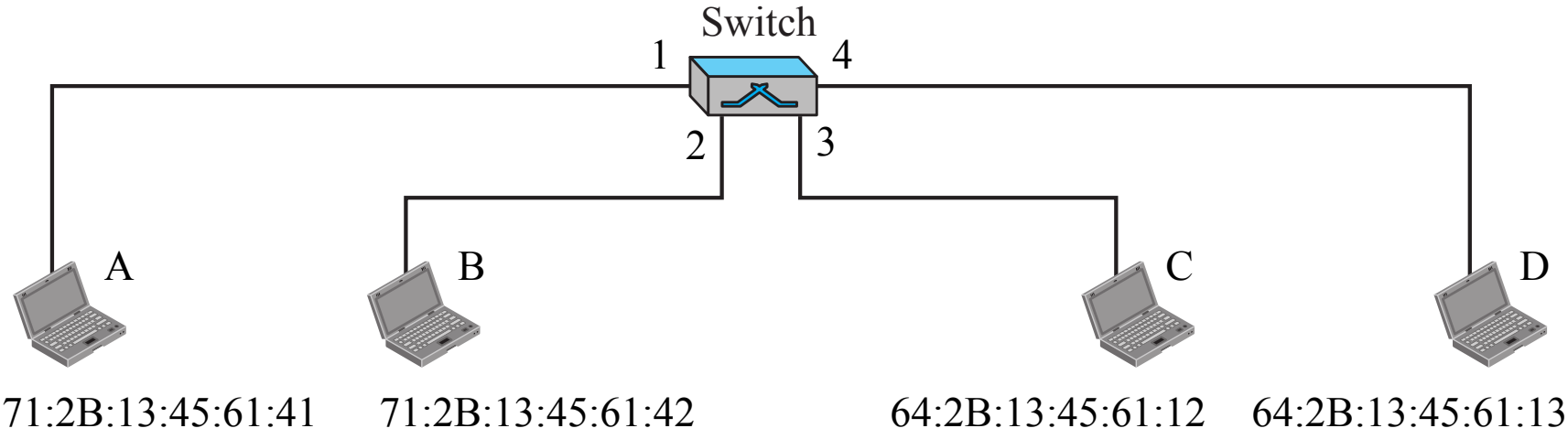
(c) Después de D envía una trama a B

Dirección	Puerto
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

(d) Después de B envía una trama a A

Dirección	Puerto
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

(e) Después de C envía una trama a D



Uso de switches

Los switches proporcionan diversas **ventajas**:

Eliminación de colisiones: al eliminar las colisiones incrementa el ancho de banda disponible para los host. En las LANs conmutadas no es necesario CSMA/CD, cada host transmite en cualquier instante.

Conexión de dispositivos heterogéneos: permite el conexionado de dispositivos que utilicen diferentes protocolos a nivel físico (tasa de datos) y diferentes medios de transmisión, ya que el formato de trama permanece invariable. Un switch puede recibir (o enviar) una trama por un puerto UTP a 10 Mbps y enviar (o recibir) por un puerto de fibra a 100 Mbps.

El **inconveniente** del switch, es la aparición de **bucles** en la red, que se resuelven con **Protocolo Spanning Tree** (fuera del alcance de esta asignatura).

Tipos:

- **Store-and-forwarding:**
- **Cut-through:**
  - Conmutación a partir de los primeros bytes de la trama (dirección destino).
  - Más rápidos.
  - No eliminan tramas erróneas de la red al no leer los bytes de FCS.

Routers

El **router** es un dispositivo de capa tres: opera a nivel **físico**, **enlace** y **red**:

- Nivel físico: regenera la señal que recibe.
- Nivel enlace: chequea la dirección física (origen y destino) contenida en la trama.
- Nivel red: tareas de enrutamiento con direcciones de red.

