

Tema 2: Capa de Enlace

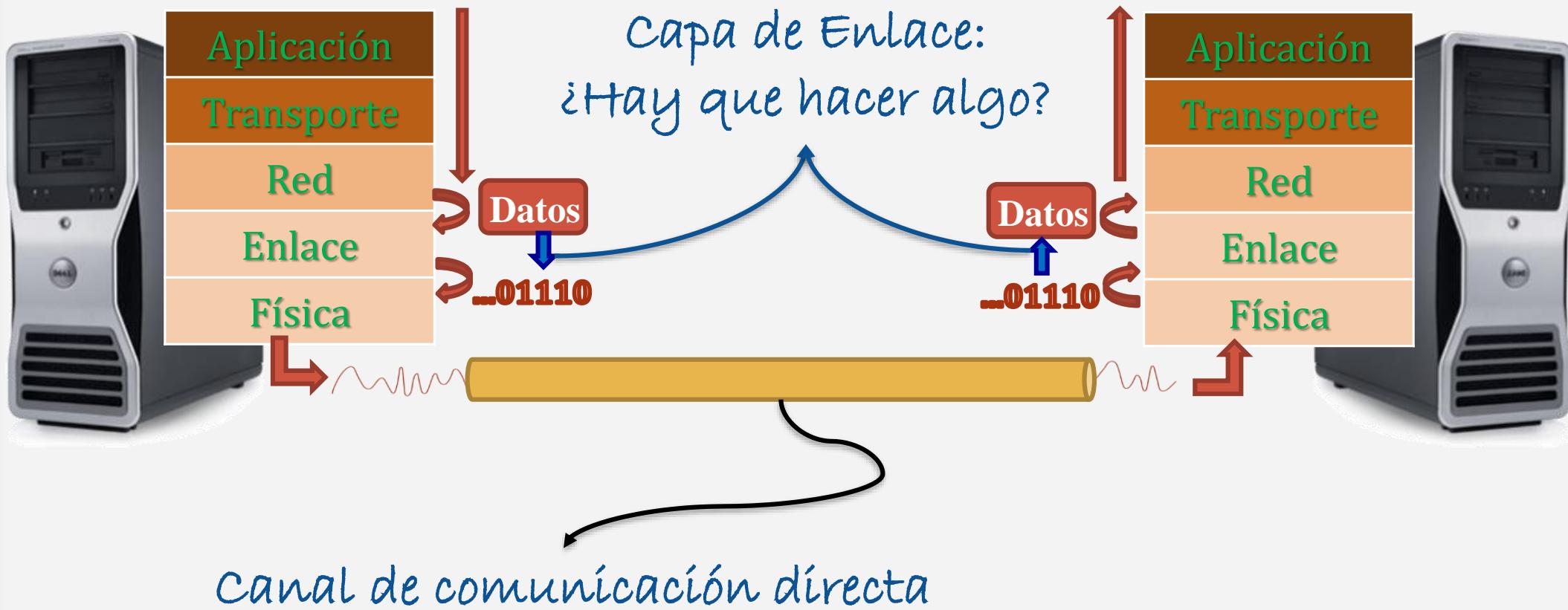
Clase del 06/02/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)



Situación inicial: Objetivo

Transferir los datos de la capa de red de un equipo a la capa de red de otro equipo con el que tiene conexión directa.



Situación inicial: Problemática



Características: ¿Sincronización? ¿Início y fin?

- Con portadora
- No fiable (interferencias, degradación)

Erros → Tramas erróneas
Tramas perdidas } ¿Detección?
} ¿Qué hacer?

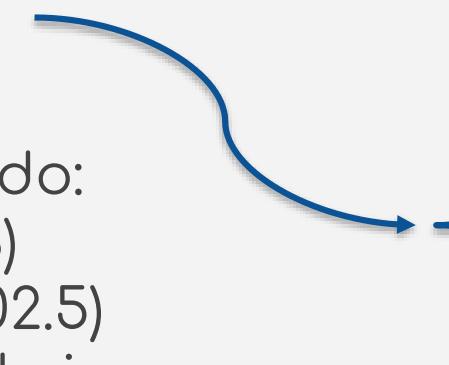


Otros servicios deseables:

- Negociación (uso, autenticación, ...)
- No saturar al destino

Organización del tema y la clase

4

- Funcionalidad de la capa y principales servicios (¿qué problemática se espera que esté solucionada?)
 - Técnicas genéricas para solventar esos problemas
 - Casos concretos:
 - Con medio cableado:
 - Ethernet (802.3)
 - Token Ring (802.5)
 - Con medio inalámbrico:
 - Wifi (802.11)
 - Bluetooth (802.15.1)
 - Alto nivel:
 - PPP (RFC 1661)
- 
- ¿Cómo detectar tramas erróneas?
 - ¿Se pueden corregir?

La Capa de Enlace

5

Objetivo básico:

Transferir los datos de la capa de red de un equipo a la capa de red de otro equipo con el que tiene **conexión directa**

Servicios que ofrece

Control de Acceso al Medio

Control de errores

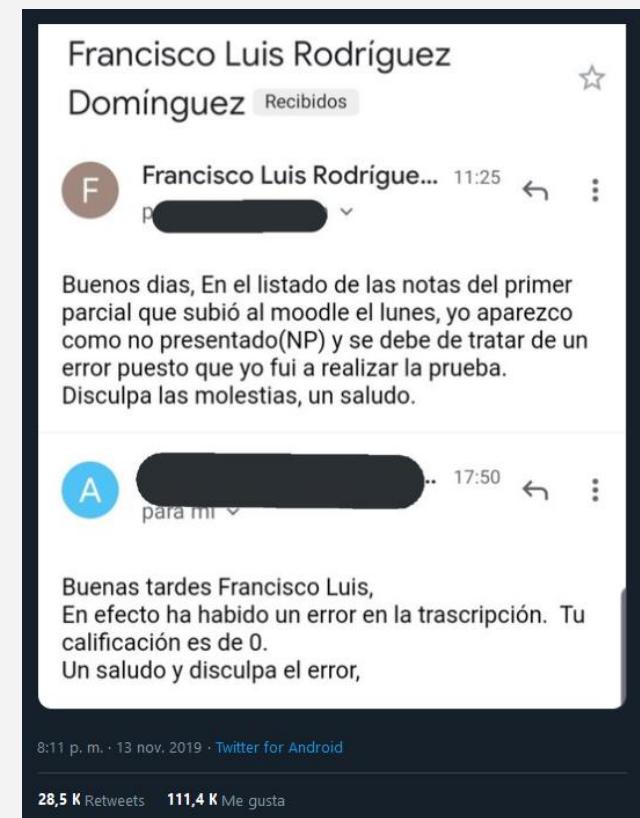
- Detección y Corrección

Control de flujo

Gestión comunicación:
half/full dúplex, ...

Enlace Control de Errores

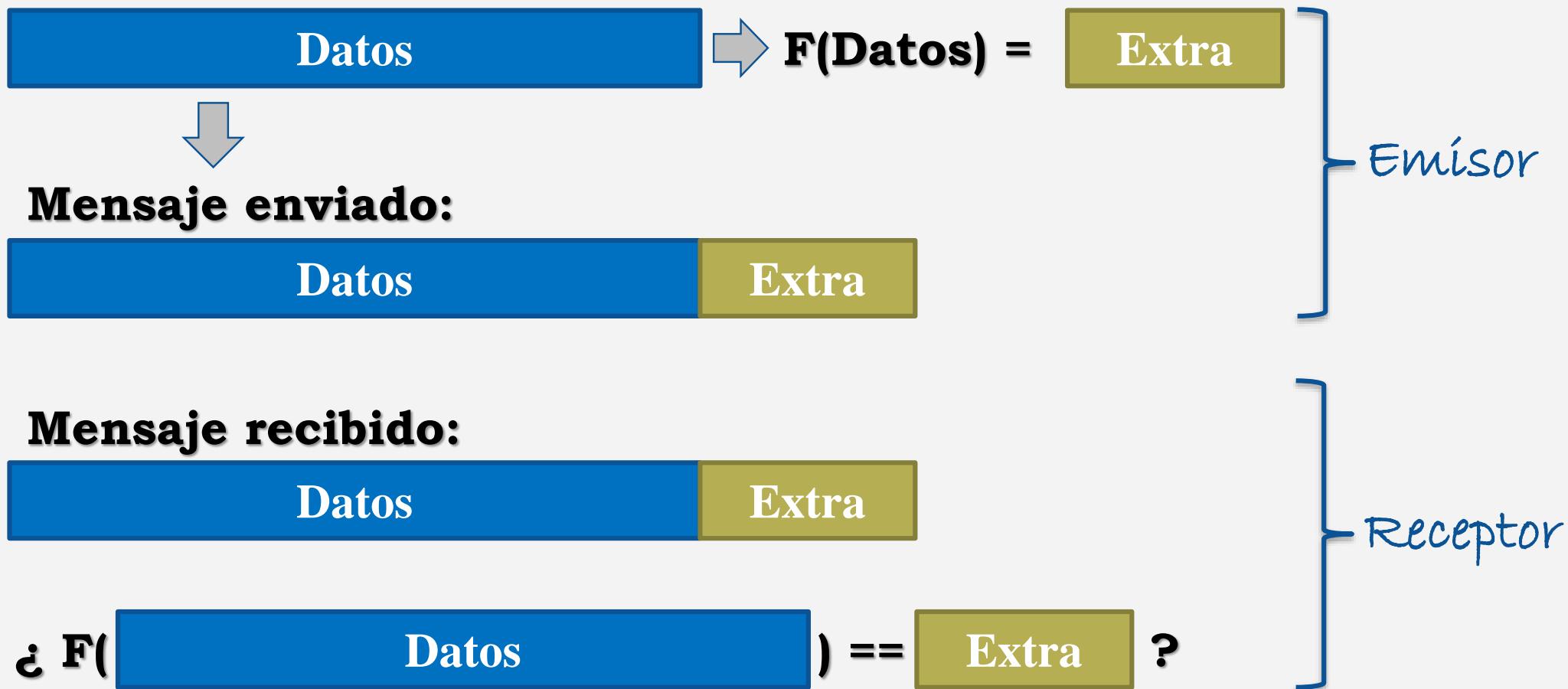
- Debe ser capaz de **detectar tramas incorrectas**
- Debe ser capaz de **corregir** esas tramas o **definir estrategias** a seguir cuando se detecten errores
- Técnicas **detectoras**:
 - Bit de paridad, CRC, checksums...
- Técnicas de **corrección de errores**:
 - Muy difícil de conseguir
 - **Códigos de Hamming**
- Técnicas de **control de errores**



Detección de errores: Planteamiento

7

Idea: Añadir más datos (**redundancia**) que nos permita **comprobar** si los datos son correctos:



Detección de errores: Características

8

- Debería ser una función fácil (**eficiente**) de calcular
- Datos similares deben tener valores resultantes muy diferentes
- Debería incorporar **pocos datos extra**:
 - Desperdicio del ancho de banda ...
 - ... pero poca información extra permite detectar menos errores.
- *[Dado $\langle \text{datos}, \text{hash} \rangle$ debería ser complicado encontrar otros datos diferentes que generen el mismo hash]*

SHATTERED – SHA-1 IS BROKEN

by: Pedro Umbelino

https://shattered.io/

97 Comments

February 23, 2017

Collision attack: same hashes		
Good doc	Sha-1	3713.42
Bad doc	Sha-1	3713.42

Detección de errores: Paridad

9

Bits de paridad

- Se añade un bit de paridad al final del bloque de datos para forzar una propiedad en los 0s o los 1s (normalmente sobre los 1s)
- Dos tipos de paridad
 - Paridad par: el número total de unos ha de ser par
 - Paridad impar: el número total de unos ha de ser impar

1	0	1	0	0	1	0	1
---	---	---	---	---	---	---	----------

Comprobación de paridad

- Detecta errores de un bit (o un **número impar** de bits)
- **No detecta** errores de pares de bits
- Ejemplo de aplicación: **código ASCII**
 - 7 bits + 1 bit de paridad

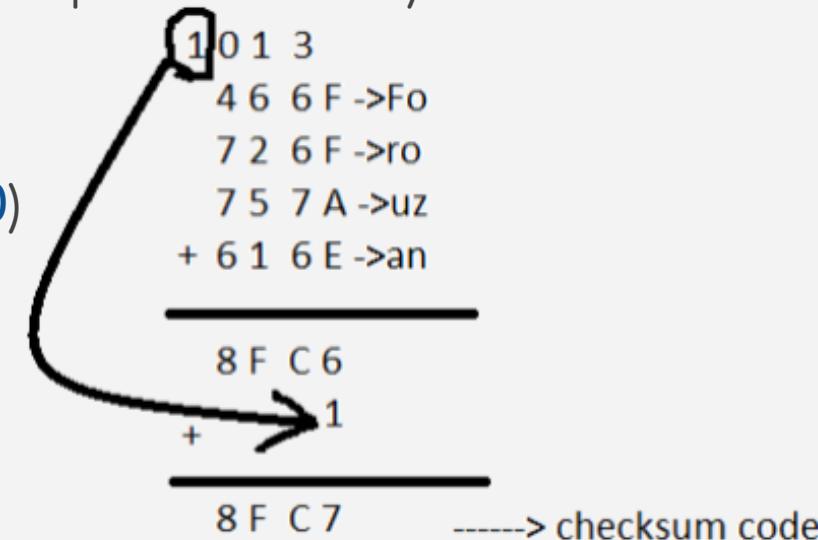
Paridad
(par)

Detección de errores: Checksum

10

Sumas de comprobación (checksum)

- Técnica general de detección de errores
- Se suele aplicar a **bloques de caracteres**, en lugar de caracteres aislados (**igual tamaño del checksum**)
- En la emisión y recepción
 - **Se suma cada bloque** al checksum (en complemento a 2)
- Al final de la emisión
 - El emisor envía el checksum al receptor, y éste lo comprueba (**la suma debe dar 0**)
- Se suele usar más en las capas de **red** y **transporte**:
 - Es un **esquema simple y rápido**
 - 16 bits en IP, TCP y UDP



Detección de errores: CRC

11

Códigos redundantes cíclicos

- Se conocen como CRC (*Cyclic Redundancy Check*)
- Funcionamiento
 - Se envían k bits de información + r bits redundantes
 - La trama de $k+r$ bits ha de ser divisible por un número predeterminado
 - Si en el receptor la división tiene resto 0, se asume que no se ha producido ningún error
- Los códigos CRC son particularmente interesantes porque su computación se puede realizar en hardware fácilmente
 - Suele emplearse en protocolos implementados en HW
 - Capa de enlace/física
 - 16/32 bits en PPP
 - 32 bits en Ethernet y Token Ring (polinomios usados: 0x04C11DB7)

Detección de errores: CRC

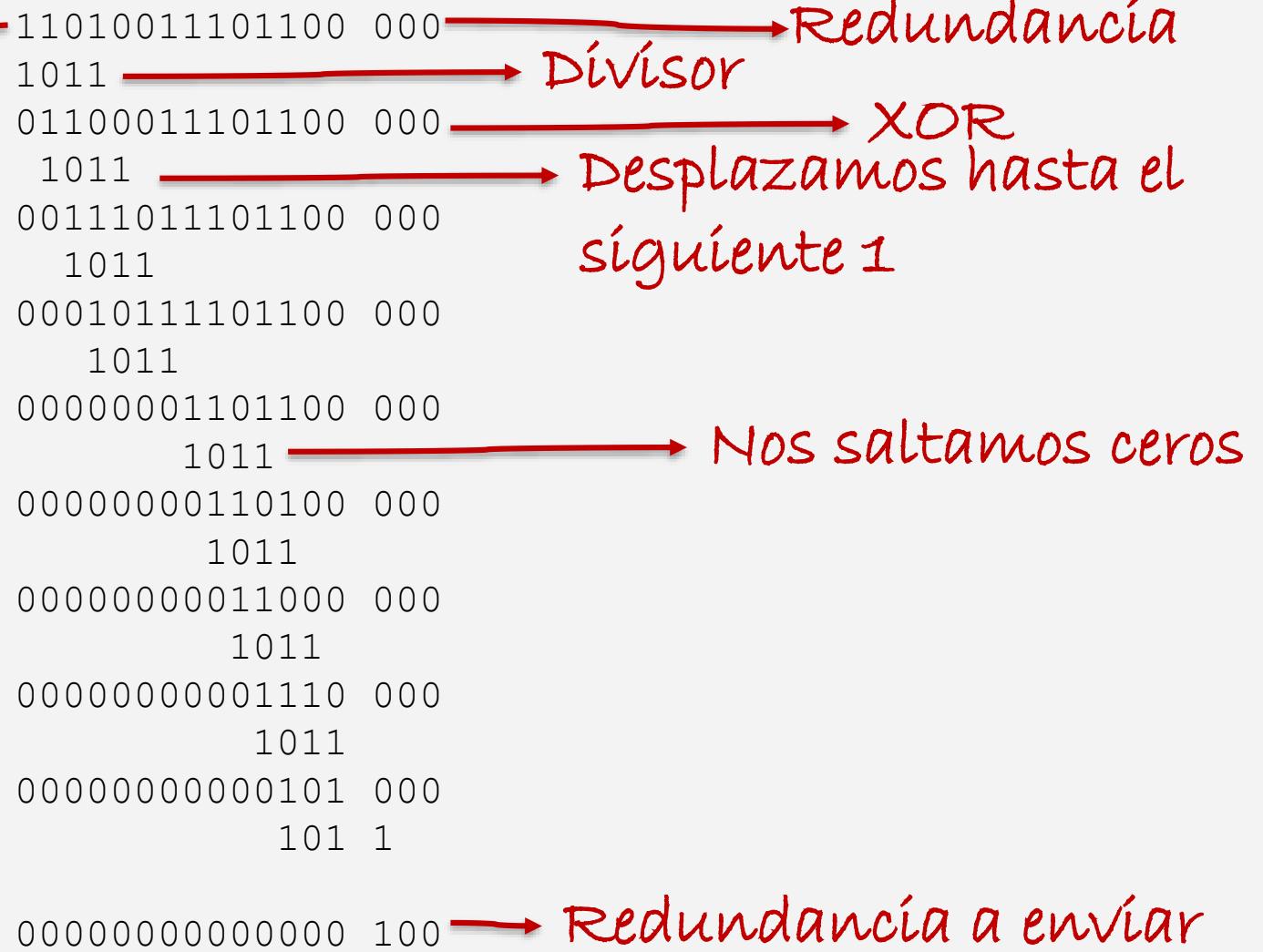
12

Ejemplo:

Info. a enviar

En la recepción se hace el mismo proceso y el resultado final debe ser todo ceros si es correcto

Estas operaciones binarias son muy rápidas (vía HW)



Tema 2: Capa de Enlace

Clase del 07/02/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)





Contexto

2

Comunicar equipos es complejo => **Modelo de capa**, donde cada nivel/capa añade una mejora/funcionalidad a anterior. La arquitectura de capas usada en Internet es **TCP/IP**.

Capa	Función	Paquete	Dirección
Aplicación	Servicio ofrecido al usuario (web, correo, mensajería, streaming...)	Mensaje	URL (recurso)
Transporte	Conexión extremo a extremo entre procesos (y que vaya bien)	Segmento / Datagrama	Puerto (proceso)
Red	Envío entre equipos no conectados directamente	Datagrama / Paquete	IP (nodo)
Acceso Al Medio	Envío entre equipos conectados directamente	Trama	MAC (nodo)
Física	Envío de bits	bit	-

Repaso

3

Funcionalidad de la capa de enlace:

Comunicación entre equipos directamente conectados

Problemas / servicios a ofrecer:

- Gestión de tramas:
Detección de inicio y fin. Sincronismo.
- Fiabilidad del canal: Errores
*Detección: bit de paridad, checksum, CRC
Actuación: ¿corregirlo?*

Detección/corrección: Cód. Hamming

Códigos de Hamming:

- Se basan en el concepto de **distancia de Hamming**
- Para **detectar n errores** se necesita una **distancia de $n + 1$**
- Para **corregir n errores** se necesita una **distancia de $2n+1$**

Bíts de paridad

	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	d_7
Orig.		0		1	1	0		1	0	1	
p_1	1	0			1	0		1	1		
p_2		0	0			1	0			0	1
p_3			0		1	1	0				
p_4					0	1	0	1			
Envío	1	0	0	0	1	1	0	0	1	0	1

	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	d_7
Recibido	1	0	0	0	1	1	0	0	1	0	0
p_1	1		0			1		0		1	0
p_2		0	0				1	0		0	1
p_3				0	1	1	0				0
p_4					0	1	0	1		0	1

	p_4	p_3	p_2	p_1
Binario	1	0	1	1
Decimal	8		2	1

Error en el bit 11

$$\Sigma = 11$$

Control de errores

Debe ser capaz de **detectar errores** y **definir estrategias** a seguir cuando se detecten **Desperdicio de BW**

Tipos de errores:

- Tramas **erróneas**
 - Detección: bit de paridad, CRC, checksum
 - Actuación: ~~corrección, informar, descartar~~
 - Tramas **perdidas**
 - Pérdida de la **confirmación**
 - ~~Confirmar la confirmación~~
 - Tramas **duplicadas**
- ¿Es la dirección correcta?
- Hasta el infinito y más allá!
- No hacer nada
- Desperdicio de BW



Repaso

Funcionalidad de la capa de enlace:

Comunicación entre equipos directamente conectados

Problemas / servicios a ofrecer:

- Gestión de tramas:
Detección de inicio y fin. Sincronismo.
- Fiabilidad del canal: Errores
Detección: bit de paridad, checksum, CRC
Actuación: corrección => confirmaciones, temporizador, numeración
- Acceso al Medio (difusión): Direccionamiento y colisiones
- Control de Flujo: evitar saturar al destino
- Gestión del medio: negociación sobre uso, seguridad

Muchos de ellos son opcionales:

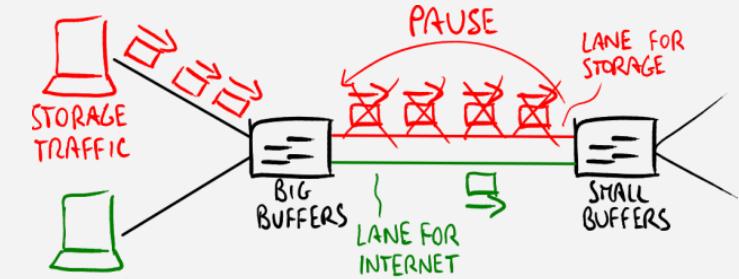
- Técnica de la avestruz (casos más generales y eficiencia)

Organización del tema y la clase

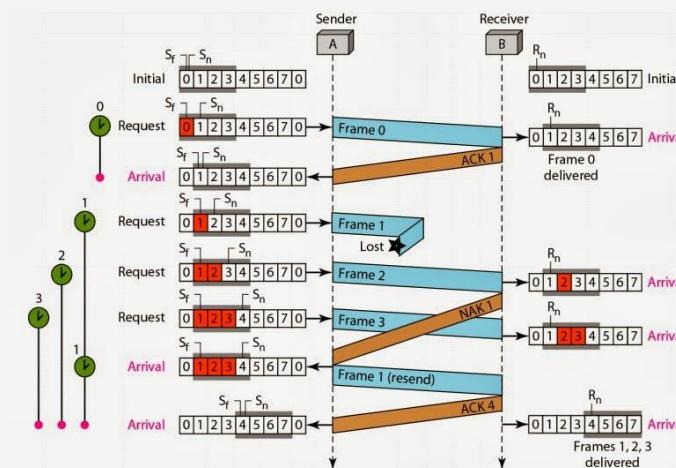
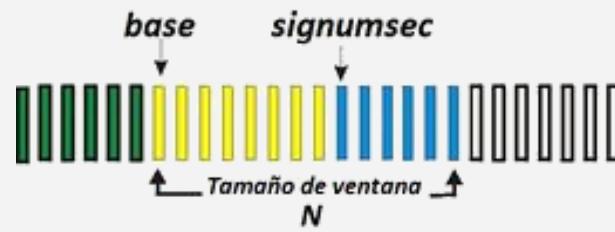
- Funcionalidad de la capa y **principales servicios** ✓
- **Técnicas genéricas** para solventar esos problemas:
 - Control de error: detección✓ y actuación
 - Control de flujo
 - Acceso al medio
- **Casos concretos:**
 - Con medio cableado:
 - Ethernet (802.3)
 - Token Ring (802.5)
 - Con medio inalámbrico:
 - Wifi (802.11)
 - Bluetooth (802.15.1)
 - Alto nivel:
 - PPP (RFC 1661)

Control de flujo

Se usa para **evitar** que el emisor **envíe** más datos al receptor de los que éste **es capaz de almacenar** para su posterior tratamiento



El propio **control de error**, ya limita la cantidad de datos a enviar



Protocolos básicos de control

9

Control del enlace de datos

- Control de error (y control de flujo)

Tres protocolos básicos:

- Protocolo de **parada y espera** (stop-and-wait)
- Protocolo **Go-Back-N**
- Protocolo de **repetición selectiva**

Estos protocolos se pueden usar:

- A nivel de enlace (bajo nivel)
- También pueden usarse en niveles superiores (ej: transporte)

Concepto relevante: Eficiencia

- Medida que indica la proporción de tiempo necesario para enviar información útil ($T_{envío_útil}$) respecto al total requerido (T_{total})
 - Lo ideal es una eficiencia del 1 (o del 100%)
- $$\text{Eficiencia} = \frac{T_{envío_útil}}{T_{total}}$$

Protocolos de parada y espera

10

Funcionamiento básico:

1. Se transmite una trama
2. El receptor envía una confirmación
3. El emisor no envía la siguiente trama hasta que recibe la confirmación (ACK)

¿perdida de la trama?

¿perdida del ACK?

Temporizadores (timeout):

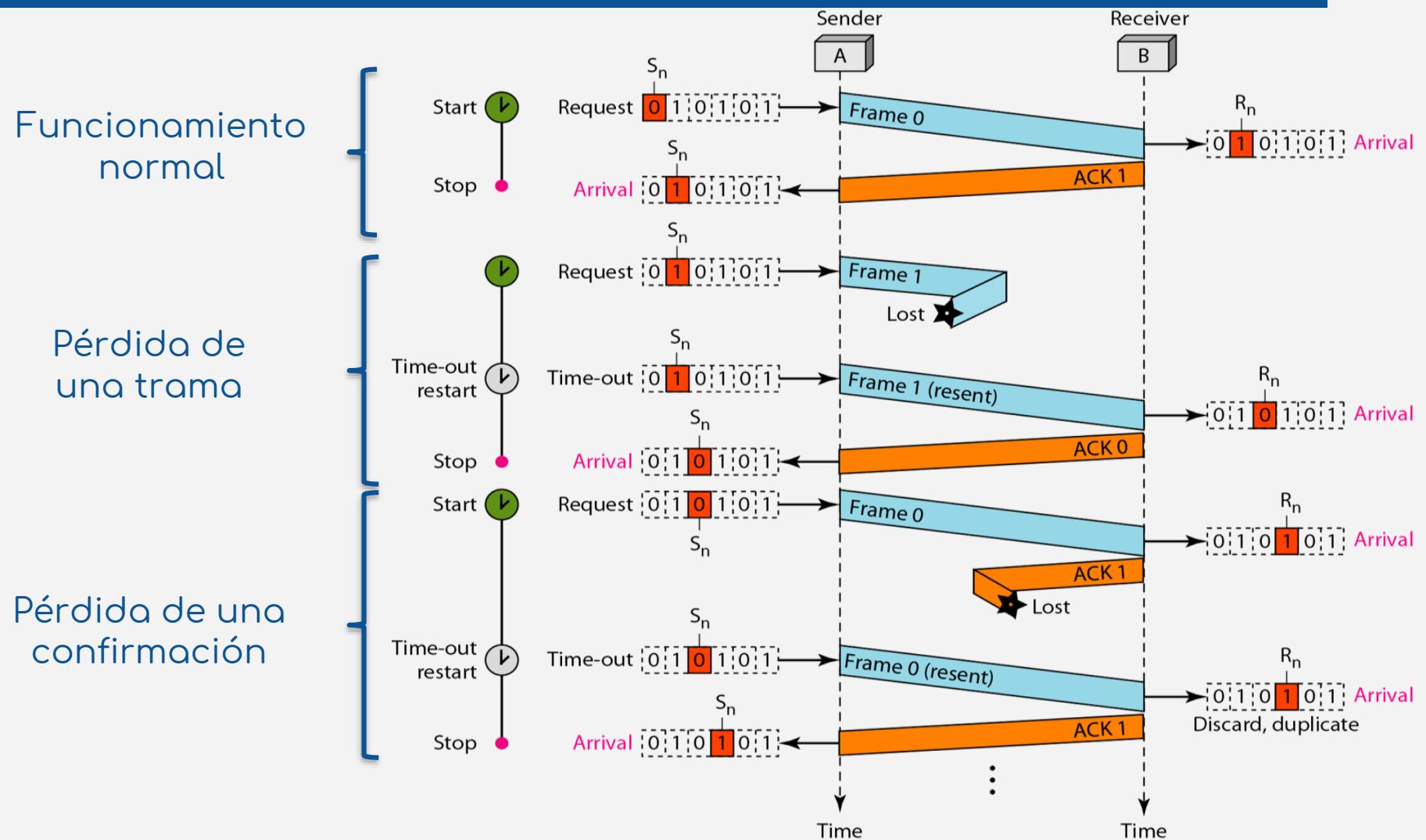
- Se activa cuando el emisor envía una trama
- Si se cumple el tiempo sin recibir confirmación -> Reenvío

Numeración de tramas y confirmaciones:

- Se numera cada trama
- ABP (Alternating Bit Protocol) usa 1 bit, valores 0 y 1 alternativo
- La confirmación (ACK o ARQ¹) se numera indicando **la siguiente trama que espera recibir**

¹En alguna literatura se usa ARQ (automatic repeat-request) en vez de ACK (acknowledgement)

Protocolos de parada y espera





Ejercicio

12

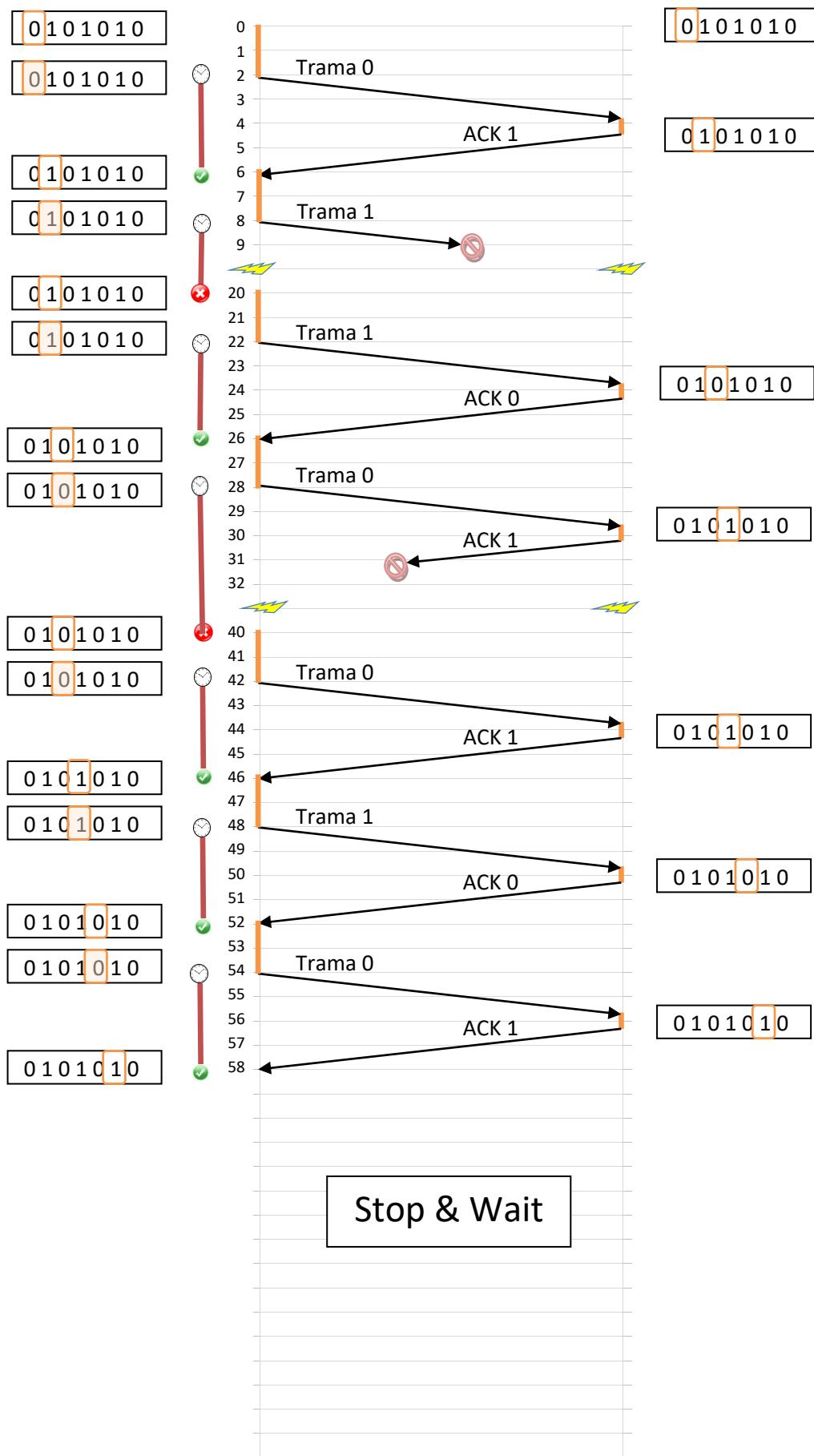
Dos máquinas A y B se encuentran conectadas mediante un enlace con las siguientes características:

t_{trans_datos}	= 2 ms	t_{prop}	= 1.75 ms
t_{proc}	= 0.25 ms	t_{trans_ACK}	= 0.25 ms
timeout	= 12 ms (doble de lo que debería tardar)		

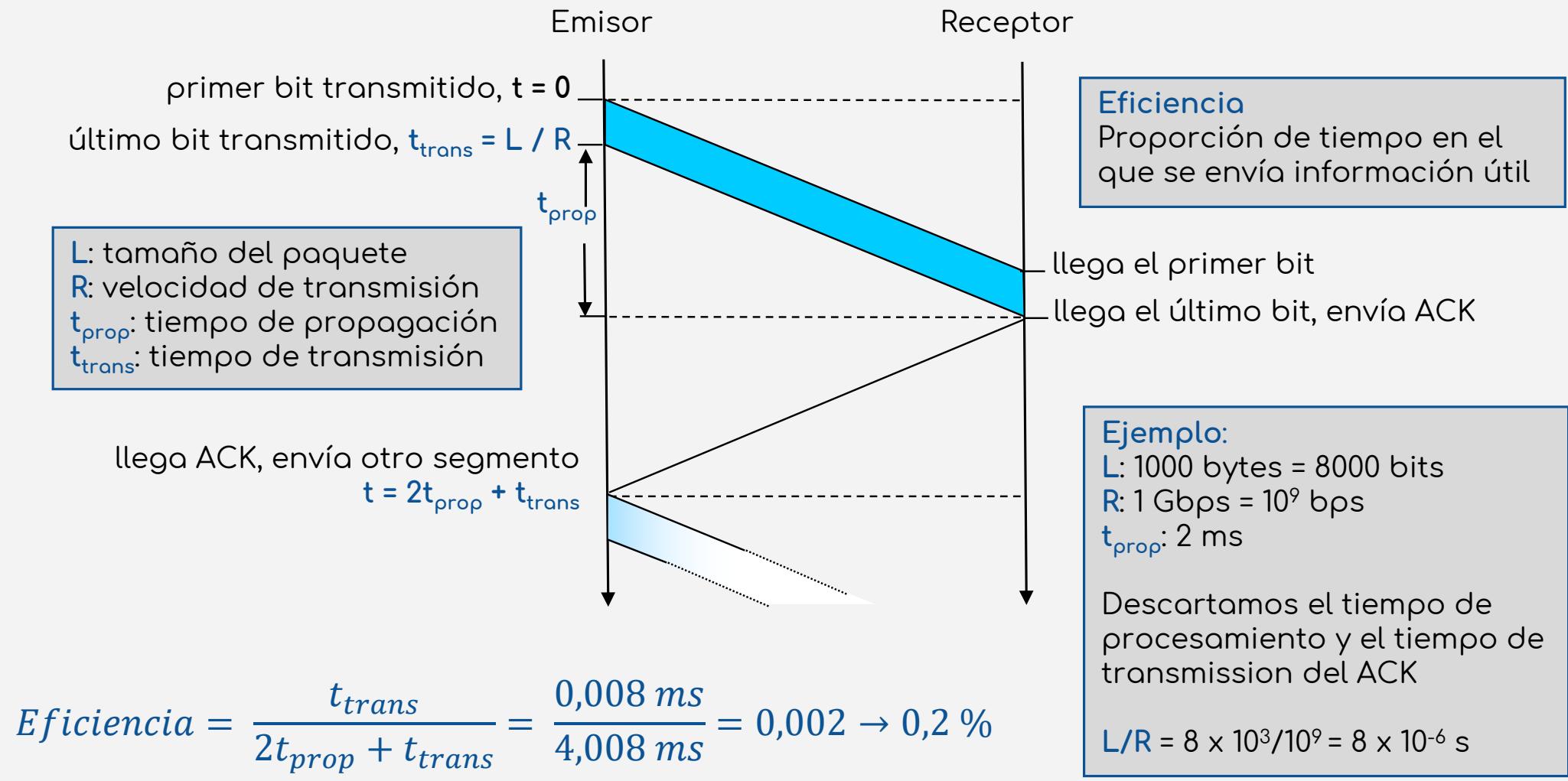
El envío tiene las siguientes características:

- La máquina A envía un archivo que requiere 5 tramas a B
- Se pierde la segunda trama que envía A
- Se pierde también la tercera confirmación enviada por B

Determine los eventos que ocurrirán en cada máquina hasta que el archivo esté totalmente para el protocolo Parada y Espera (S&W).



Protocolos de parada y espera



Protocolos de parada y espera

14

Ventajas

- Simple de implementar
- Eficiente si los mensajes son de gran tamaño

Inconvenientes

- Ineficiencia si usan mensajes pequeños
- No siempre los mensajes pueden ser de gran tamaño

Motivos para romper mensajes grandes

- Tamaño limitado de la memoria del receptor
- Si hay errores hay que retransmitir mucha información
- En medios de acceso múltiple la red no puede estar ocupada durante mucho tiempo

Mejora: Pipelining

Pipelining:

- Enviar más de un mensaje consecutivamente, sin esperar confirmaciones de los anteriores

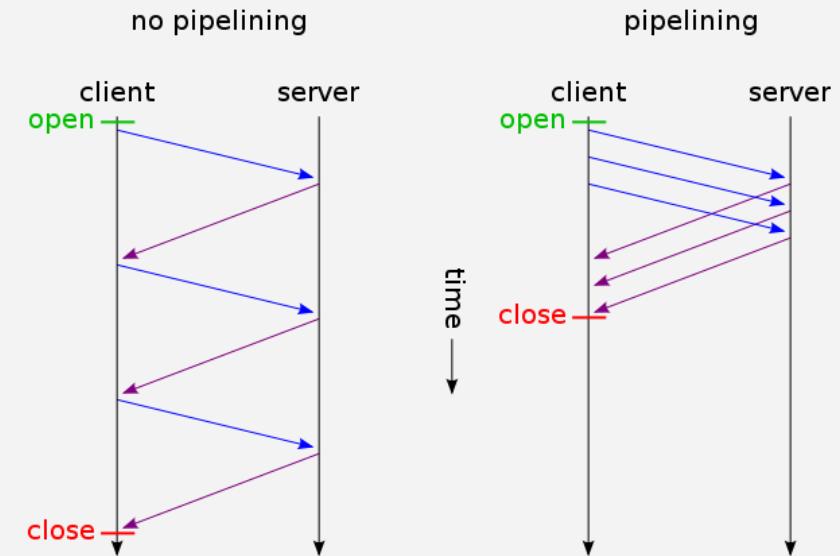
Consecuencias

- El rango de los números de secuencia ha de ser ampliado
- El receptor y/o el emisor han de usar buffers

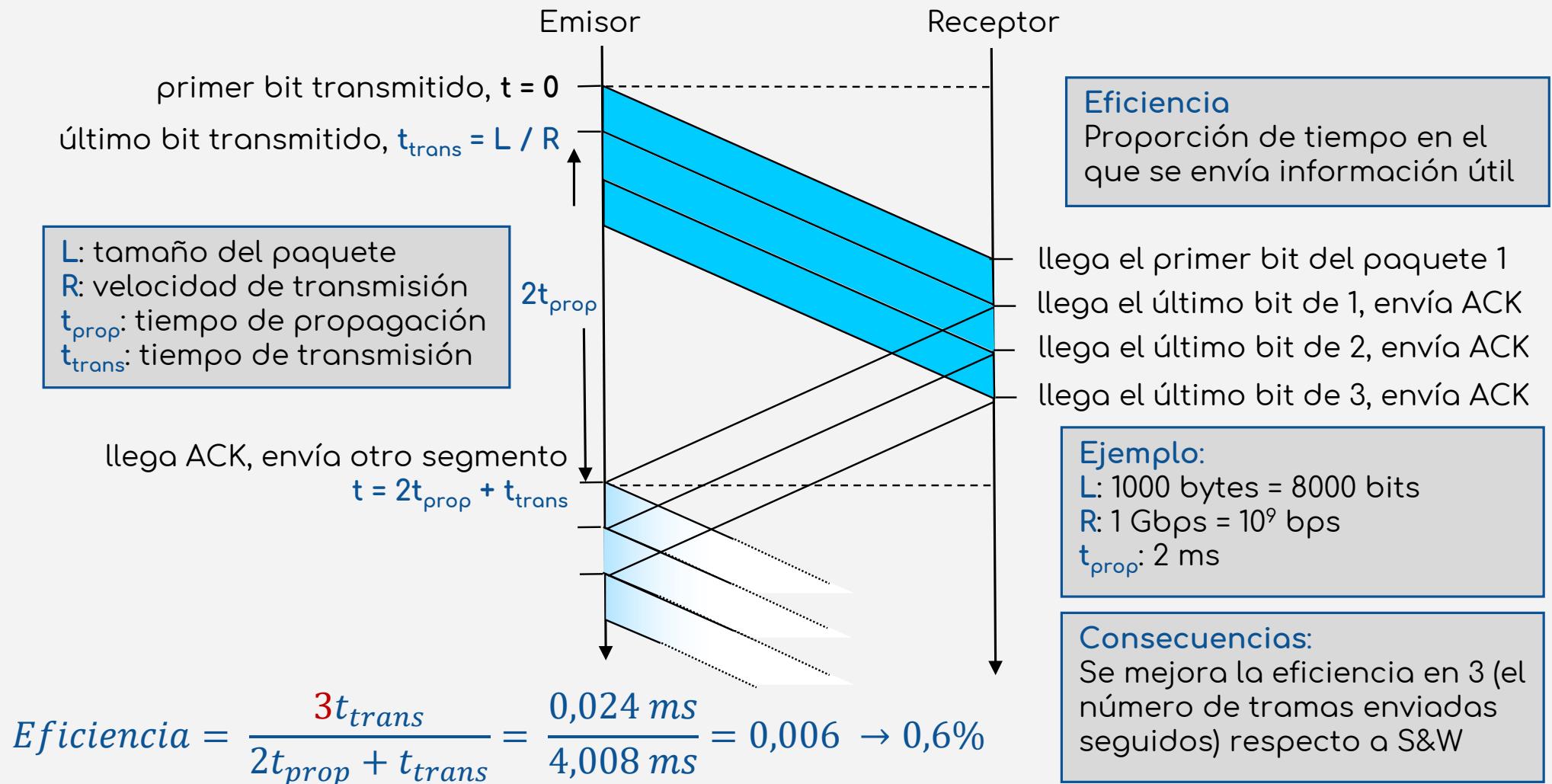
Dos técnicas básicas

- Go-Back-N
- SRP (Selective Repeat Protocol) – (variante Rechazo selectivo)

Se basan en el concepto de **ventana deslizante**



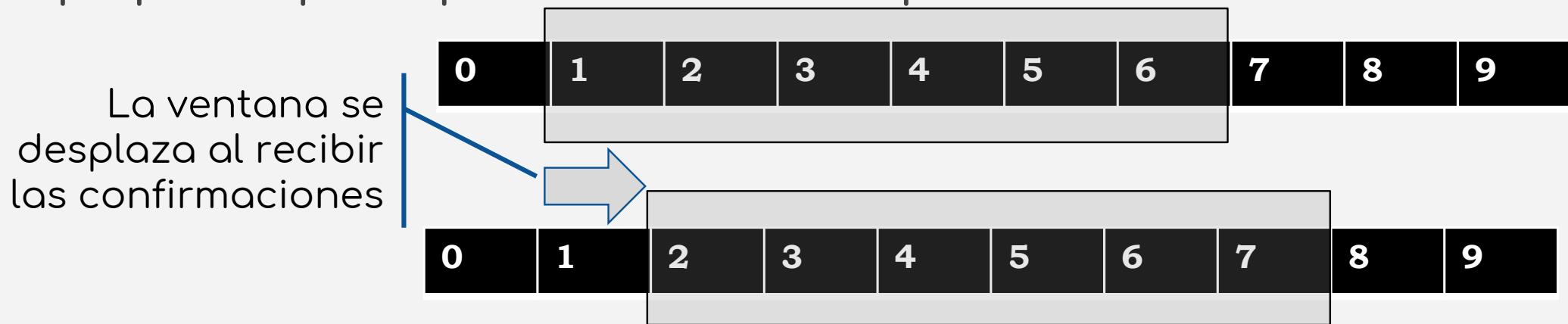
Protocolos de parada y espera



Ventana deslizante

Concepto de ventana deslizante:

- Para el **emisor**: Una ventana (de emisión) es el conjunto de paquetes que se pueden enviar sin esperar confirmación



- Para el **receptor**: Una ventana (de recepción) es el conjunto de paquetes que debe estar preparado para recibir

Los mensajes usan **m bits para numerar** los paquetes:

- Numeración**: Mensajes numerados de $[0, 2^m - 1]$
- Máximo tamaño de ventana**: 2^m

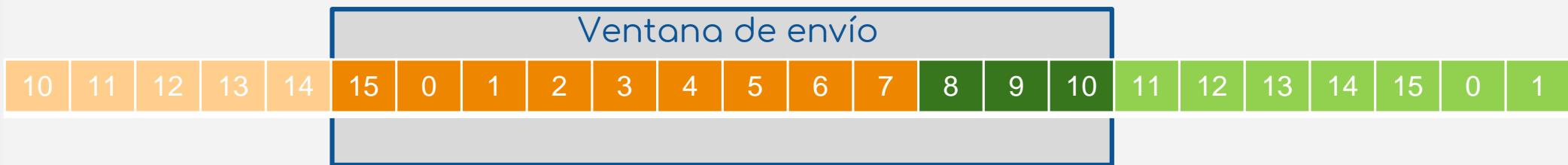
Ventana deslizante



18

Ejemplo:

- $m = 4$ bits \Rightarrow Numeración: [0, 15]
- Tamaños posibles de la ventana: [1, 16] \Rightarrow Tamaño elegido: 12



- Confirman las tramas 15, 0 y 1



Protocolo Go-Back-N

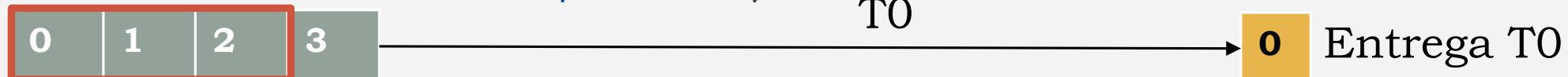
Características:

- Permite al **emisor** tener múltiples paquetes sin confirmar, sin que el receptor tenga que almacenar los paquetes en un buffer (**Tamaño de la ventana de envío < 2^m**):

Si $m=2 \rightarrow W < 4$.