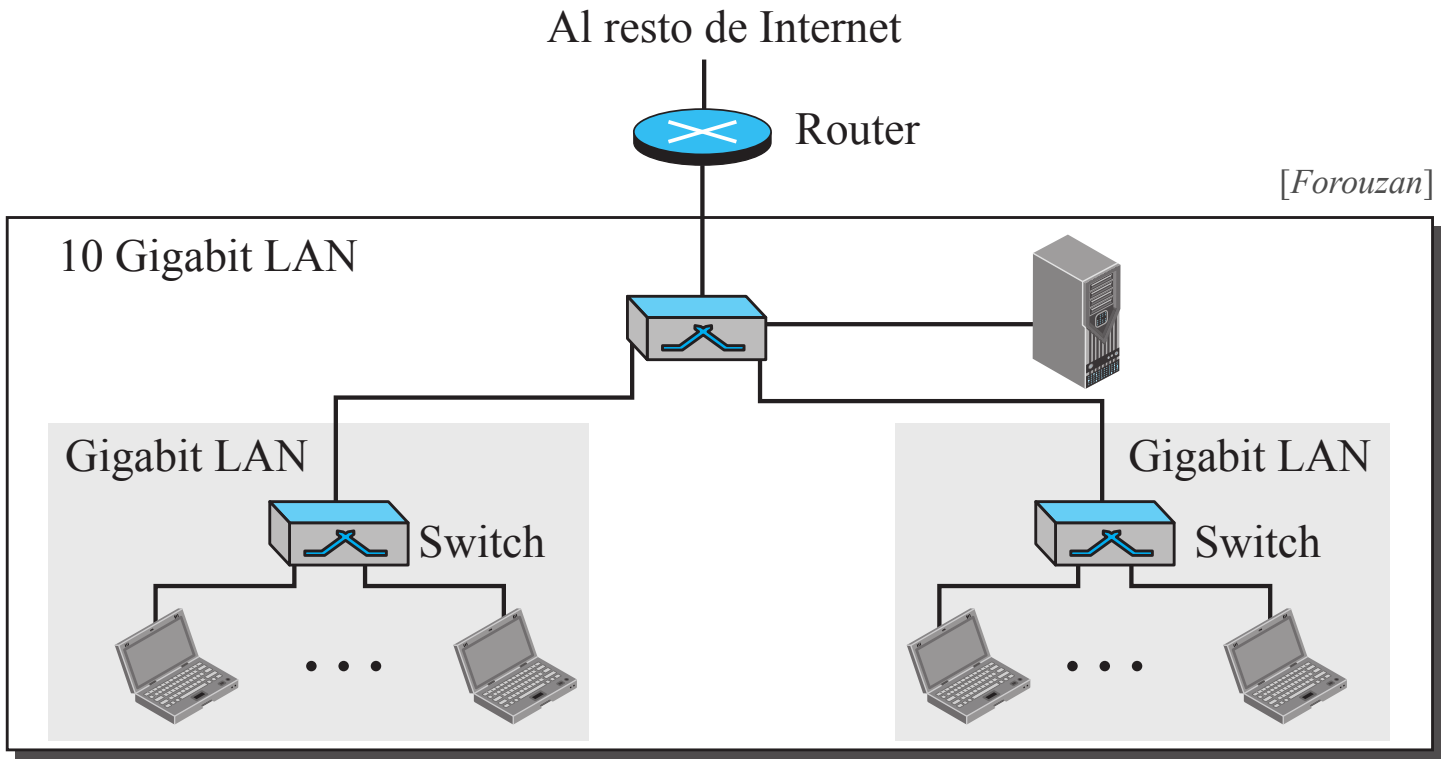
Un router puede conectar redes, de forma que a partir de redes independientes, forma una interred.

Las diferencias del router comparado con el switch o hub son:

1. El router tiene una dirección física (MAC) y lógica (IP) por cada una de sus interfaces.
2. El router actúa sólo con aquellos paquetes en los que la dirección destino, a nivel de enlace, coincide con la dirección de la interface por el que llega la trama.
3. Un router **cambia la dirección de enlace** (origen y destino) de aquellas tramas que reenvía por algún interface.