Si $m=3 \rightarrow W < 8$.

- El **receptor** sólo almacena el paquete que espera recibir (**Tamaño de la ventana de recepción = 1**)



- El **receptor** sólo confirma si recibe la trama indicada en su ventana. ACK con el número de trama que espera recibir (**confirmación positiva**)



- Si la trama recibida no es la esperada, no contesta ni hace nada

Protocolo Go-Back-N

20

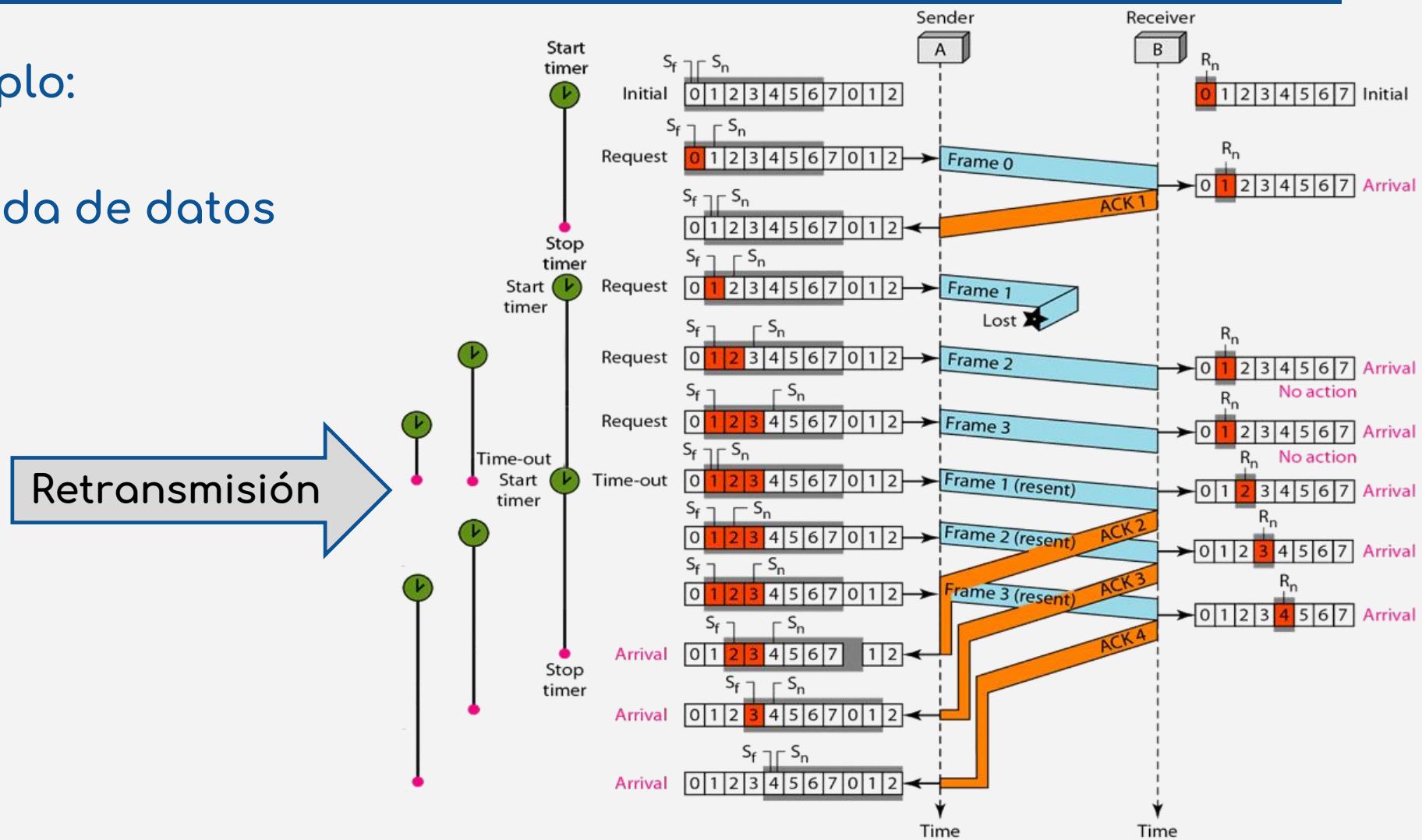
Características:

- La recepción de un ACK con número de secuencia X permite al receptor confirmar todas las tramas pendientes con número de secuencia < X (**confirmación acumulada** o acumulativa)
- Control de errores
 - Pérdida de tramas de datos
 - Uso de **temporizadores** en el emisor.
 - Cuando se cumple sin haber recibido la confirmación positiva se reenvían (retransmisiones) todas las tramas de datos pendientes de confirmación
 - Pérdida de ACK
 - El **siguiente ACK** realiza la misma función (**acumulativos**)
- Más eficiente que parada y espera

Protocolo Go-Back-N

Ejemplo:

Perdida de datos

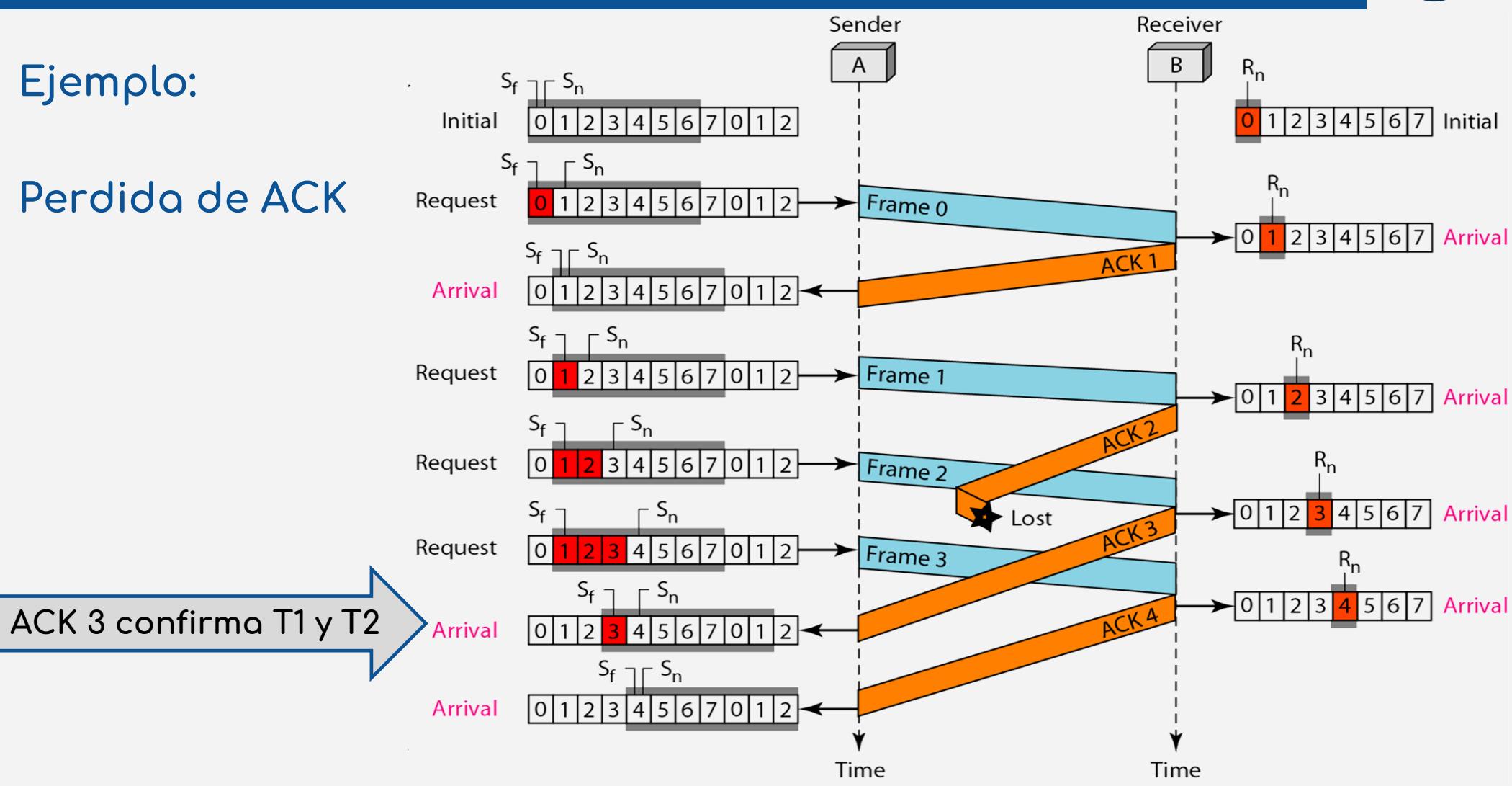


Protocolo Go-Back-N

22

Ejemplo:

Perdida de ACK





Ejercicio

23

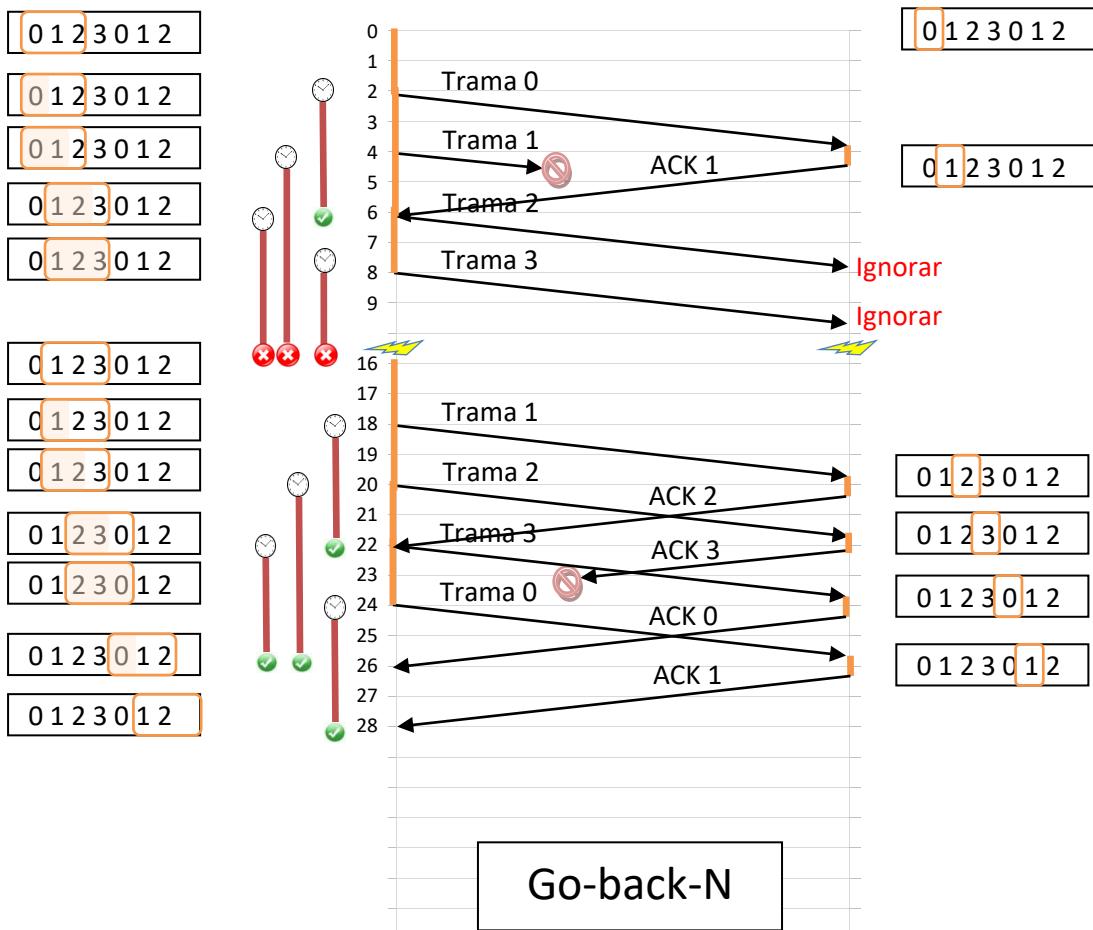
Dos máquinas A y B se encuentran conectadas mediante un enlace con las siguientes características:

t_{trans_datos}	= 2 ms	t_{prop}	= 1.75 ms
t_{proc}	= 0.25 ms	t_{trans_ACK}	= 0.25 ms
timeout	= 12 ms	numeración	= 2 bits

El envío tiene las siguientes características:

- La máquina A envía un archivo que requiere 5 tramas a B
- Se pierde la segunda trama que envía A
- Se pierde también la tercera confirmación enviada por B

Determine los eventos que ocurrirán en cada máquina hasta que el archivo esté totalmente para el protocolo Go-Back-N



Protocolo Repetición Selectiva

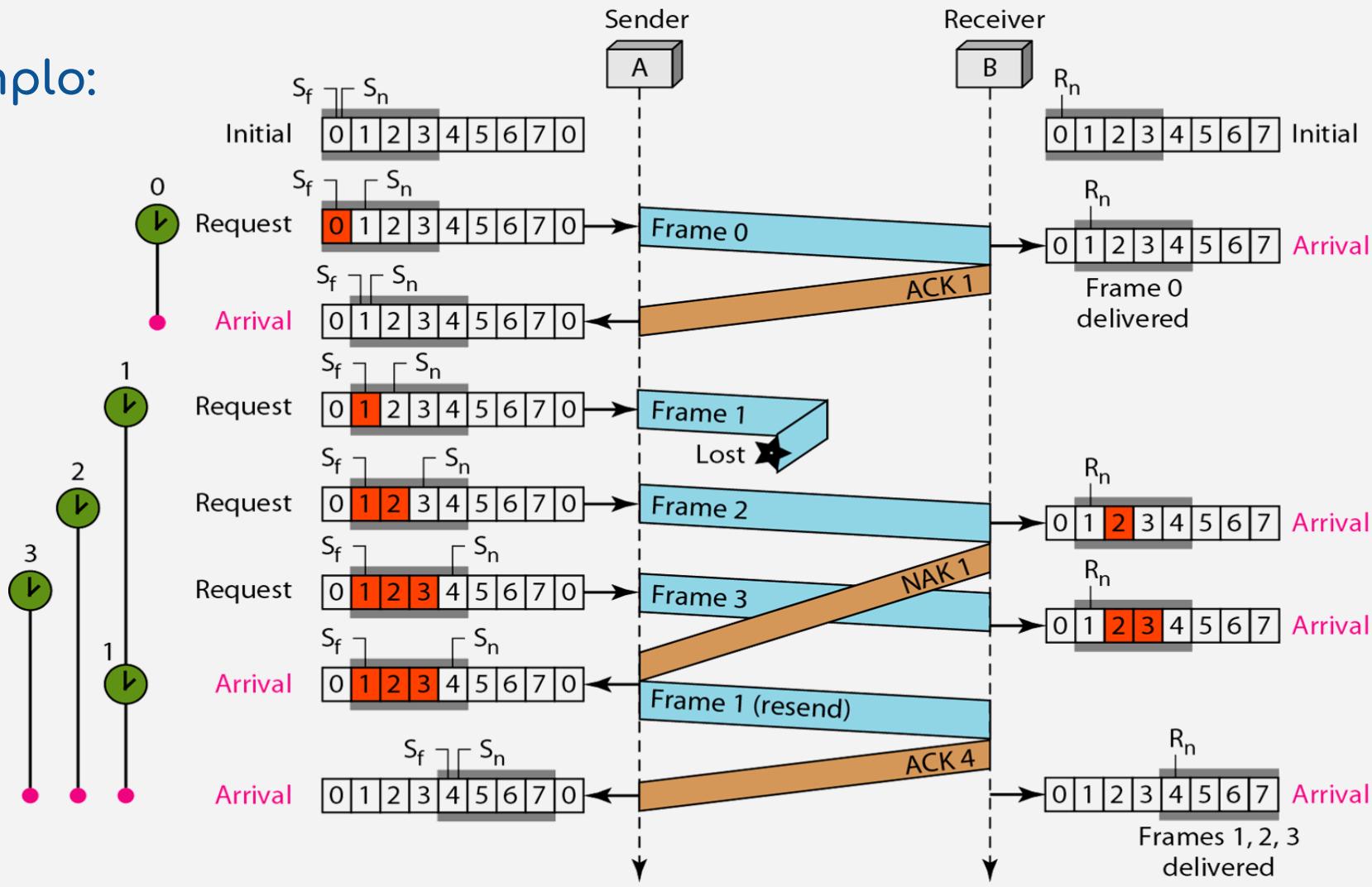
24

Características:

- Solo se retransmiten aquellas tramas no confirmados:
 - Las tramas pueden llegar fuera de orden
- En el emisor:
 - Es necesario un buffer para almacenar las tramas no confirmados (Tamaño máximo ventana de envío: 2^{m-1})
 - Reenvía tramas a petición del receptor o por temporizador
- En el receptor:
 - Es necesario un buffer para almacenar las tramas que llegan fuera de orden (Tamaño máximo ventana de recepción: 2^{m-1})
 - Si recibe una trama no esperada, envía una petición de repetición (NAK, confirmación negativa) con la que esperaba
 - Confirmación (POSITIVA) acumulativa

Protocolo Repetición Selectiva

Ejemplo:



Ejercicio

26

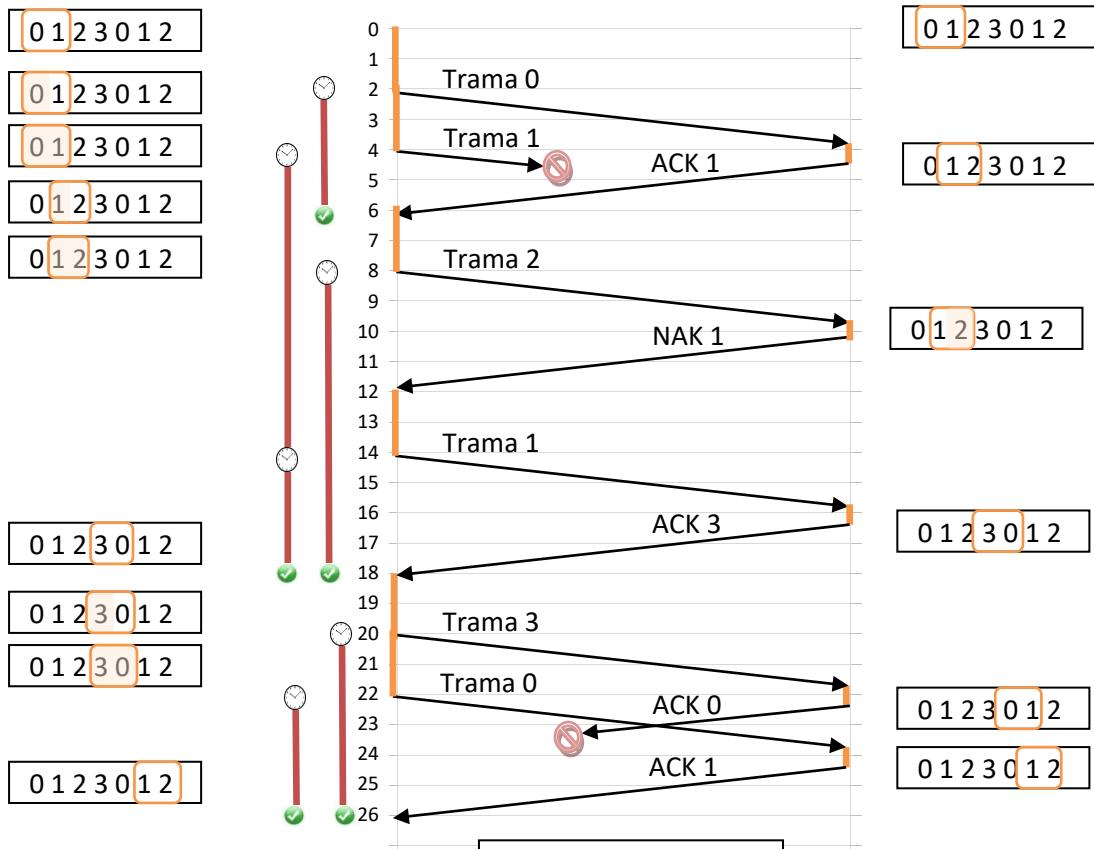
Dos máquinas A y B se encuentran conectadas mediante un enlace con las siguientes características:

t_{trans_datos}	= 2 ms	t_{prop}	= 1.75 ms
t_{proc}	= 0.25 ms	t_{trans_ACK}	= 0.25 ms
timeout	= 12 ms	numeración	= 2 bits

El envío tiene las siguientes características:

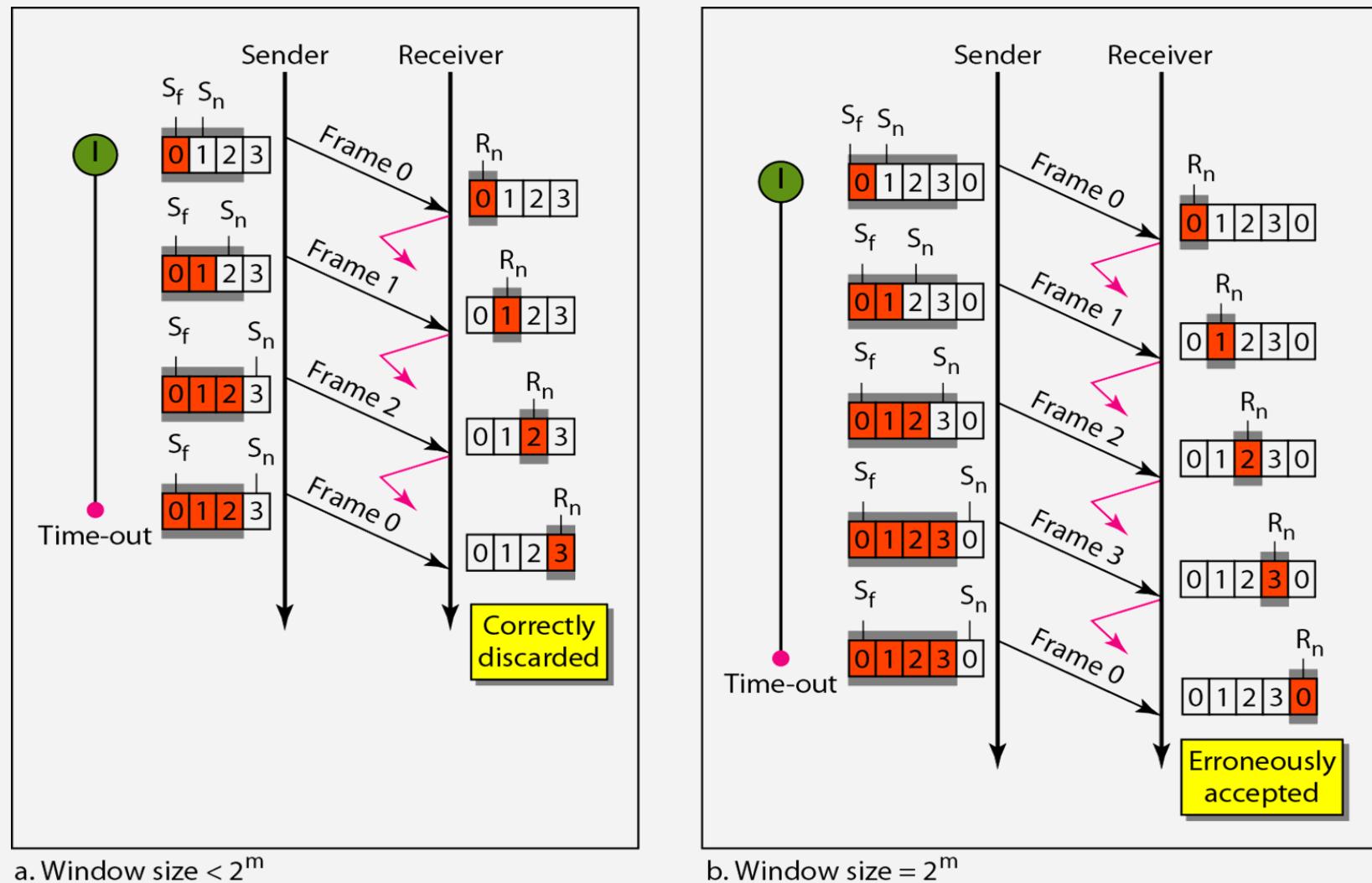
- La máquina A envía un archivo que requiere 5 tramas a B
- Se pierde la segunda trama que envía A
- Se pierde también la tercera confirmación enviada por B

Determine los eventos que ocurrirán en cada máquina hasta que el archivo esté totalmente para el protocolo Repetición Selectiva



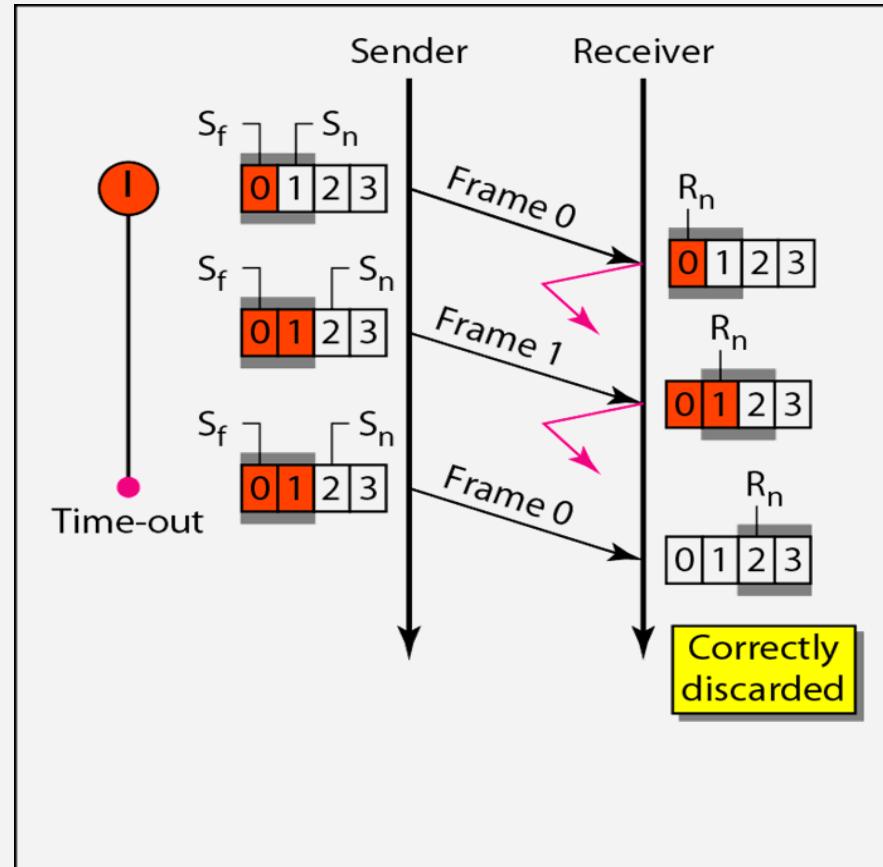
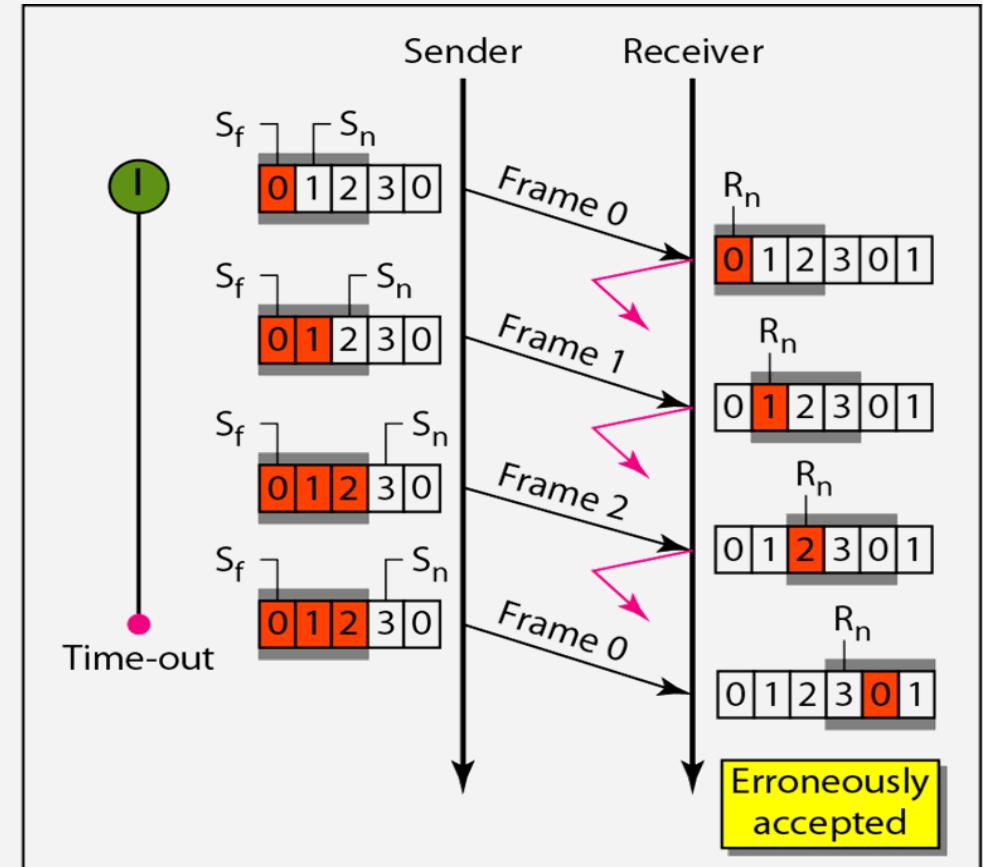
Numeración y tamaño de ventana

Go-Back-N:



Numeración y tamaño de ventana

Repetición selectiva:

a. Window size = 2^{m-1} b. Window size $> 2^{m-1}$

Tema 2: Capa de Enlace

Clase del 13/02/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)

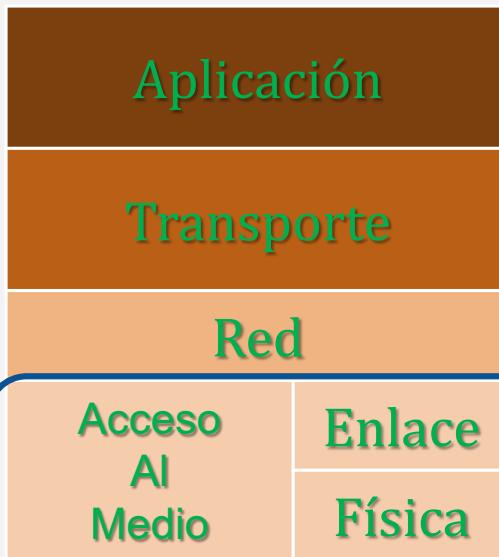


Contexto

2

Comunicar equipos es complejo => **Modelo de capa**, donde cada nivel/capa añade una mejora/funcionalidad a anterior. La arquitectura de capas usada en Internet es **TCP/IP**.

Capa



Función

- | | |
|--|-----------------|
| Servicio ofrecido al usuario (web, correo, mensajería, streaming...) | Aplicación |
| Conexión extremo a extremo entre procesos (y que vaya bien) | Transporte |
| Envío entre equipos no conectados directamente | Red |
| Envío entre equipos conectados directamente | Acceso Al Medio |
| Envío de bits | Enlace Física |

Repaso de protocolos de control

Características	Parada y Espera (Stop & Wait – S&W)	Go-Back-N (GBN)	Repetición Selectiva (Selective Rep. – SRP)	
Numeración	{0,1} (1 bit)	{0, 1, ..., 2 ^m -1} (m bits)	EMISOR	
Ventana envío	1	< 2 ^m		
Envío	Si dentro de la ventana hay numeración sin que ya fuese enviado			
Salta temporizador	Retransmisión todas las pendientes	Retransmite la que salta		
Recibe ACK X	Confirma todas las tramas en la ventana < X (avanza la ventana a la primera no confirmada)			
Recibe NAK X	-	Retransmite la X		
Ventana recepción	1	Igual ventana de envío		
Llega la primera trama en ventana	Confirma la siguiente a recibir y avanza la ventana hasta que al inicio de la misma haya una no recibida			
Llega una trama fuera de la ventana	Descarta y reenvía ACK	Descarta y no envía nada		
Llega una trama que no es la primera	-	Almacena (la apunta en la ventana) y envía NAK de la primera		

Variante examen Mayo'16

Ventana emisor (N=4)

0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8

0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8

0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8

emisor

T0

T1

T2

T3

(wait)

T4

T5



Timeout T2

T2

Almacena ack4

Almacena ack5

receptor

ack0

ack1

ack3

Almacena ack3

Almacena T5

envía ack5

entrega T2, T3, T4, T5, envía ack2

Almacena T4

envía ack4

Almacena ack2

- ACK NO acumulativos

- ACK X confirma T-X

- Temporizador por T-Y y si salta se reenvía T-Y

- Error: no hacer nada

- Se guardan Tramas y ACKs fuera de orden

- ¿Cuántas tramas puede enviar el emisor hasta que se le cierra la ventana (en general y en la situación mostrada al final de la figura)?
- ¿Cómo detecta el emisor que se ha perdido la trama 2 (T2)?
- ¿Qué acciones realiza el emisor cuando llega el ack2?
- Describa un mecanismo para recuperarse de un ack perdido y qué requisitos necesita para que funcione.

Variante examen Mayo'16

5

¿Cuántas tramas puede enviar el emisor hasta que se le cierra la ventana (en general y en la situación mostrada al final de la figura)?

En general: 4 (tamaño de la ventana)

La situación final: 0 (ventana llena)

¿Cómo detecta el emisor que se ha perdido la trama 2 (T2)?

Salta el temporizador

¿Qué acciones realiza el emisor cuando llega el ack2?

Desplaza la ventana hasta 6

Describa un mecanismo para recuperarse de un ack perdido y qué requisitos necesita para que funcione.

Cuando se pierde un ack, saltará el temporizador y se reenviará la trama. Eso provocará que el receptor recibirá una trama repetida.

El receptor al recibir una trama fuera de la ventana o repetida, la descarta pero la debe confirmar.

Para evitar aceptar una repetida como nueva $N \leq 2^{m-1}$

Piggybacking

- Los protocolos vistos son adecuados para **flujos de datos unidireccionales**
- Las aplicaciones intercambian datos **en ambos sentidos**
 - Necesario flujo de datos y flujo de control bidireccional
 - Baja eficiencia de los protocolos unidireccionales
- **Piggybacking** (información de control “a cuestas”)
 - Transporta información de control (ej: ACK, NAK) junto con los datos
 - Se definen dos ventanas de recepción y dos de emisión
 - Ej: HDLC, LLC, TCP...



Organización del tema y la clase

- Funcionalidad de la capa y **principales servicios** ✓
- **Técnicas genéricas** para solventar esos problemas:
 - Control de error: detección✓ y actuación✓
 - Control de flujo ✓
 - Difusión: **Direccionamiento** y Acceso al medio
- **Casos concretos:**
 - Con medio cableado:
 - **Ethernet (802.3)**
 - **Token Ring (802.5)**
 - Con medio inalámbrico:
 - **Wifi (802.11)**
 - **Bluetooth (802.15.1)**
 - Alto nivel:
 - **PPP (RFC 1661)**

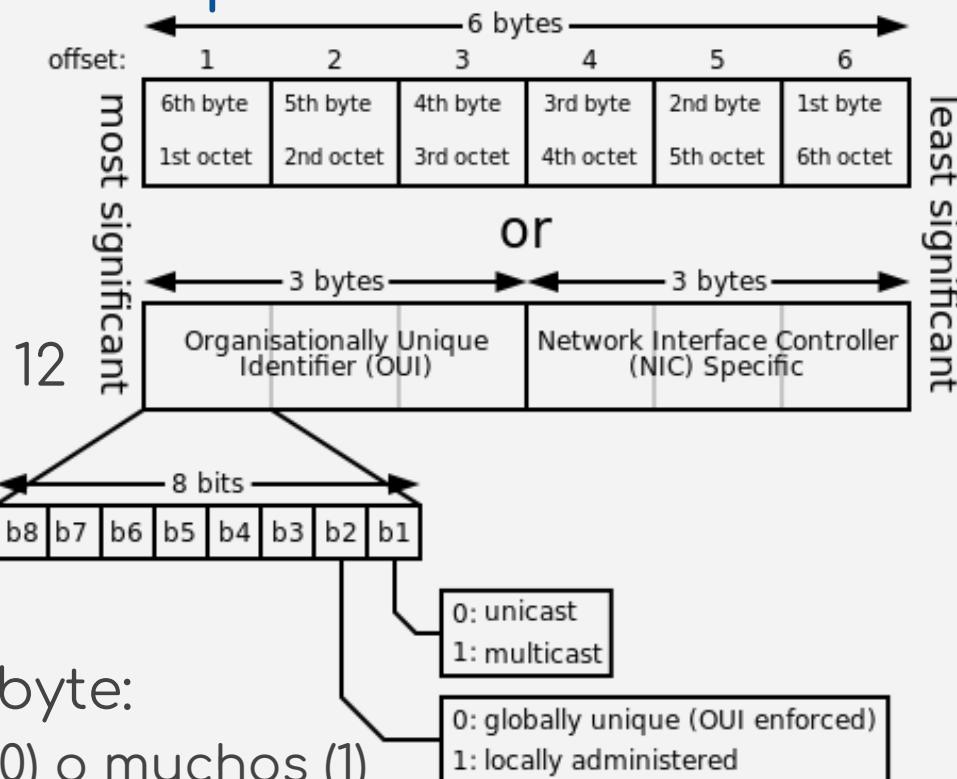
Difusión: direccionamiento

¿Cómo identificar el destino es un medio compartido?

- Direcciones MAC: 6 bytes
- También llamada:
 - Dirección hardware
 - Dirección física
- Representados habitualmente como 12 dígitos hexadecimal, separados por dos puntos:

68:07:15:1f:99:a5

- 3 primeros bytes: **fabricante**. Primer byte:
 - Menos significativo 1 bit: Un equipo (0) o muchos (1)
 - Segundo menos significativo 1 bit: Global (0) o local (1)
- 3 últimos bytes: **identificador**.



Difusión: direccionamiento

¿Cuál dirección MAC estamos usando?

- Windows:
 - ipconfig / all
 - get mac
- Linux / Mac / Android (con emulador de terminal):
 - ifconfig -a (en Linux recientes requiere instalar net-tools)
 - ip link show (en Mac requiere instalar iproute2mac)
- Android:
 - Ajustes -> Acerca el teléfono -> Estado
- iPhone:
 - ~~Regaladme un iPhone y lo miro~~
 - Ajustes -> General -> Información

¿Se puede cambiar?

- Generalmente sí, aunque puede requerir ser administrador:
 - sudo ip link set dev INTERFAZ address NUEVAMAC

Redes de área local IEEE 802

El estándar IEEE 802

IEEE 802.x

OSI

IEEE 802.x							LLC	MAC	Física	2	1
Control del Enlace Lógico											
802.2											
802.3 csma-cd	802.4 token-bus	802.5 token-ring	802.6 dqdb	802.7 b. ancha	802.8 fibra ópt.	802.9 rdsi					

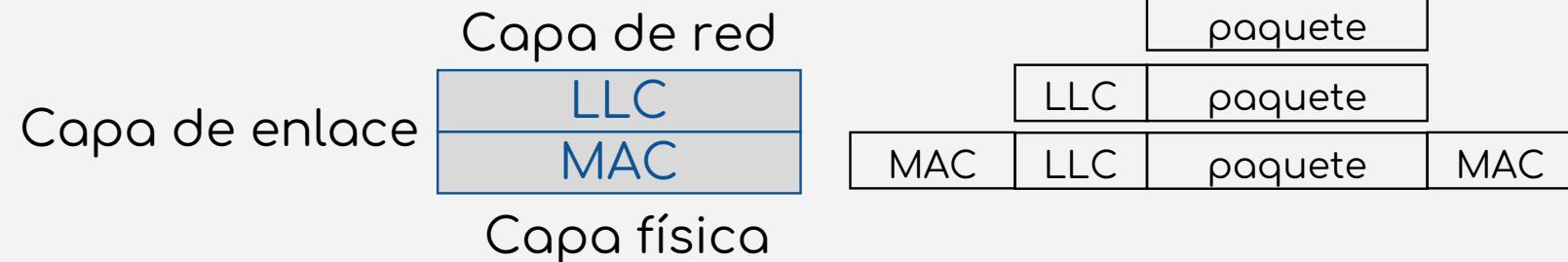
MAC (Medium Access Control)

Control de Acceso al Medio

LLC (Logical Link Control)

Control del Enlace Lógico

La capa LLC (Logical Link Control) ofrece una **interfaz entre la capa de red y la capa MAC**

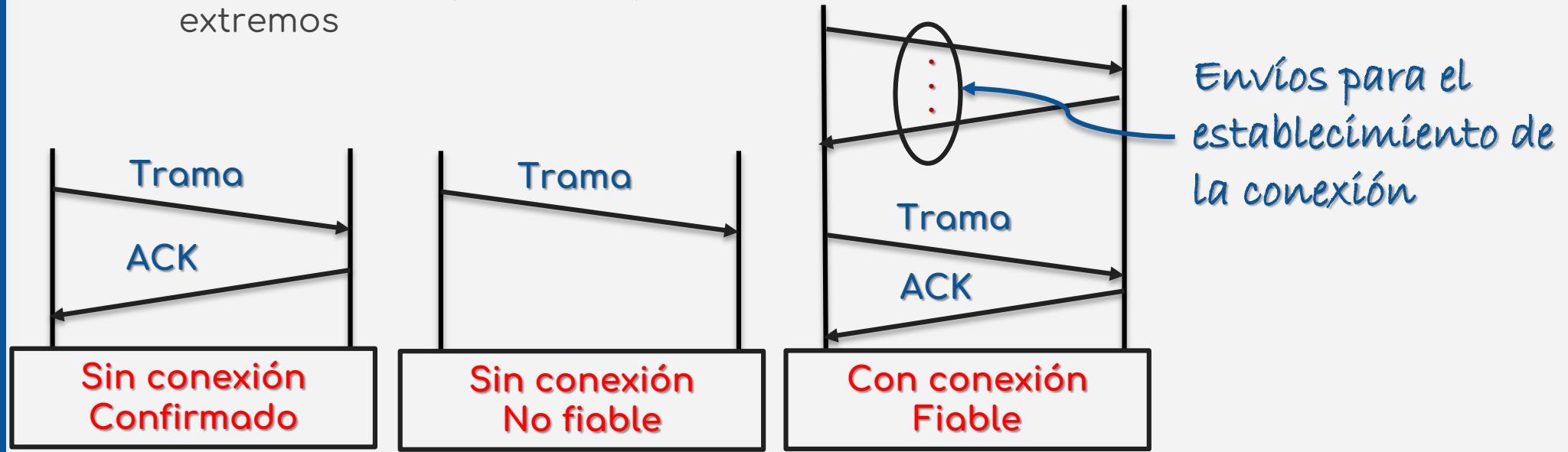


Redes de área local IEEE 802

Servicios que ofrece LLC:

- Servicio sin conexión confirmado
 - No se puede enviar una trama si no se ha confirmado la anterior
- Servicio sin conexión no fiable
 - No se garantiza que el paquete llegue bien a su destino
- Servicio orientado a la conexión fiable
 - Tiene una fase/primitivas para el establecimiento de una conexión con el otro extremo

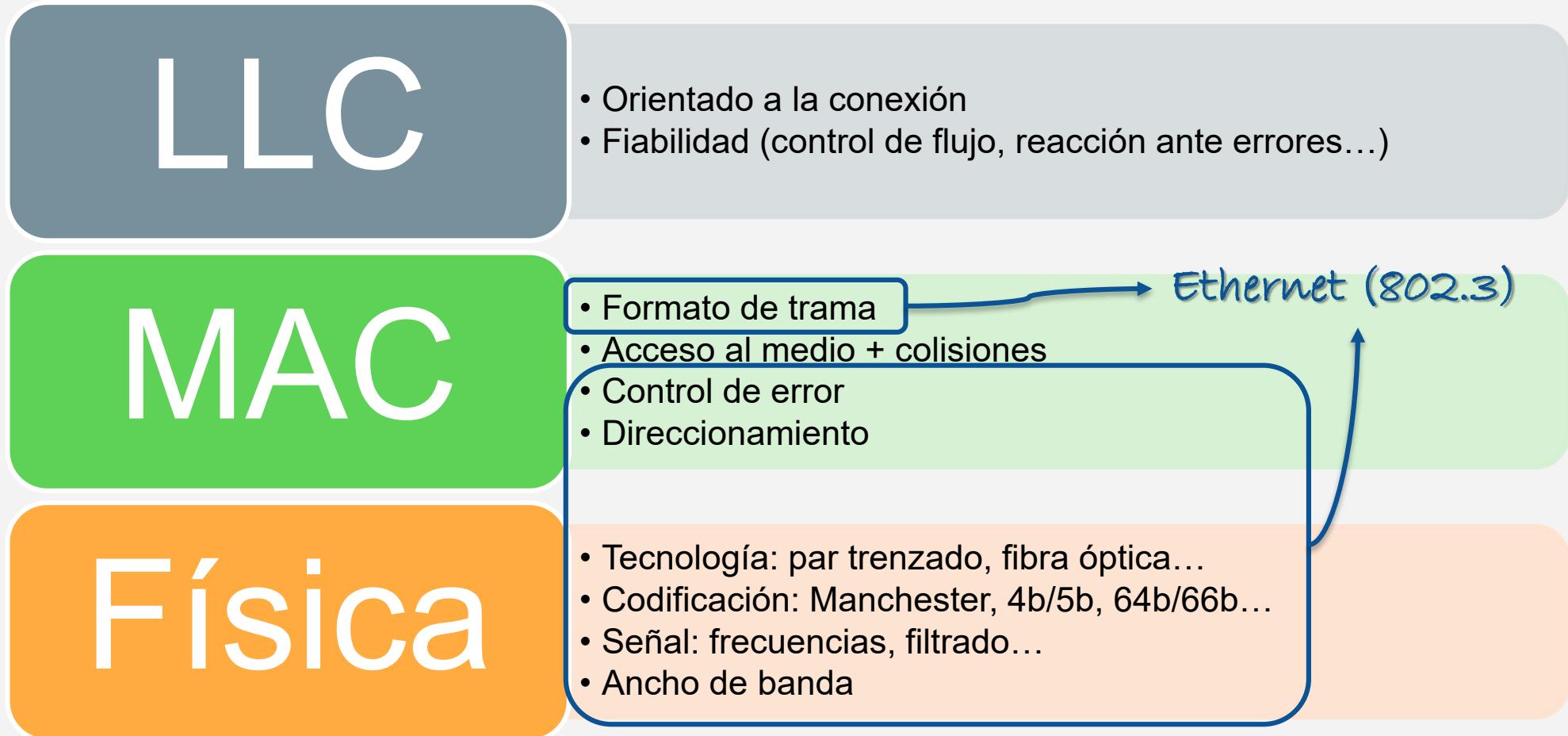
Las LANs y MANs así:
"best effort"



Redes de área local IEEE 802

12

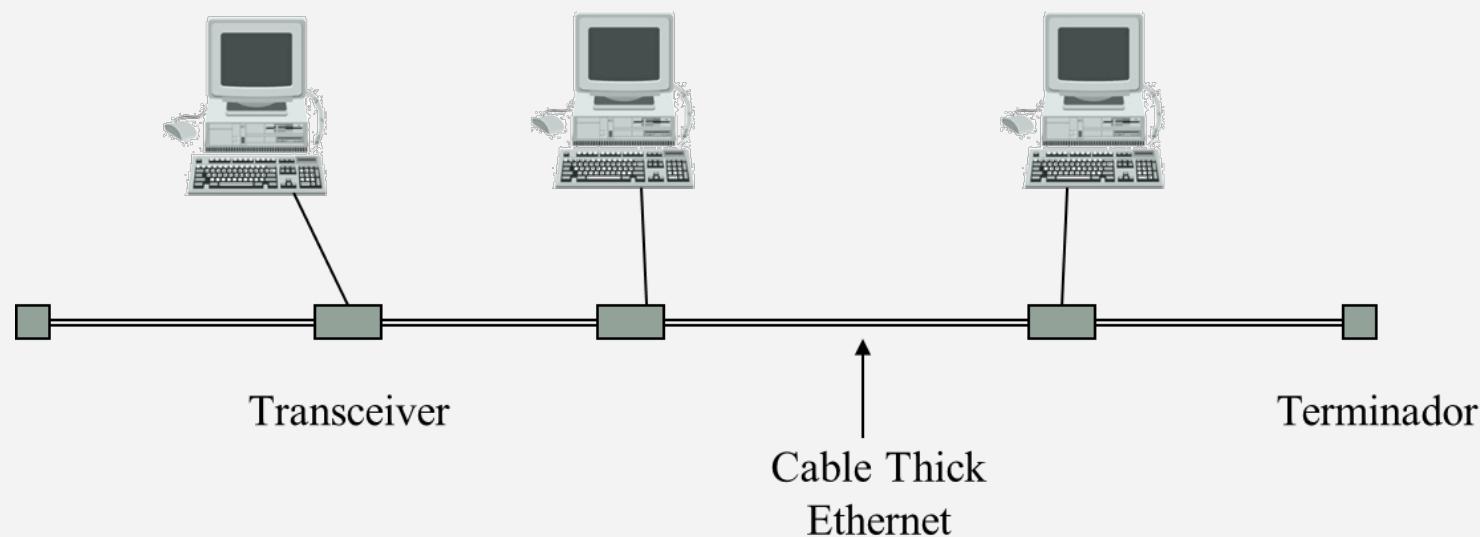
Capas en IEEE 802



Red IEEE 802.3 (Ethernet)

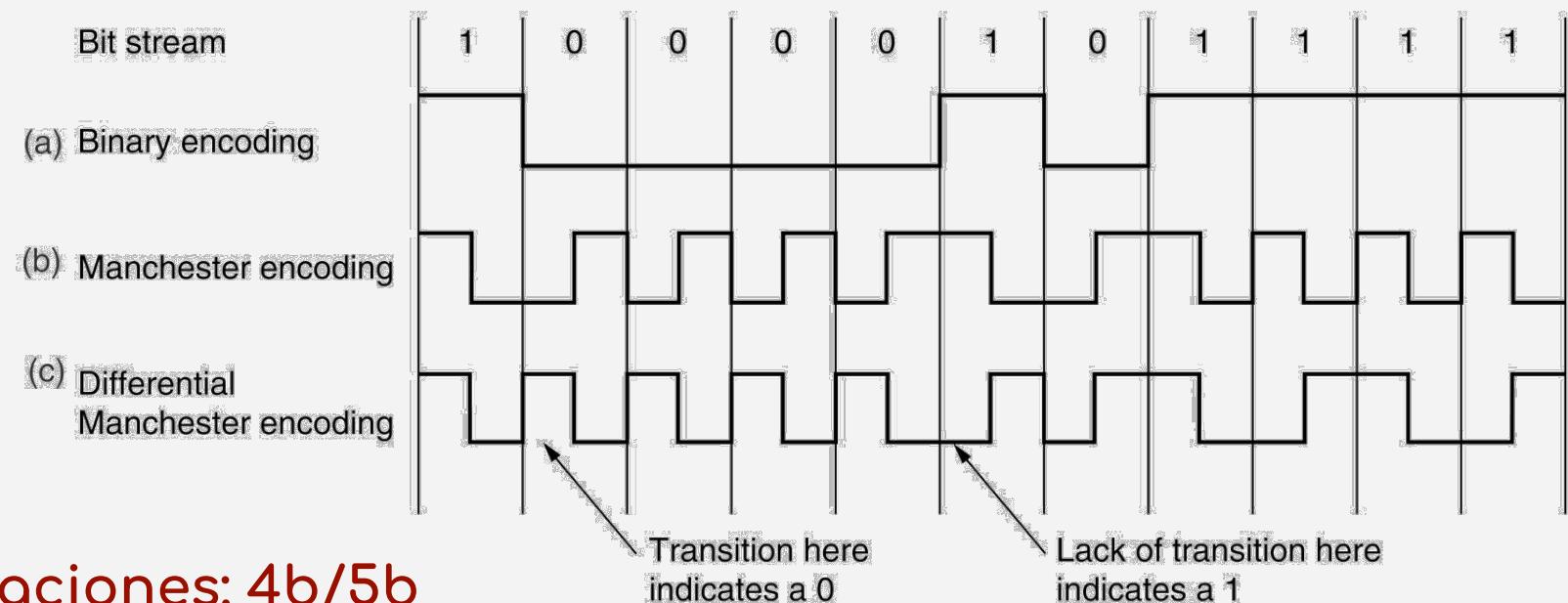
El estándar IEEE 802.3 define la red Ethernet

- Es la red **más usada** hoy día (versión Fast o Gigabit Eth.)
- Fue desarrollada por **Xerox** en los años **70** (los primeros estándares IEEE 802.3 son del 1983).
- Tradicionalmente la red tenía **topología de bus**
- Usa un protocolo MAC de tipo **CSMA-CD**



Red IEEE 802.3 (Ethernet)

Codificación Manchester



Otras codificaciones: 4b/5b

- Binario pero para evitar muchos valores consecutivos hace un mapeado de cada 4b en 5b evitando eso
- Más eficiente (80% vs 50%)

Mejoras: 64b/66b

Red IEEE 802.3 (Ethernet)

Especificaciones IEEE 802.3 a 10 Mbps (Ethernet)

	10Base5	10Base2	10Base-T	10Broad36	10Base-FP
Medio	Coaxial	Coaxial	Par trenzado	Coaxial	Fibra óptica
Diámetro	10 mm (<i>thick</i>)	5 mm (<i>thin</i>)	0,4-0,6 mm	0,4-1,0 mm	62,5/125 µm
Codificación	Manchester	Manchester	Manchester	DPSK	Manchester
Máx. segm.	500 m	185 m	100 m	1800 m	500 m
Nodos/segm.	100	30	1024	1024	33
Topología	Bus	Bus	Estrella	Bus/Árbol	Estrella

Ejemplos: 100BASE-T4, 10GBASE-CX4, 10GBASE-LR

Velocidad: 10, 100, 1000 (Mbps), 10G, 2.5G (Gbps), ...

Señalización: Base (sin nada), Pass (con filtro), ...

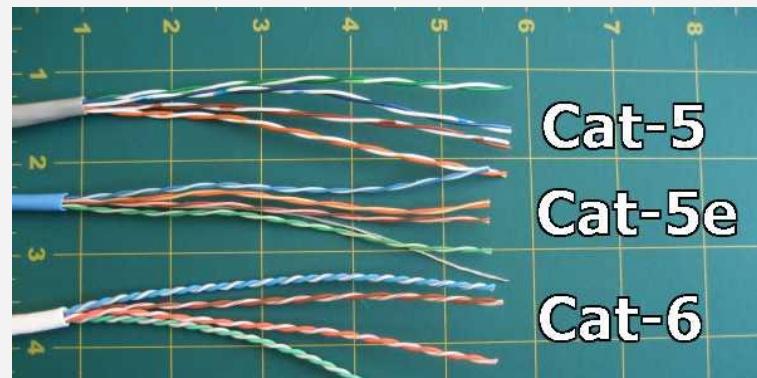
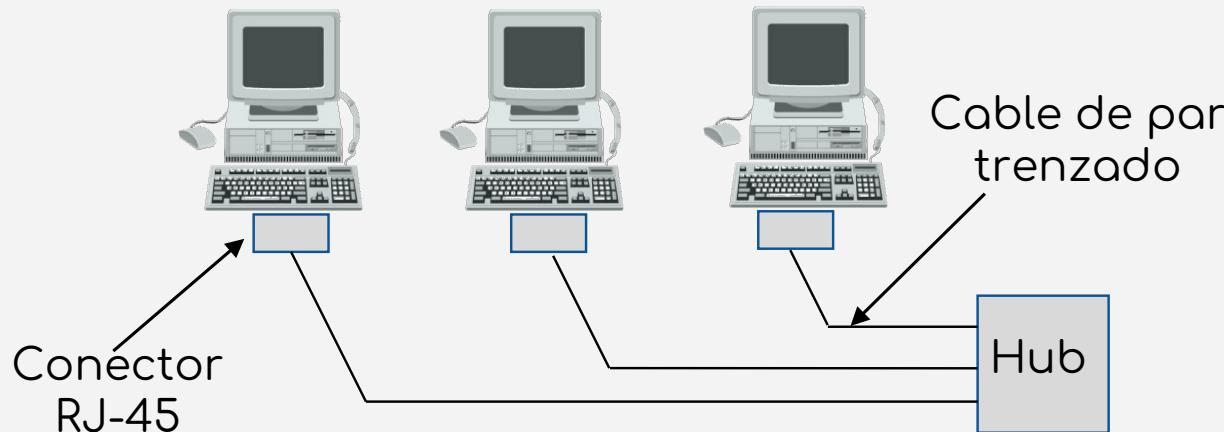
Medio: -T (par trenzado), 2,5,36 (Coaxial), -C (cobre), -L/F/... (fibra)

Codificación: por defecto (Manchester), X (4 → 5), R (64 → 66)

Canales en paralelo: por defecto (1), 2, 4, ...

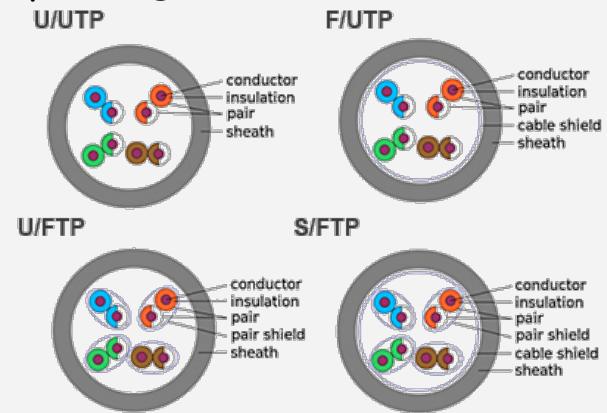
Red IEEE 802.3 (Ethernet)

Ethernet con par trenzado



Estandar IEC/ISO pero no TIA
Telecommunications Industry Association

Topología lógica: **bus**
Topología física: **estrella**



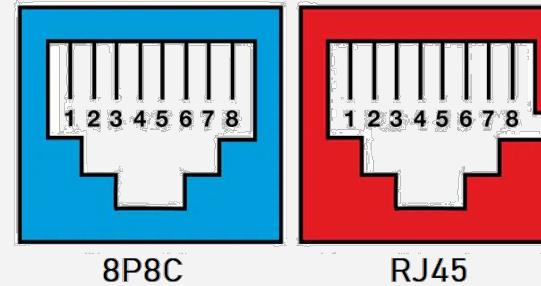
Cable	Tipo	BW	Uso (100 m)
Cat5	U/UTP	100 Mhz	100Base-TX
Cat5e	U/UTP	100 Mhz	1GBase-T
Cat6	U/UTP	250 Mhz	1GBase-T
Cat6A	U/FTP	500 Mhz	10GBase-T
Cat7	S/FTP	600 Mhz	10GBase-T
Cat8	S/FTP	1,6 - 2 Ghz	40GBase-T (30 m)

Red IEEE 802.3 (Ethernet)

17

Materiales

- Cable 5e o superior
- Conector RJ45 (8P8C)
- Crimpadora
- Opcional: pelacables, testeador



Pasos

- Pelar cable
- Ordenar cables según T568A o T568B
- Meterlos en el conector
- Apretarlo con la crimpadora
- Rezar para que todo vaya bien

PIN	T568A	T568B
1	white and green	white and orange
2	green	orange
3	white and orange	white and green
4	blue	blue
5	white and blue	white and blue
6	orange	green
7	white and brown	white and brown
8	brown	brown

<https://www.youtube.com/watch?v=5FagmAlbD-I>

Red IEEE 802.3 (Ethernet)

Formato de la trama de Ethernet II:

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 octetos	6 octetos	6 octetos	2 octetos	46- 1500 octetos	4 octetos

- **Preámbulo:** 7 bytes para sincronizar + 1 inicio de trama
- **Direcciones MAC origen y destino**
- **Tipo de trama** (Ethernet II – valor >1536) o longitud de la trama sin preámbulo (802.3 – valor < 1500)
- **Datos** del protocolo encapsulado (puede ser necesario “relleno/padding”)
- **Control de errores:** CRC (32 bits)
- **IPG:** tiempo de espera entre tramas (gap aproximado de 96 bits)

Tema 2: Capa de Enlace

Clase del 14/02/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)



Organización del tema y la clase

- Funcionalidad de la capa y **principales servicios** ✓
- **Técnicas genéricas** para solventar esos problemas:
 - Control de error: detección✓ y actuación✓
 - Control de flujo ✓
 - Difusión: Direcccionamiento✓ y **Acceso al medio**
- **Casos concretos:**
 - Con medio cableado:
 - Ethernet (802.3) ✓
 - Token Ring (802.5)
 - Con medio inalámbrico:
 - Wifi (802.11)
 - Bluetooth (802.15.1)
 - Alto nivel:
 - **PPP (RFC 1661)**

Acceso al medio

En enlaces **punto a punto**:

- Se debe garantizar el envío de bits de un extremo a otro



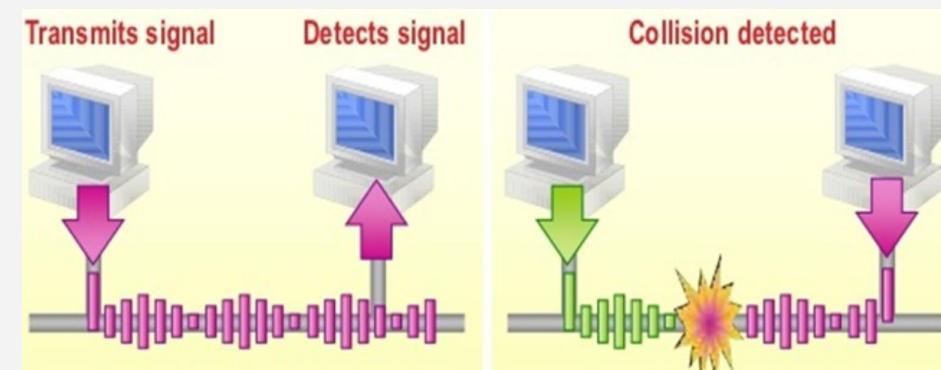
En enlaces de **difusión**:

- Además, hay que controlar el acceso al medio compartido
- **Protocolos MAC: Medium Access Control**



Pueden existir **colisiones**

- Una colisión se produce cuando dos tramas se transmiten a la vez
- Las colisiones son detectables (directa o indirectamente)
- Una trama que colisiona debe ser retransmitida

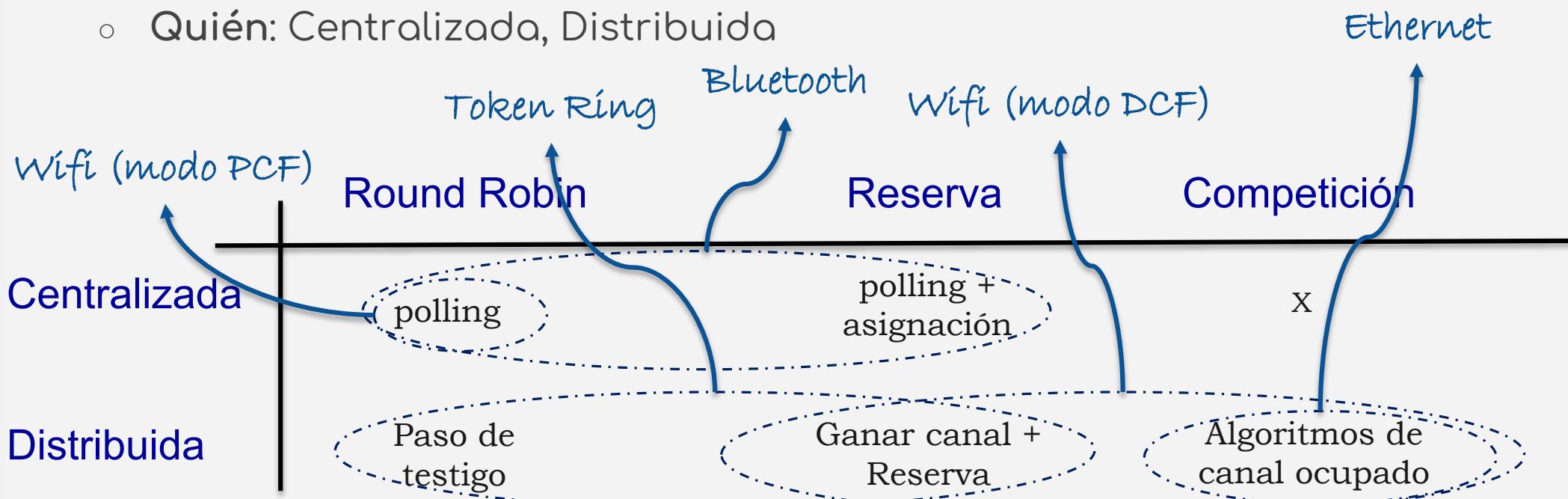


Control de acceso al medio: resumen

4

Asignación (a quién le toca):

- Estática:
 - FDM y TDM
- Dinámica:
 - Cómo: Round Robin, Reserva, Competición
 - Quién: Centralizada, Distribuida



Algoritmos de canal ocupado: ALOHA

5

El protocolo ALOHA es un protocolo MAC:

- Principios de los 70 en las islas Hawái
- Comunicación por radio (**medio de difusión**)

Idea básica

- Las estaciones transmiten paquetes de **longitud fija** cuando tienen datos que enviar
- **No existe detección de portadora** (posibles colisiones)

El nodo central confirma con ACK

- Si el emisor no recibe ACK tras un timeout supone que su paquete colisionó y lo **reenviará tras un retraso aleatorio**

Sin embargo, es poco eficiente 18%

- Una variante, el Aloha Slotted llega al 37%
- Baja eficiencia porque no utiliza detección de portadora

Protocolos basados en CSMA

CSMA (Carrier Sense Multiple Access)

- (1) Detecta si alguien está transmitiendo en ese momento. Esta transmisión se detecta por la presencia de una señal portadora
- (2) Si el canal está inactivo, la estación puede transmitir
- (3) Si el canal está activo, la estación no puede transmitir => Algoritmos de canal ocupado:
 - CSMA no persistente
 - CSMA 1-persistente => CSMA/CD
 - CSMA p-persistente
- (4) Si hay colisión:
 - Las variantes simples no comprueban colisiones

Protocolos basados en CSMA

CSMA 1-persistente:

- Revisa en canal y envía en cuanto puede.

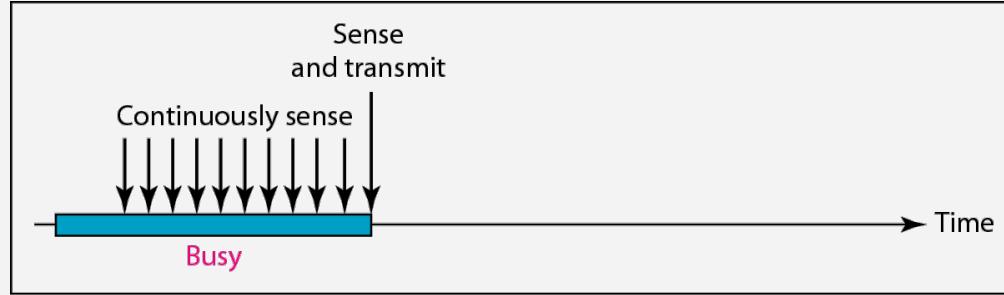
CSMA no persistente:

- Espera tiempos aleatorios.

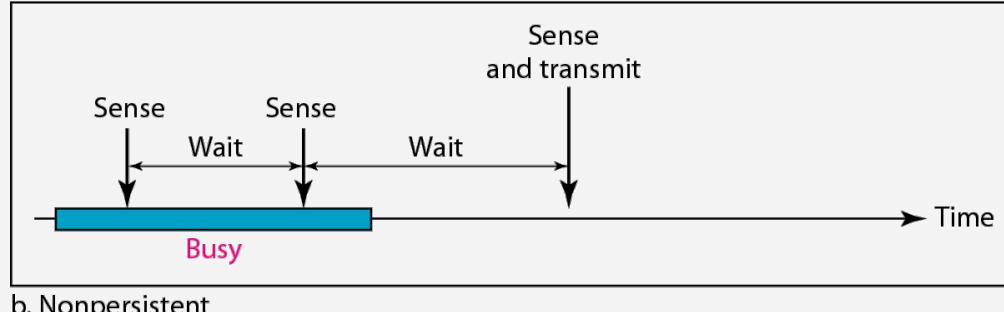
CSMA p-persistente:

- Se usa cuando el tiempo se divide en intervalos (slots)
- Cuando detecta el canal libre tiene una probabilidad p de enviar sino espera al siguiente slot.