El router encamina datagramas pero sin alterarlos o modificarlos.

Routers

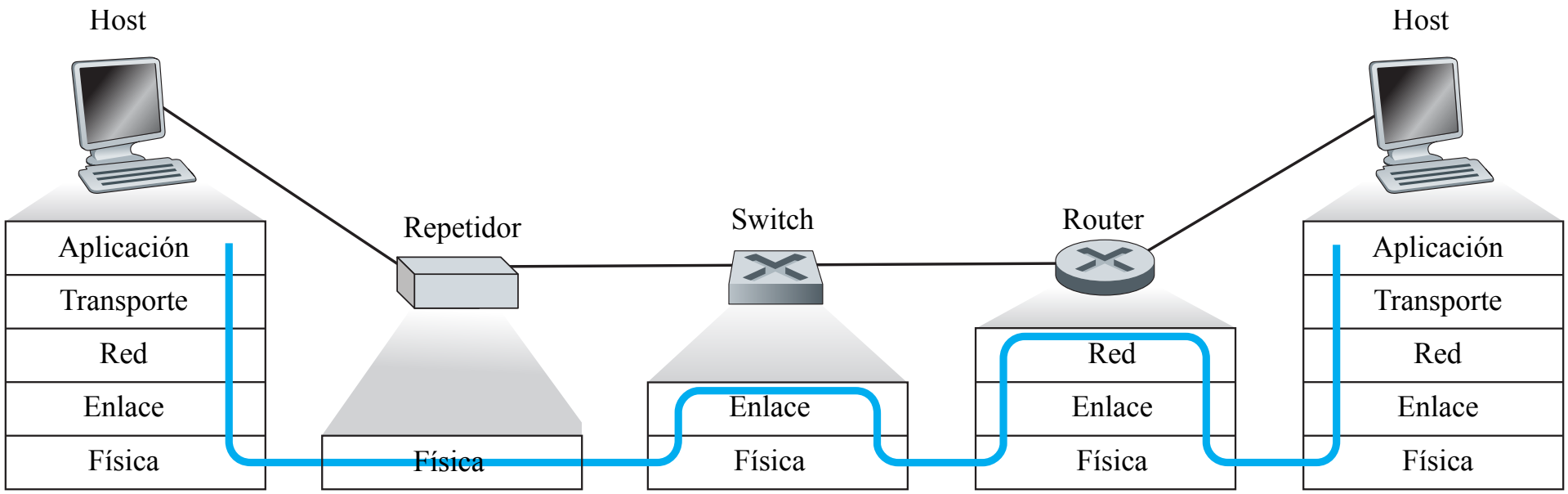


Supongamos una organización con dos edificios separados con Gigabit Ethernet LAN en cada edificio.

En cada edificio hay un switch, que conecta con otra LAN más grande utilizando tecnología 10 Gigabit Ethernet para proporcionar acceso de alta velocidad a zona de servidores.

El router conecta todo el sistema a Internet.

Dispositivos



Cuestiones de revisión

El estudiante debería ser capaz de responder a las siguientes cuestiones:

¿Donde aparece la componente aleatoria en Aloha y Aloha ranurado?

¿Cómo se detecta la pérdida de tramas en entornos inalámbricos?

¿Qué es una topología de red?

¿Por qué hay múltiples estándares LAN?

¿Cuáles son las funciones de un puente?

¿Cuál es la diferencia entre hub y switch?

¿Cuál es la diferencia entre un switch *store-and forward* y *cut-throw*?

Explica los tres métodos de persistencia en CSMA.

¿Qué es CSMA/CD?

Explica el retroceso exponencial binario.

¿Cuáles son las opciones de medios de transmisión en Fast Ethernet?

En el contexto de Ethernet, ¿cuál es la operación full-duplex?

UNIVERSITAS
Miguel Hernández