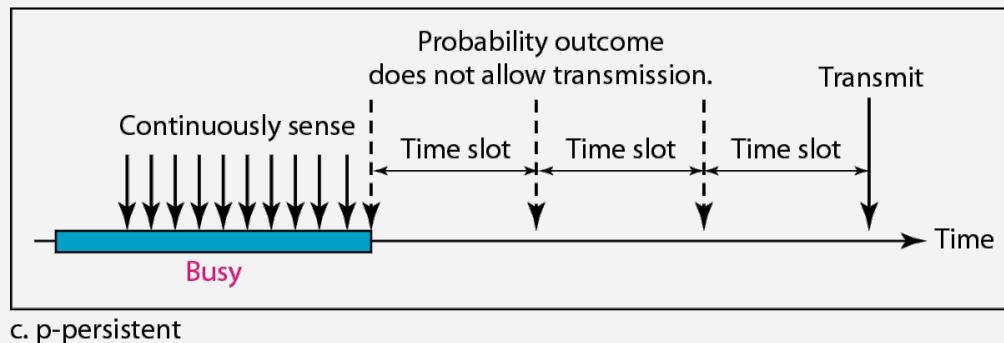
¿Ventajas e inconvenientes?



a. 1-persistent

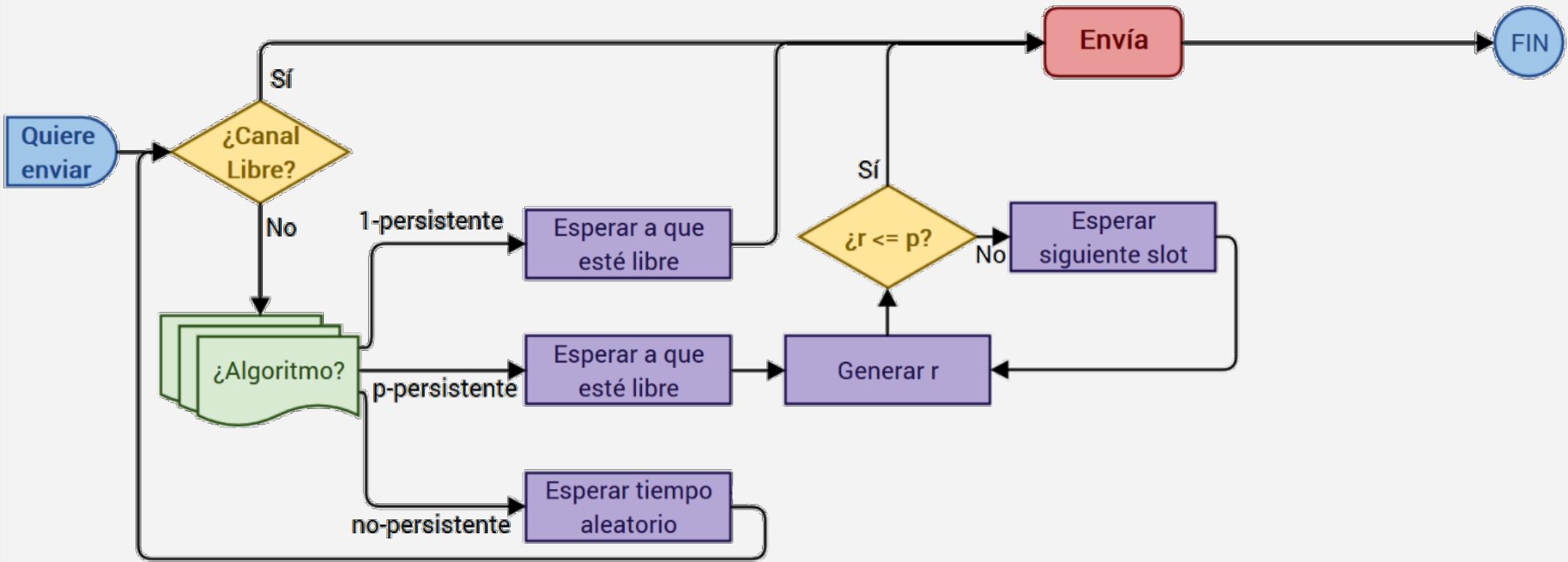


b. Nonpersistent



c. p-persistent

Protocolos basados en CSMA



Protocolos basados en CSMA/CD

CSMA/CD

- Carrier Sense Multiple Access with **Collision Detection**
- Se basa en que las estaciones abortan la transmisión tan pronto como detectan una colisión
 - En los protocolos anteriores las tramas se transmiten enteras

Funcionamiento

- Cuando se quiere transmitir
 - Si el canal está libre, se transmite
 - Si el canal está ocupado, se espera hasta que esté libre (**1-persistencia**)
- Si se detecta colisión
 - Se transmite una señal corta de interferencia para informar al resto de estaciones (**señal de jamming**)
 - Y se espera un **tiempo aleatorio** antes de empezar de nuevo

¿Cómo se detecta una colisión?

10



¿Cómo se detecta una colisión?

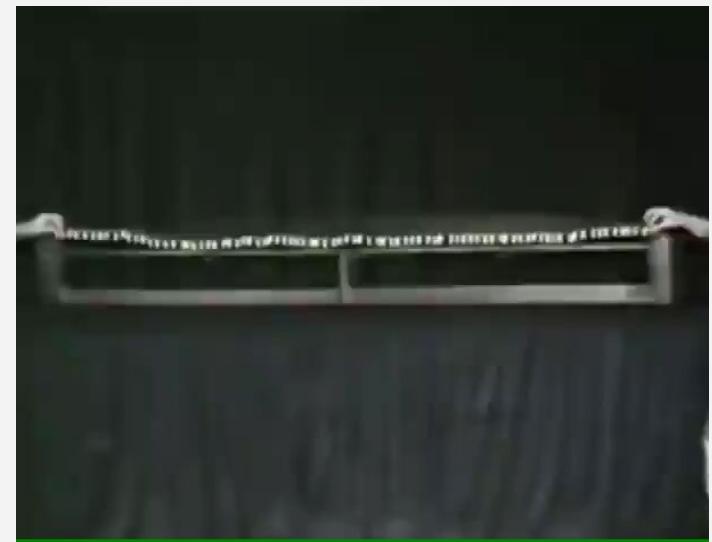
11



¿Cómo se detecta una colisión?

12

¿Es suficiente recibir y enviar simultáneamente para detectar la colisión?



Necesitamos que la trama sea lo suficientemente larga para detectar el peor caso. **¿Cuál es el peor caso?**

Sabiendo que las primeras redes Ethernet tenían un rtt máximo de 50 μ s (peor caso) e iban a 10Mbps, **¿cuál es el menor tamaño (en bytes) para una trama? Y si no hay suficientes datos, ¿qué hacemos?**

¿Cómo se detecta una colisión?

13

Necesitamos que la trama sea lo suficientemente larga para detectar el peor caso. **¿Cuál es el peor caso?**

Que envíe un equipo en un extremo de la red y justo cuando va a llegar al otro extremo de la red, el equipo en ese otro extremo envíe.

Sabiendo que las primeras redes Ethernet tenían un rtt máximo de 50 µs (peor caso) e iban a 10Mbps, **¿cuál es el menor tamaño (en bytes) para una trama?**

Debemos estar transmitiendo al menos esos 50 µs, como sabemos que la $t_{trans} = \text{datos}/\text{BW} \Rightarrow \text{datos} = t_{trans} * \text{BW} = 50 \times 10^{-6} \times 10 \times 10^6 = 500$ bits ≤ 63 B (realmente se usan 64 bytes)

Cabecera = 6 + 6 + 2 + 4 = 18 B -> Mínimo cantidad datos = 46 B

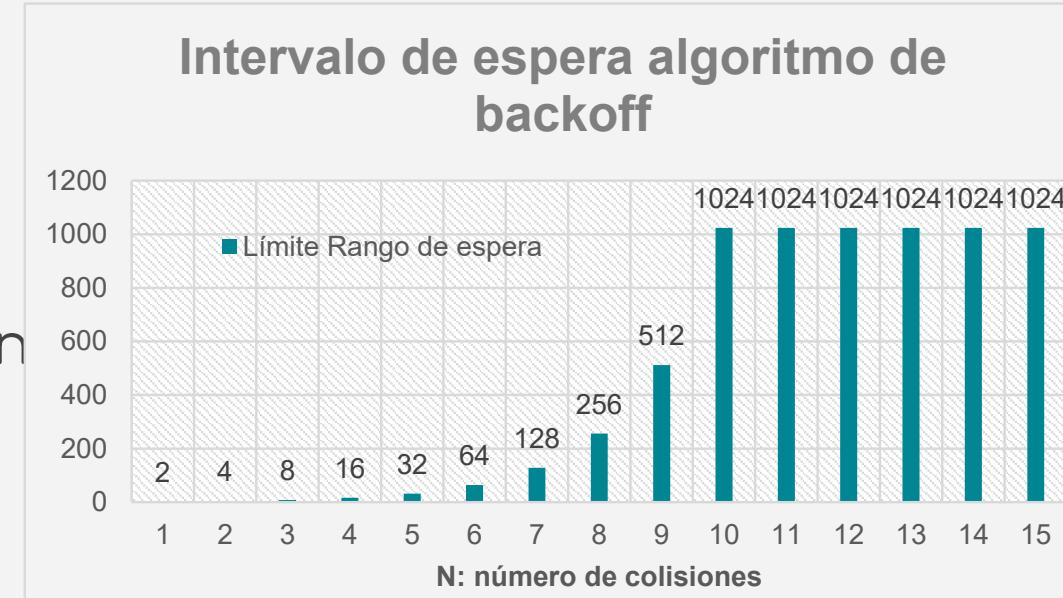
Y si no hay suficientes datos, ¿qué hacemos?

Se rellena con 0s hasta que ocupa 64 B (padding)

Protocolos basados en CSMA

CSMA-CD: Algoritmo de retroceso exponencial binario (Backoff)

- Se utiliza para **definir las esperas** en caso de colisión
- Si el paquete ha colisionado $n < 16$ veces seguidas
 - El nodo selecciona un número aleatorio k con igual probabilidad del conjunto $\{0,1,2,3,\dots 2^c-1\}$, donde $c=\min[10,n]$
 - El nodo espera $512 \cdot k$ tiempos de bit (a 10 Mbps, 1 tiempo de bit es 10^{-7} segundos)
- Si $n = 16$, se finaliza la transmisión



Protocolos basados en CSMA

15

CSMA-CD: Algoritmo de retroceso exponencial binario. Análisis

- Si hay pocas colisiones, la espera es pequeña
- Si hay muchas colisiones, espera razonable que crece poco a poco
- Si el tiempo de espera fuera fijo y muy grande
 - Pocas colisiones, pero las que hay introducen mucho retraso
- Si el tiempo de espera fuera fijo y pequeño
 - Muchas colisiones

Consecuencia

- Las tramas deben ser lo suficientemente largas para que se detecte una colisión antes de que finalice la transmisión
- En caso contrario, las prestaciones son las mismas que CSMA

CSMA/CD y IEEE 802.3 (Ethernet)

- 802.3 usa CSMA/CD para acceso al medio:
 - Los primeros esquemas trabajan a half-dúplex.
 - Las topologías en bus o con un concentrador (hub) son medios de difusión y puede haber colisiones.
- En el 802.3x (1997) se describió el modo full-dúplex:
 - Conexiones punto a punto (no hubs sino switches).
 - Todos (switch y nodos) deben permitirlo.
- En full-dúplex no produce colisiones -> no hay que seguir el CSMA/CD ni su tamaño mínimo.
- Para ser un 802.3 debe permitir trabajar en half-dúplex.



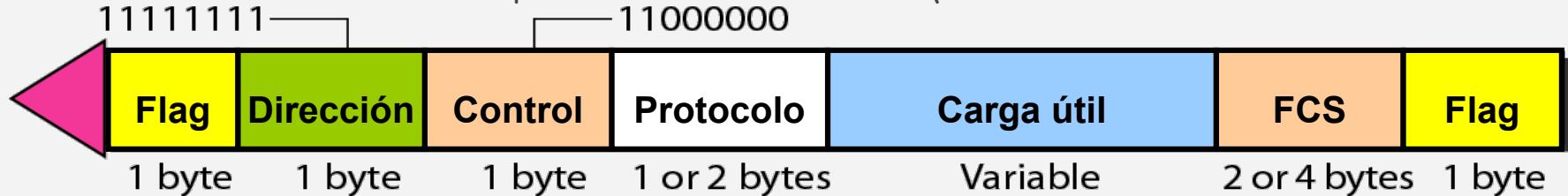
PPP: Introducción

- Protocolo muy extendido para el **acceso punto a punto**
PPPoE : PPP over Ethernet
- **Aspectos definidos por PPP:**
 - Formato de la trama a intercambiar
 - Cómo negociar establecimiento del enlace e intercambio de datos
 - Cómo encapsular datos de nivel de red
 - Autenticación entre dispositivos
 - Soporte de múltiples protocolos y servicios a nivel de red
 - Configuración de direcciones de red
- **Aspectos no definidos por PPP:**
 - Control de flujo
 - Control de error mínimo: CRC para detección de error (en silencio). Sin numeración de secuencia

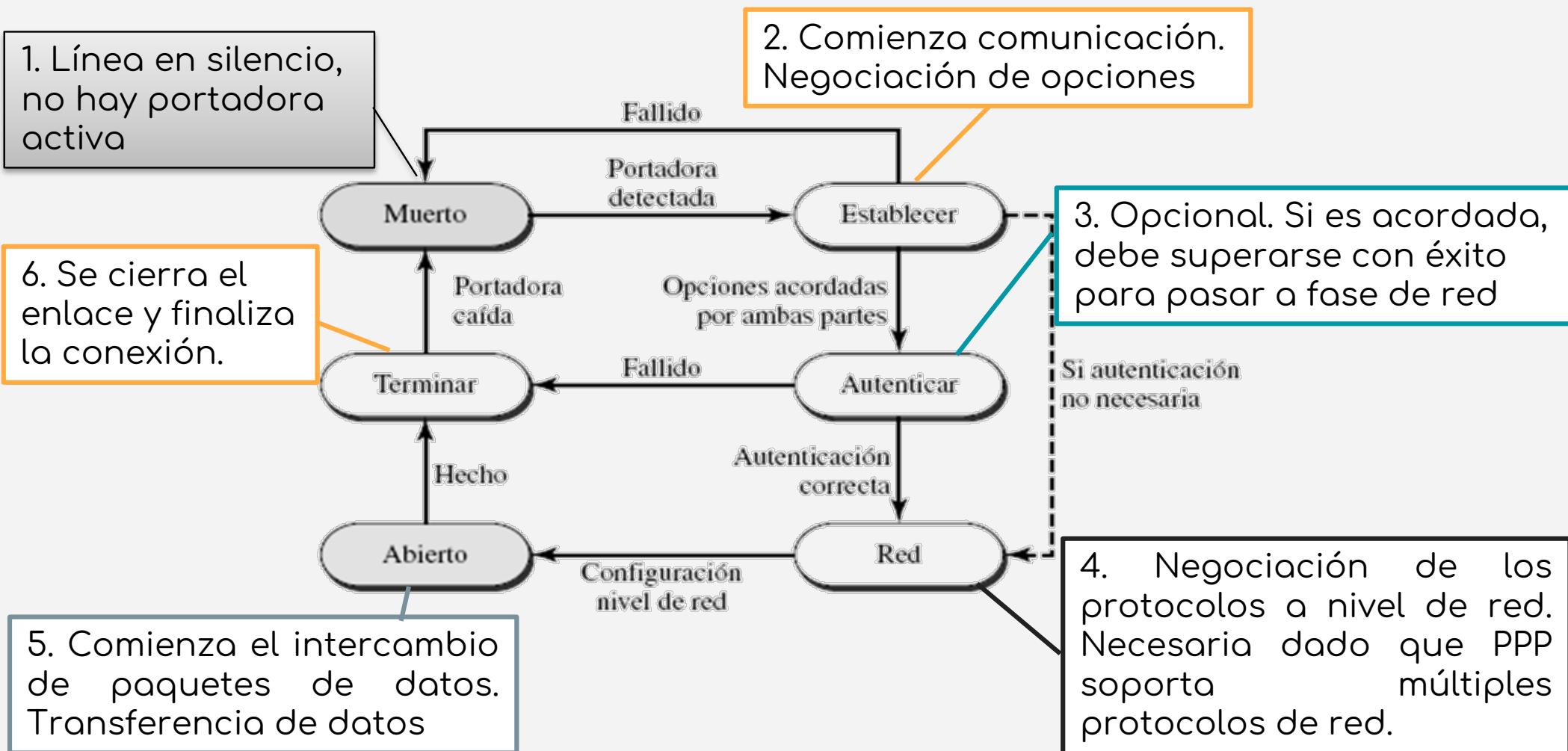
PPP: Unidad de datos (trama)

Creación de tramas:

- Protocolo **orientado a byte**: transparencia a nivel de byte (escape: 01111101)
- **Campos**:
 - **Flag**: Patrón 01111110
 - **Dirección**: Constante 11111111 (dirección de broadcast). Se puede negociar su omisión.
 - **Control**: Constante 11000000. Innecesario, omitible por negociación
 - **Protocolo**: Qué se transporta en campo datos (datos de usuario u otros)
 - **Carga útil**: datos de usuario u otra información. Máximo inicial 1500 bytes
 - Si la cantidad de datos reales es inferior al tamaño negociado -> padding
 - **FCS**: Secuencia de comprobación de trama (CRC estándar de dos o cuatro bytes)



PPP: Funcionamiento básico



PPP: Principales protocolos

20

LCP (*Link Control Protocol*): Protocolo de control de enlace

- Establecer, mantener, configurar y terminar enlace
- Negociación de opciones entre ambos extremos

Protocolos de autenticación:

- Valida la identidad del usuario sobre el enlace de marcado
- Dos protocolos en PPP:
 - PAP (password authentication protocol)
 - CHAP (challenge handshake authentication protocol)

NCP (*Network Control Protocol*): Protocolos de control de red

- Protocolo de control de red específico para cada protocolo de red
 - IPCP configura enlace para transportar paquetes de datos IP
 - Los paquetes NCP no llevan datos de nivel de red
 - Sólo configura el enlace al nivel de red para los datos que llegan

Tema 2: Capa de Enlace

Clase del 15/02/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)



Organización del tema y la clase

2

Capa Enlace:

- Comunicación entre equipos conectados “directamente”

Principales servicios:

- Fiabilidad (control de errores), saturación (control de flujo), medios de difusión (acceso al medio) y gestión tramas

Casos concretos: **Wifi (802.11) – inalámbrica (ondas de radio)**

- Arquitectura

- Capa física:

- Introducción y problemas derivados
 - Versiones (802.11X)

- Capa de enlace (Acceso al Medio):

- **Introducción y elementos básicos**
 - **Modo distribuido (DCF):** Protocolos de acceso al medio (MACA, MACAW, CSMA/CA)
 - **Modo centralizado (PCF)**

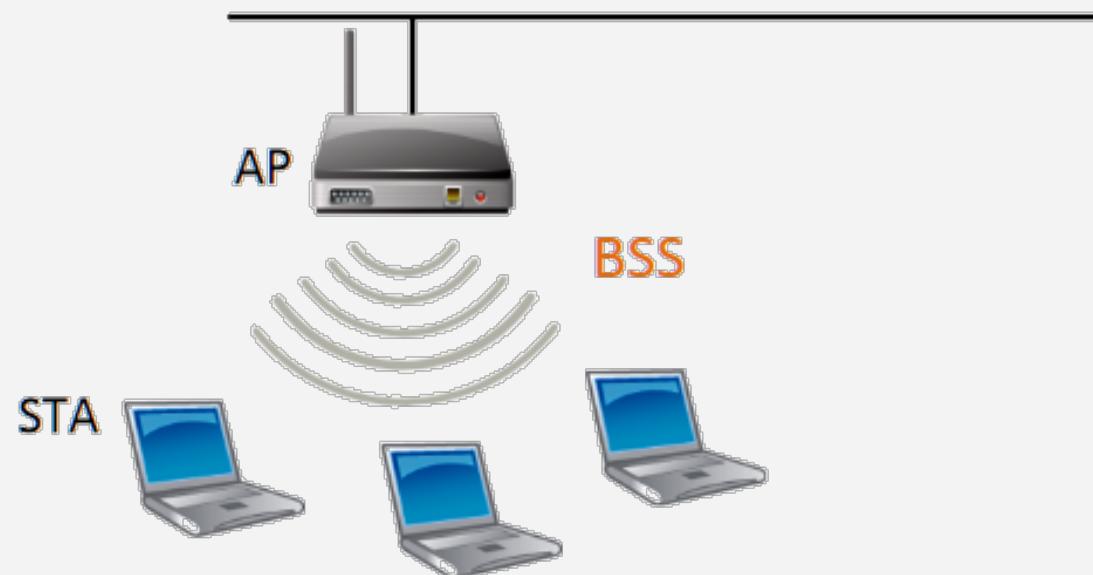
Arquitectura: Modo Infraestructura

3

BSS (Basic Service Set): Grupo de estaciones (STA) que se comunican entre sí

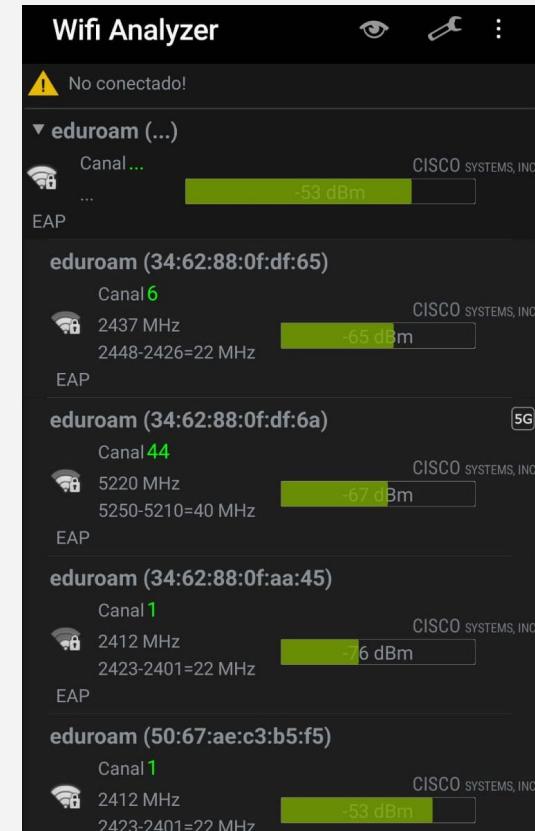
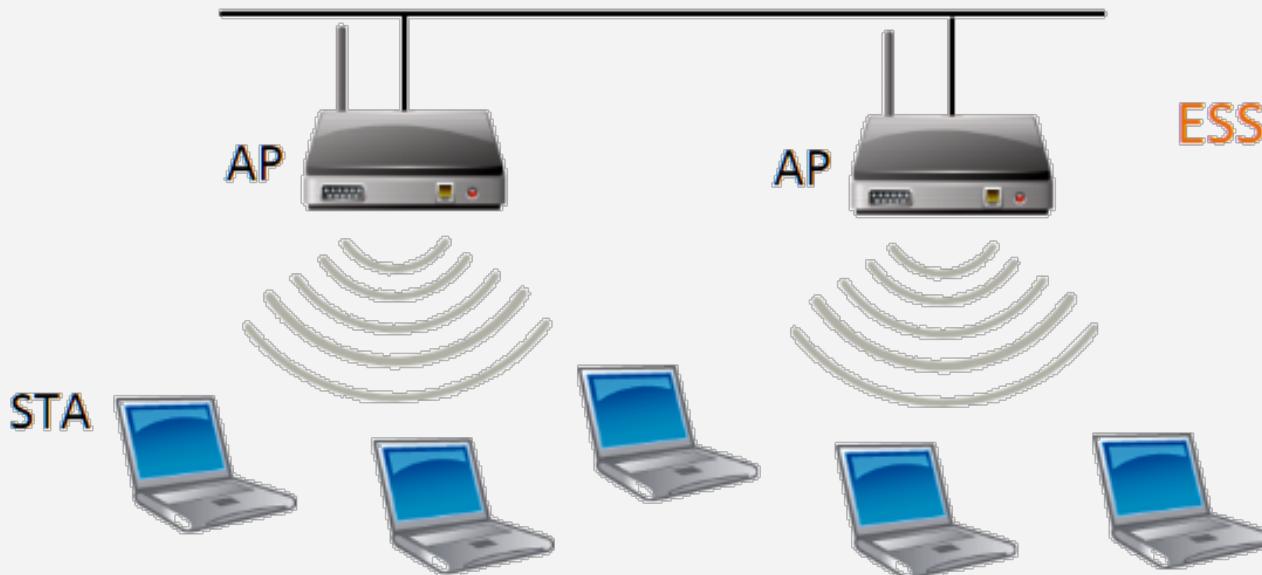
Red con Infraestructura: BSS con **AP** (Access Point)

- El **AP** nos ofrece comunicación con otras redes y entre equipos



Podemos formar redes mayores uniendo varios BSS a través de un sistema de distribución (DS) formando un ESS (Extended Service Set)

Las estaciones pueden moverse entre BSS dentro de un ESS
(roaming)



Arquitectura: Modo Infraestructura

Se puede utilizar la propia red inalámbrica como sistema de distribución (**WDS - Wireless DS**)

Habitualmente no soportan roaming (802.11k ni 802.11r)

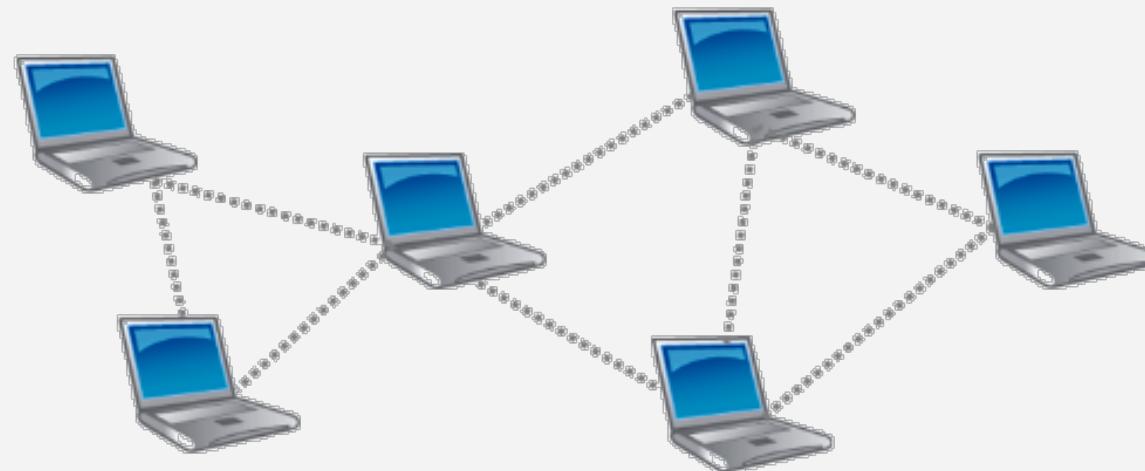
The screenshot shows the ZTE F680 web interface. The top bar displays the ZTE logo and the model number F680. The left sidebar has a green header labeled "-Network" and contains the following options: "+WLAN Common Setting", "+WLAN Radio2.4G(Online)", "-WLAN Radio5G(Online)" (which is selected and highlighted in green), "Basic", "SSID Settings", "Security", "Access Control List", "Associated Devices", and "WDS" (which is also highlighted in green). The main content area shows the path "Path: Network-WLAN Radio5G(Online)-WDS". It includes a warning message: "WDS Mode switching will take effect immediately." followed by a yellow warning icon. Below this, there is a dropdown menu for "WDS Mode" with the following options: "Disabled" (selected), "Disabled", "WDS+Root", and "WDS+Repeater" (highlighted in blue).

Arquitectura: Modo ad-hoc

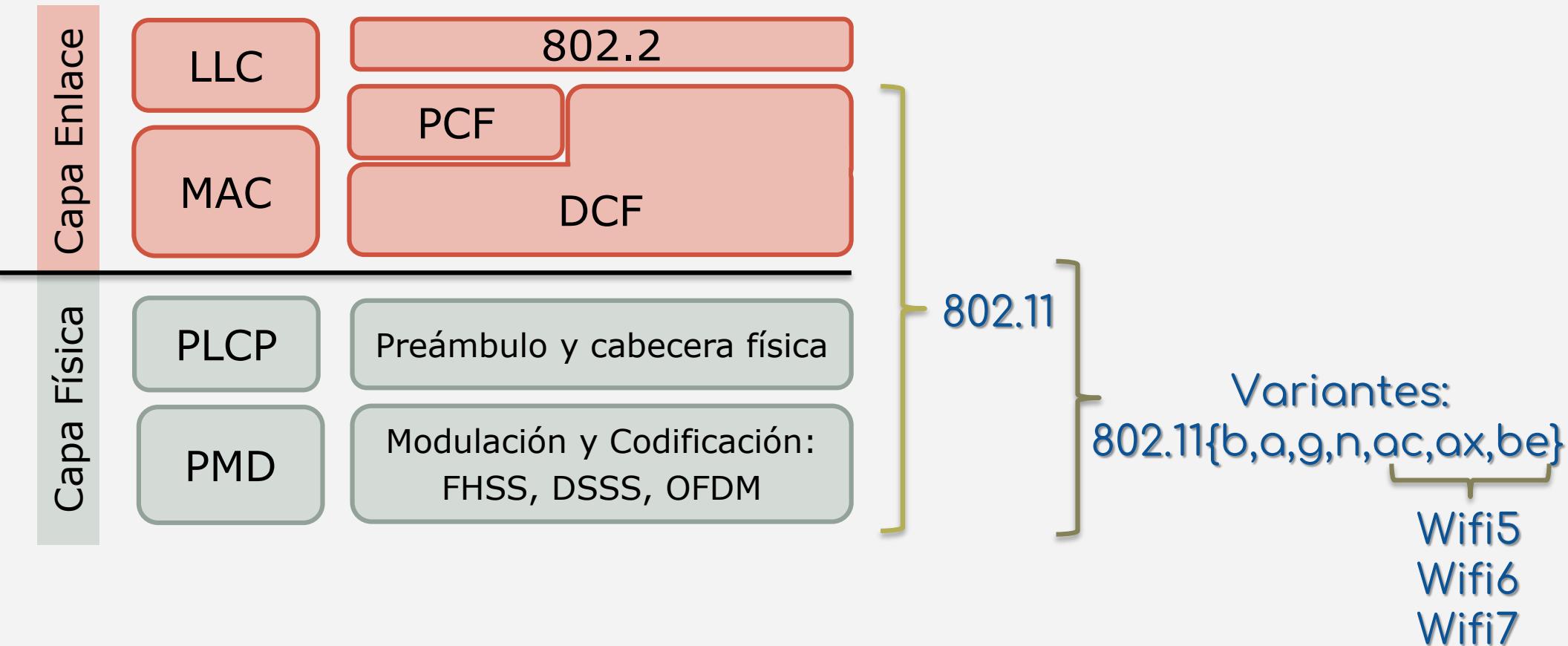
Modo ad hoc: BSS sin AP

No pueden enviar a otros BSS (red independiente)

Forman un **IBSS (Independent Basic Service Set)**



Estándar IEEE 802.11

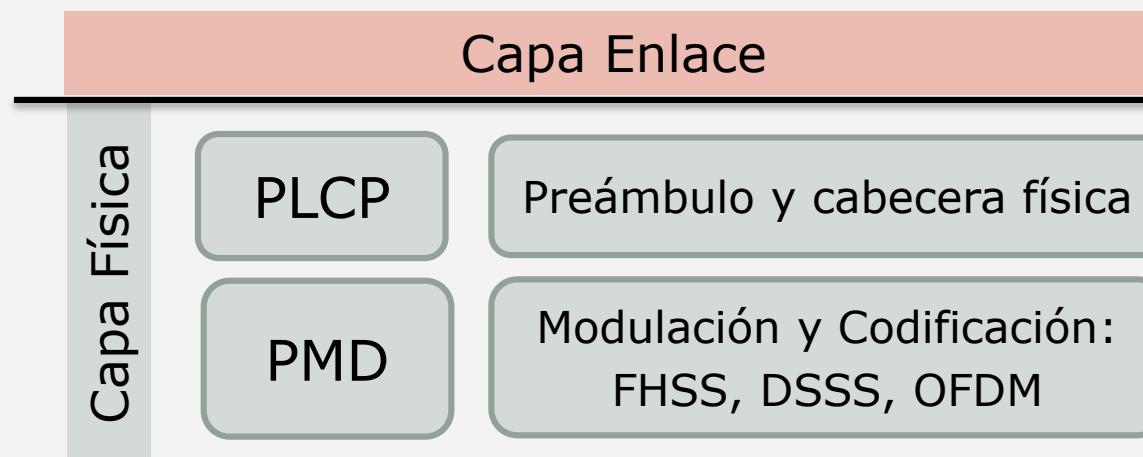


Estándar IEEE 802.11: Capa física

8

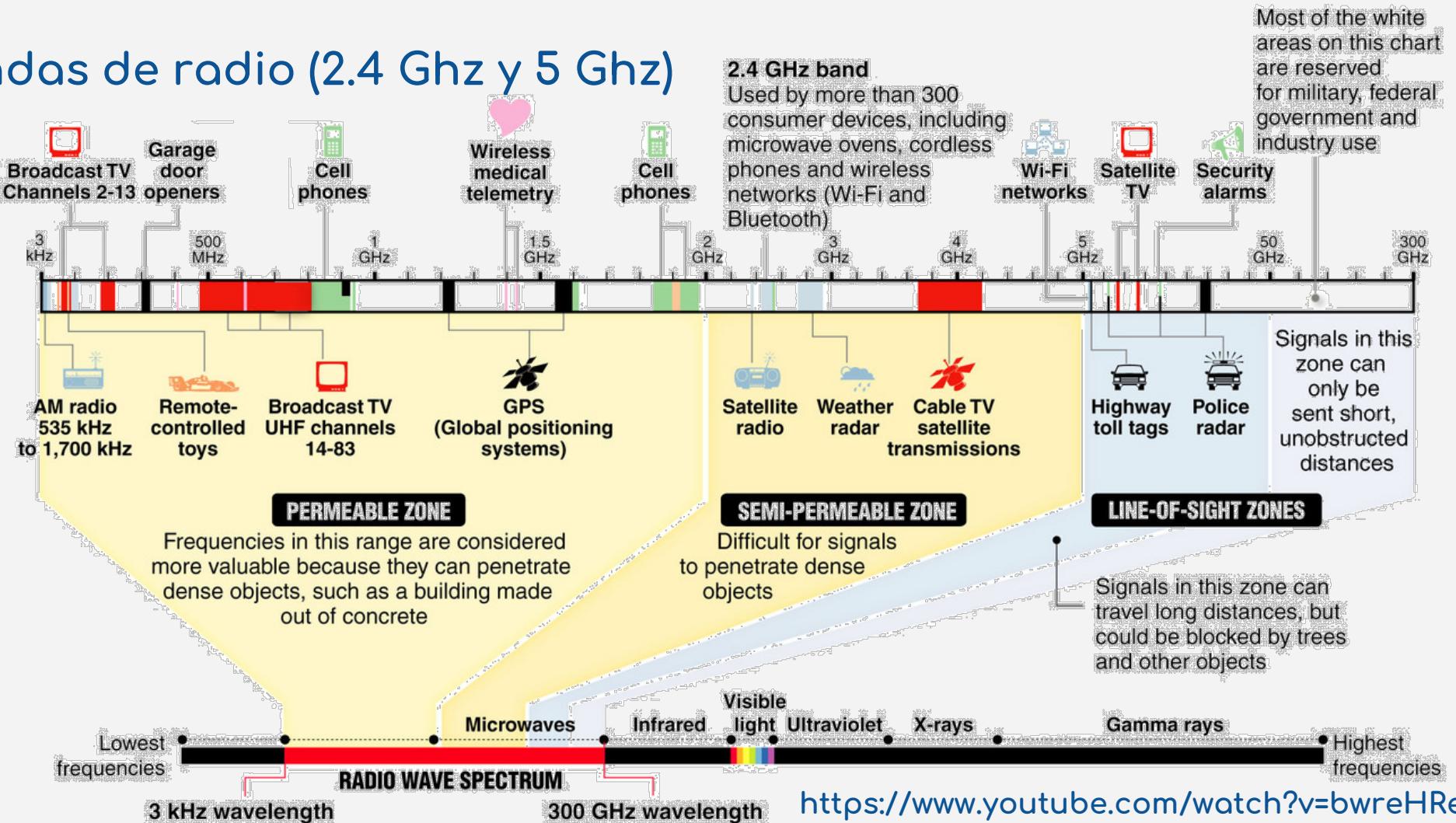
Divide la capa en dos subcapas:

- **PMD** (Physical Medium Dependant): Define cómo se enviarán los datos (**modulación y codificación**)
- **PLCP** (Physical Layer Convergence Procedure): Añade una cabecera con el **preámbulo** para la sincronización y ciertos parámetros para indicar como se usará el medio



Estándar IEEE 802.11: Capa física (PMD)

Ondas de radio (2.4 Ghz y 5 Ghz)



Estándar IEEE 802.11: Capa física (PMD)

10

El colegio salmantino que ha quitado el WiFi del centro por la seguridad de pequeños y mayores

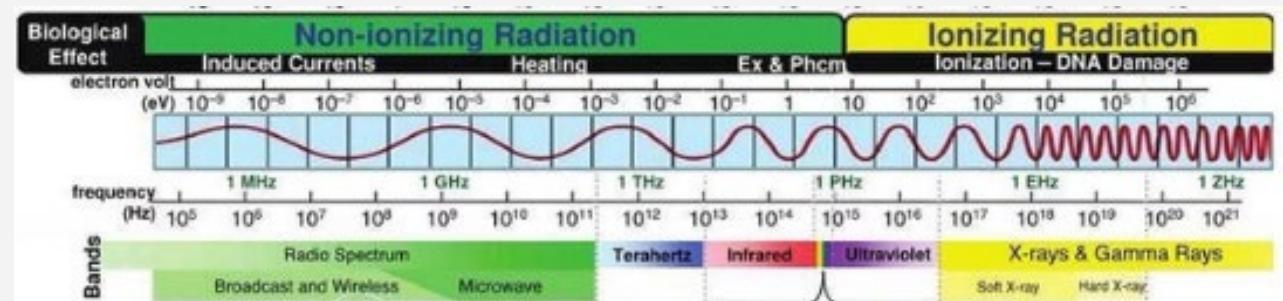


Cómo es vivir con electrosensibilidad: "Tuve que irme de la ciudad a vivir al campo para escapar de las ondas electromagnéticas"

Redacción
BBC News Mundo

2 marzo 2020

f m t e Compartir



- Usa frecuencias **no ionizante** (capacidad de afectar al ADN) **ni potencia suficiente** para afectar.
- <http://radiandando.es/>

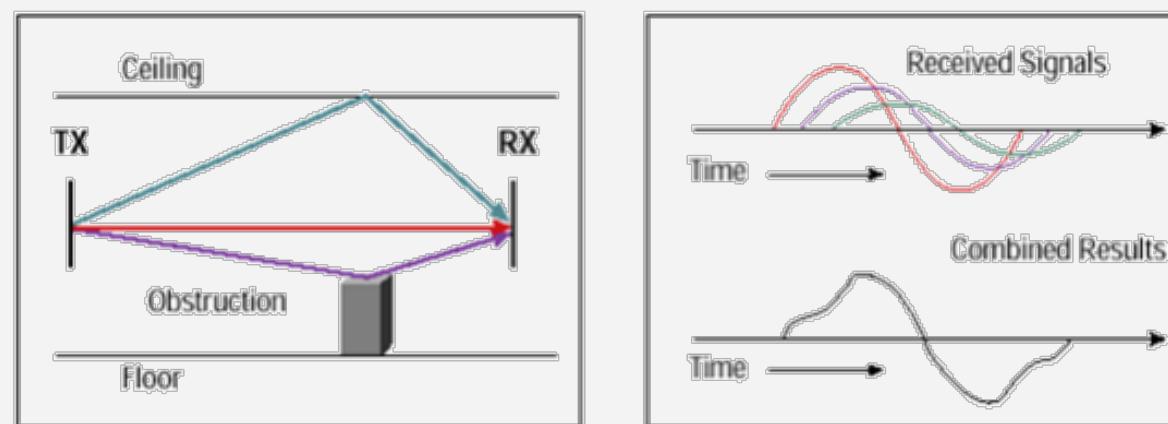
Estándar IEEE 802.11: Problemática

11

Interferencias: Frecuencias muy utilizadas (especialmente 2.4 GHz):

- Dispositivos 802.11 no deseados (otras wlans)
- Otros elementos no 802.11 (bluetooth, microondas, teléfonos inalámbricos, luces fluorescentes, controladores inalámbricos...)

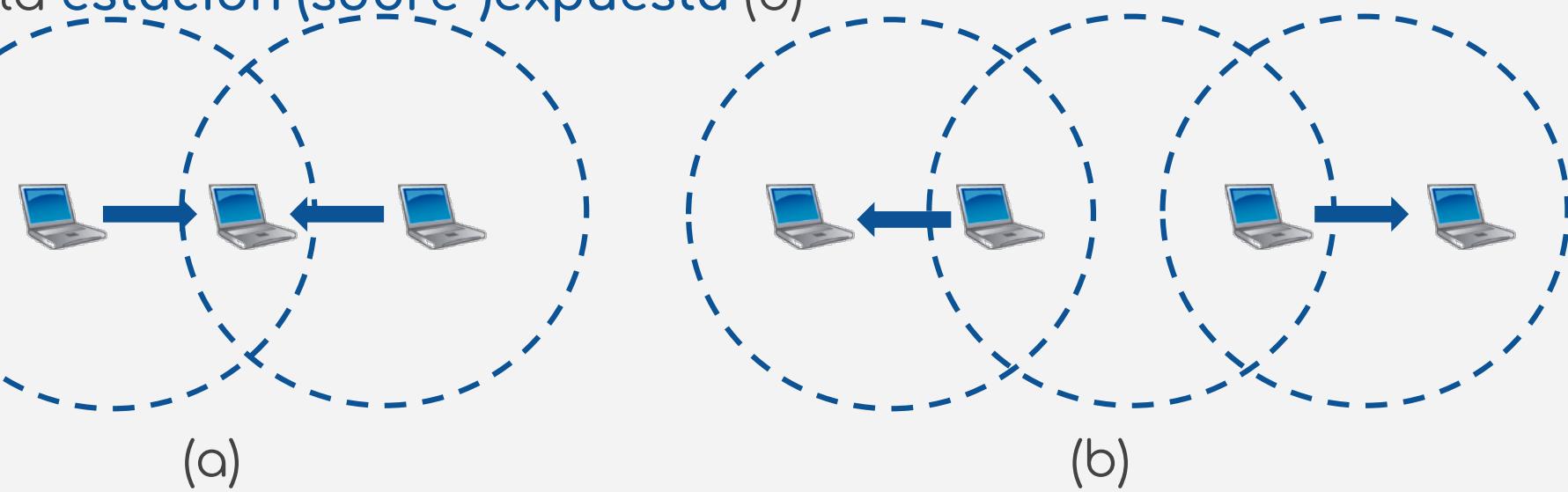
Obstáculos: Las señales no atraviesan ciertos materiales (metal, agua, hormigón, espejos...) y ciertos materiales además reflejan ciertas frecuencias => Problemas de multicamino:



Estándar IEEE 802.11: Problemática

12

Atenuación: No asegura cobertura => Problema de la **estación oculta** (a) y la **estación (sobre-)expuesta** (b)



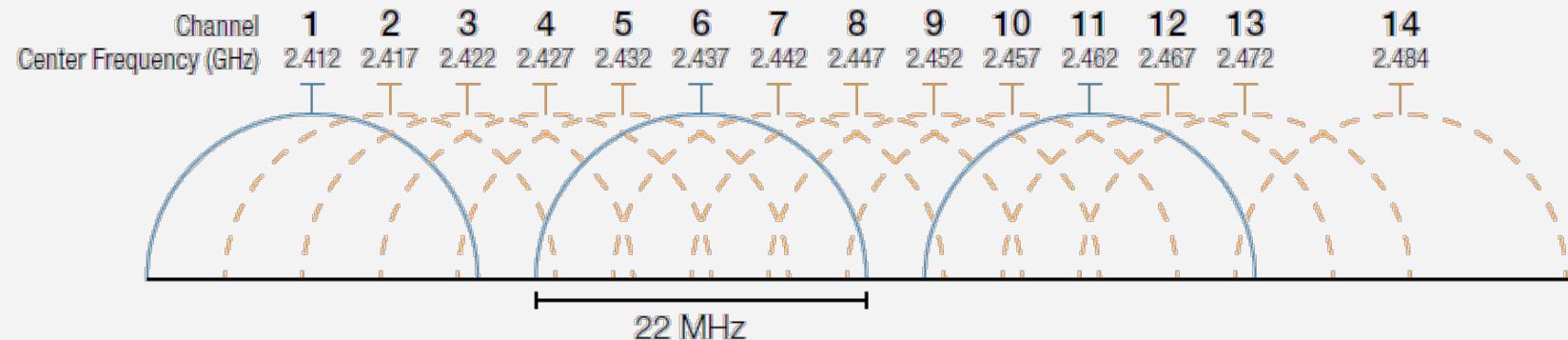
No se puede detectar colisiones:

- Señal enviada mucho más potente de la recibida
- Con la distorsión no es capaz de distinguir entre señal recibida y ruido propio del medio

Estándar IEEE 802.11: Capa física (PDM)

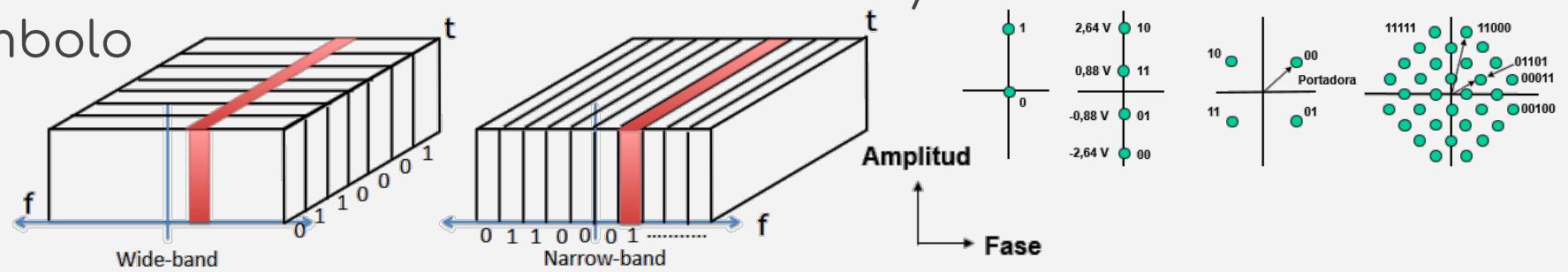
13

Divide el rango de frecuencia disponible en canales de ~20 Mhz solapados:



PDM define las frecuencias, cómo se usan y el ancho:

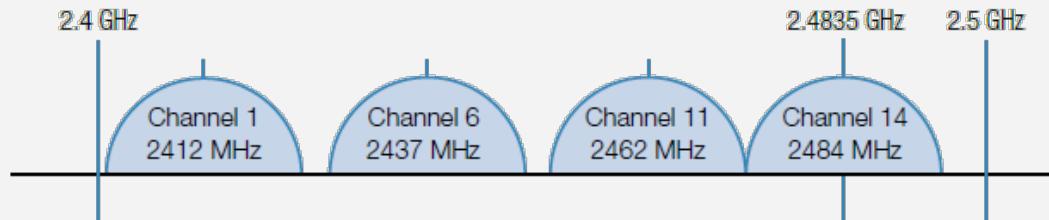
- **DSSS:** Usa todas las frecuencias para el envío
- **OFDM:** Divide los canales en subcanales y en cada subcanal envía un símbolo



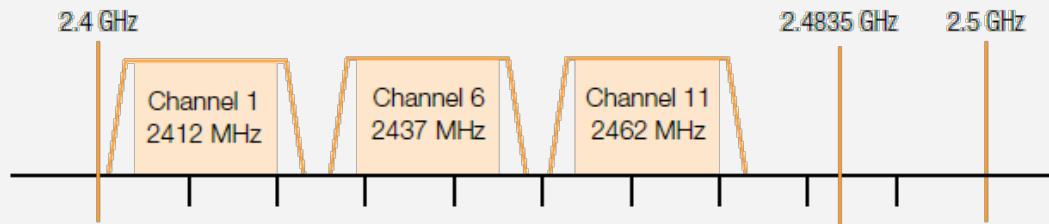
Estándar IEEE 802.11: Capa física (PDM)

Non-Overlapping Channels for 2.4 GHz WLAN

802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz channel width - 16.25 MHz used by subcarriers



802.11n (OFDM) 40 MHz channel width - 33.75 MHz used by subcarriers



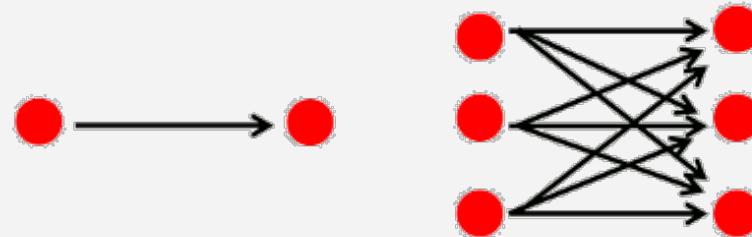
Estándar IEEE 802.11: Capa física (PDM)

15

Año	Estándar	Frec (GHz)	Ancho de Canal (MHz)	Modulación	Antena	Máx BW (Mbps)
1997	802.11	2.4	20	DSSS, FHSS	SISO	2
1999	802.11b	2.4	20	DSSS	SISO	11
1999	802.11a	5	20	OFDM	SISO	54
2003	802.11g	2.4	20	DSSS, OFDM	SISO	54
2009	802.11n	2.4 y 5	20, 40	OFDM	MIMO (4)	600
2013	802.11ac	5	40, 80, 160	OFDM	MU-MIMO (8)	6,9 Gbps
2019	802.11ax	2.4 y 5 (6)	20 a 160	OFDM (A)	MU-MIMO (16)	10 Gbps
2024	802.11be	2.4, 5 y 6	20 a 320	OFDM (A)*	MU-MIMO (16)	48 Gbps

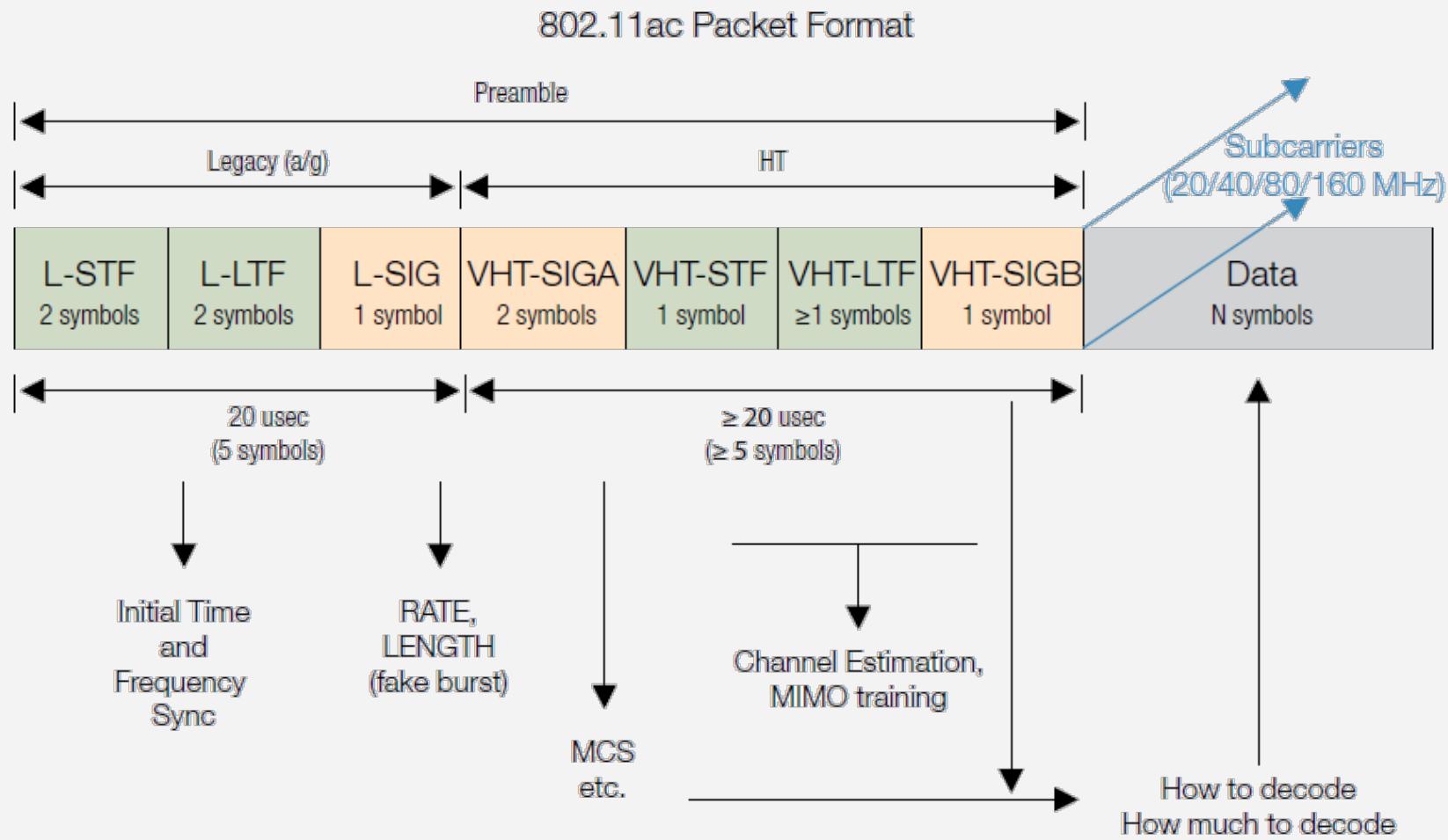
SISO

MIMO

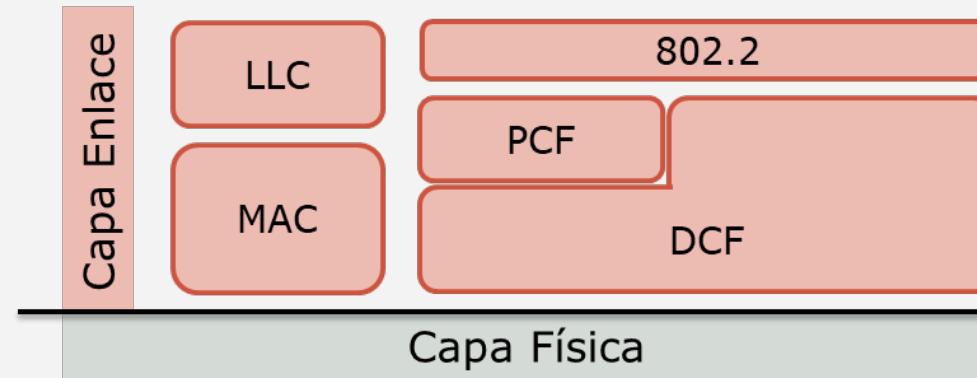


Estándar IEEE 802.11: Capa física (PLCP)

PLCP define las cabeceras para sincronización y uso del medio



Estándar IEEE 802.11: Capa de enlace



Canal muy propenso a error:

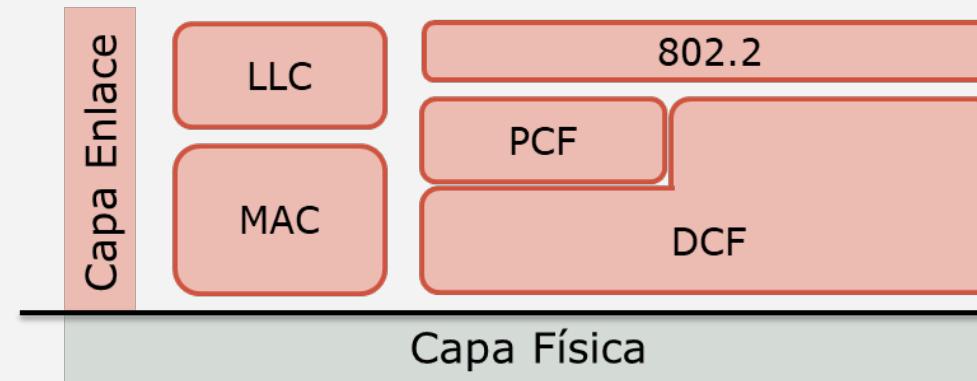
- La capa MAC incluye control de error y flujo (propio de LLC)
- Las tramas de datos son confirmadas con ACKs (Stop & Wait)

No es posible detectar colisiones:

- Los protocolos intentan evitar colisiones (en caso de haberlas se detectarán con ACKs no recibidos)
- Tramas especiales que indican que se va a usar el canal (RTS, CTS y Beacon) que lo reservan (activan NAV)
- Prioridad de trama a la hora de obtener el canal, mediante tiempo de espera diferentes entre tramas (IFS - interframe space)

Estándar IEEE 802.11: Capa de enlace

18



Dos modos de adquisición del medio:

- Centralizado (PCF) y Distribuido (DCF)

Función de coordinación distribuida (DCF)

- Competen por el canal usando CSMA/CA (CA = Collision Avoidance):
 - Variante de CSMA no-persistente (tiempo de espera aleatorio depende de backoff)
 - Dos modos de comprobar el canal ocupado
 - Usa RTS/CTS (opcional)
 - Confirma los datos

Función de coordinación puntual (PCF)

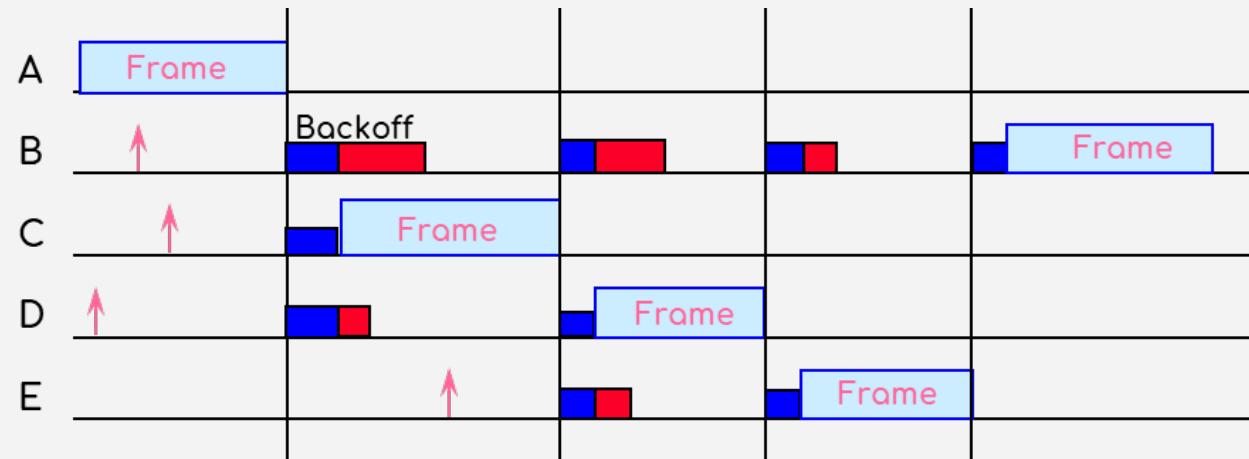
- El AP adquiere el canal y usa polling para dar paso a los nodos

802.11: Capa de enlace: DCF: CSMA/CA

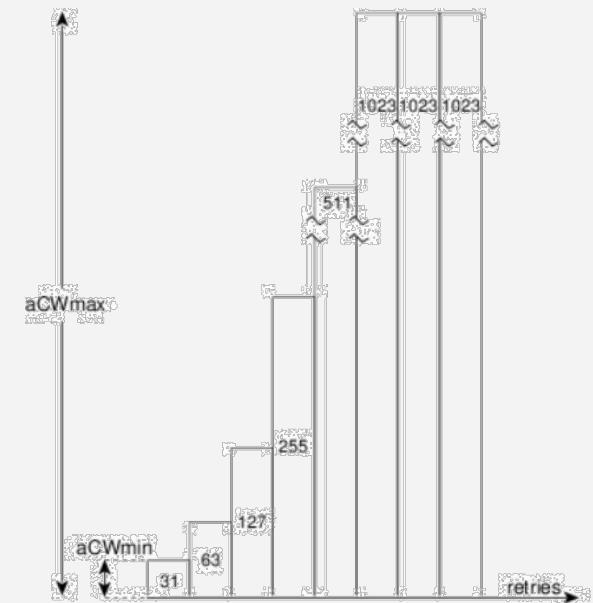
En Ethernet (CSMA/CD) usamos un esquema 1-persistente, ¿porqué no es adecuado en 802.11?

Usar tiempo de espera aleatorio (no persistente) tras detectar el canal libre ... pero ¿cuánto?

Mecanismo basado en el algoritmo de retroceso exponencial (backoff):



CWindow = Contention Window
= Backoff
= Remaining Backoff



802.11: Capa de enlace: DCF: CSMA/CA

20

El mecanismo anterior intenta evitar colisiones, pero no lo asegura ... además hay otras fuentes de error externas posibles => Necesita mecanismo que asegure la corrección => Envío de ACK (Stop & Wait)

Problema: Los ACKs compiten con igual probabilidad que el resto y no podemos asegurar que lleguen en un periodo razonable (timeout).

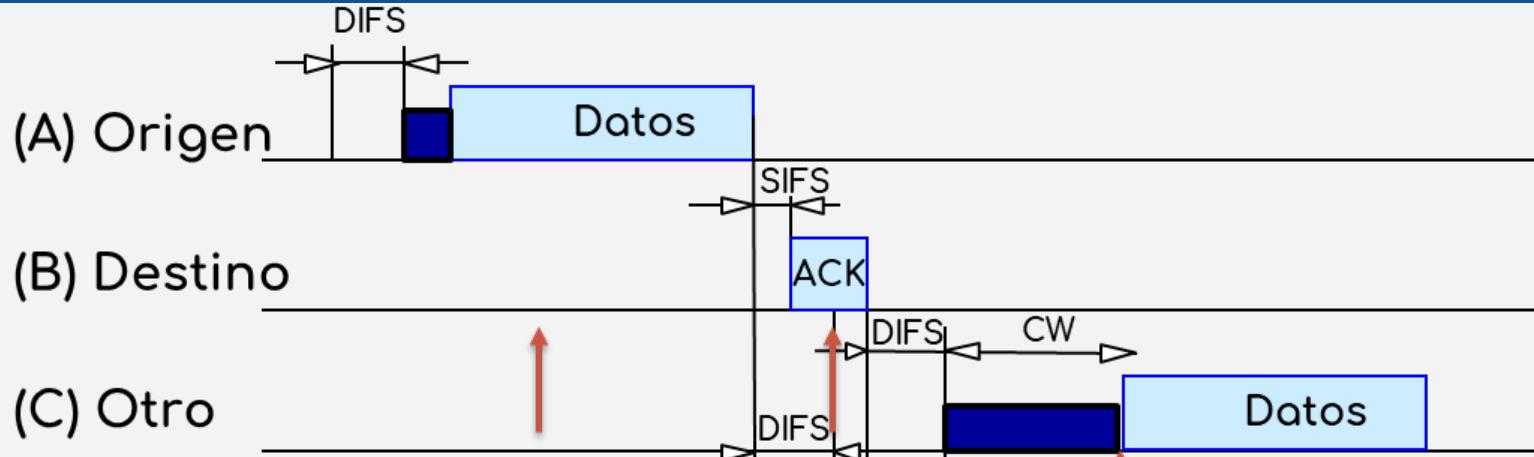
Eliminar el CW de estas tramas asegura su prioridad pero es susceptible a colisiones (con equipos con CW cercanos a 0).

Añadir tiempo de espera adicional y diferentes a cada tipo de trama (prioridad):

- **DIFS:** Tiempo de espera DCF de tramas de inicio de comunicación
- **SIFS:** Tiempo de espera corto para respuestas ($SIFS \ll DIFS$)

802.11: Capa de enlace: DCF: CSMA/CA

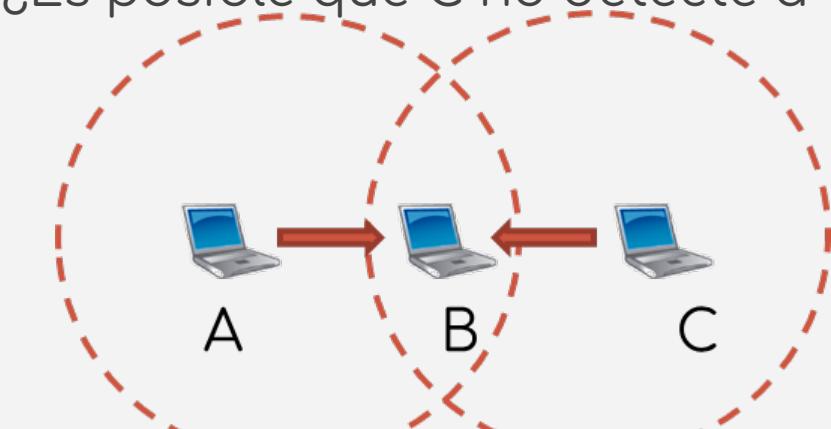
21



Esto funciona bien si C detecta el envío de A, pero en caso contrario, su envío podría colisionar o retrasar el ACK de B. ¿Es posible que C no detecte a A pero si tenga interferencias con B?

Problema de **la estación oculta**:

El equipo A está “oculto” para C

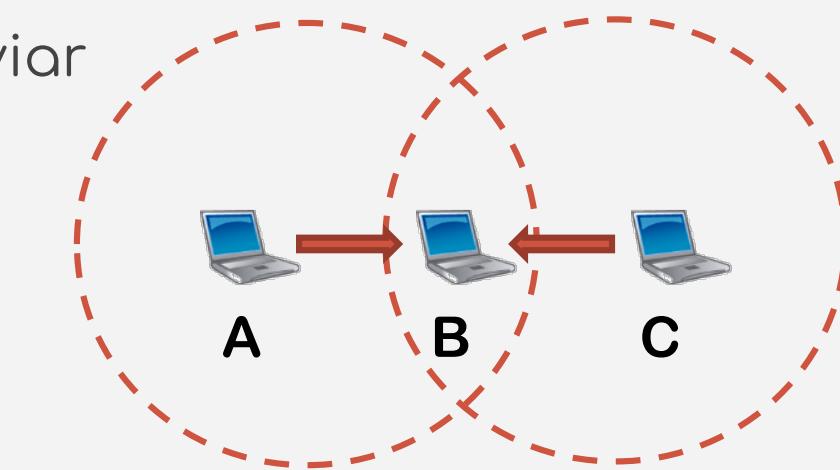


802.11: Capa de enlace: DCF: CSMA/CA

22

Para esos problemas, se envían **pequeñas tramas de control previas** indicando si está disponible y avisando a todos los nodos visibles

- **RTS (Request to Send):** Quiero enviarte datos
- **CTS (Clear to Send):** Puedes enviar



Cuando A quiere enviar:

B lo recibe:

C ve el canal libre pero sabe que B se comunica con un equipo "oculto" pero **¿cuánto debe esperar C para intentar el envío?**

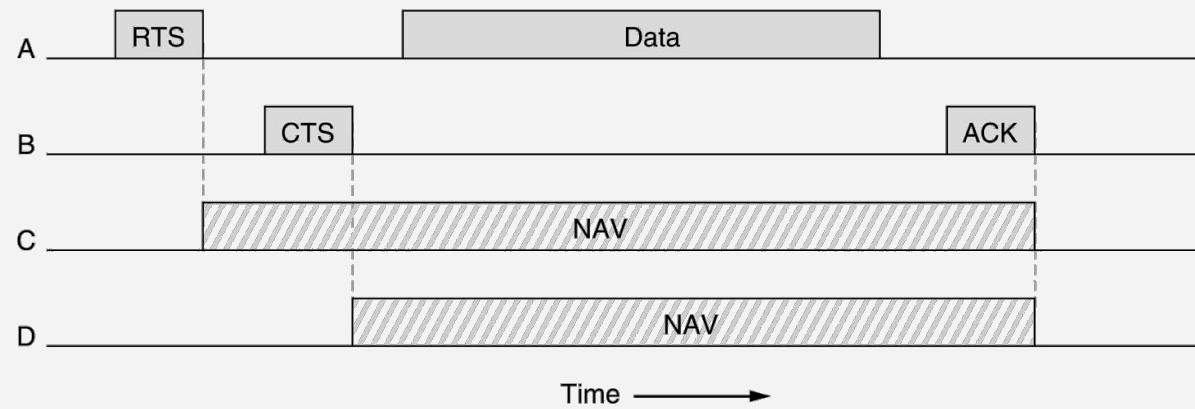
Envía RTS a B

Envía CTS a A (y también lo ve C)

802.11: Capa de enlace: DCF: CSMA/CA

Las tramas indican cuánto tiempo necesitan para el envío (y su ACK)

NAV: Network Allocation Vector



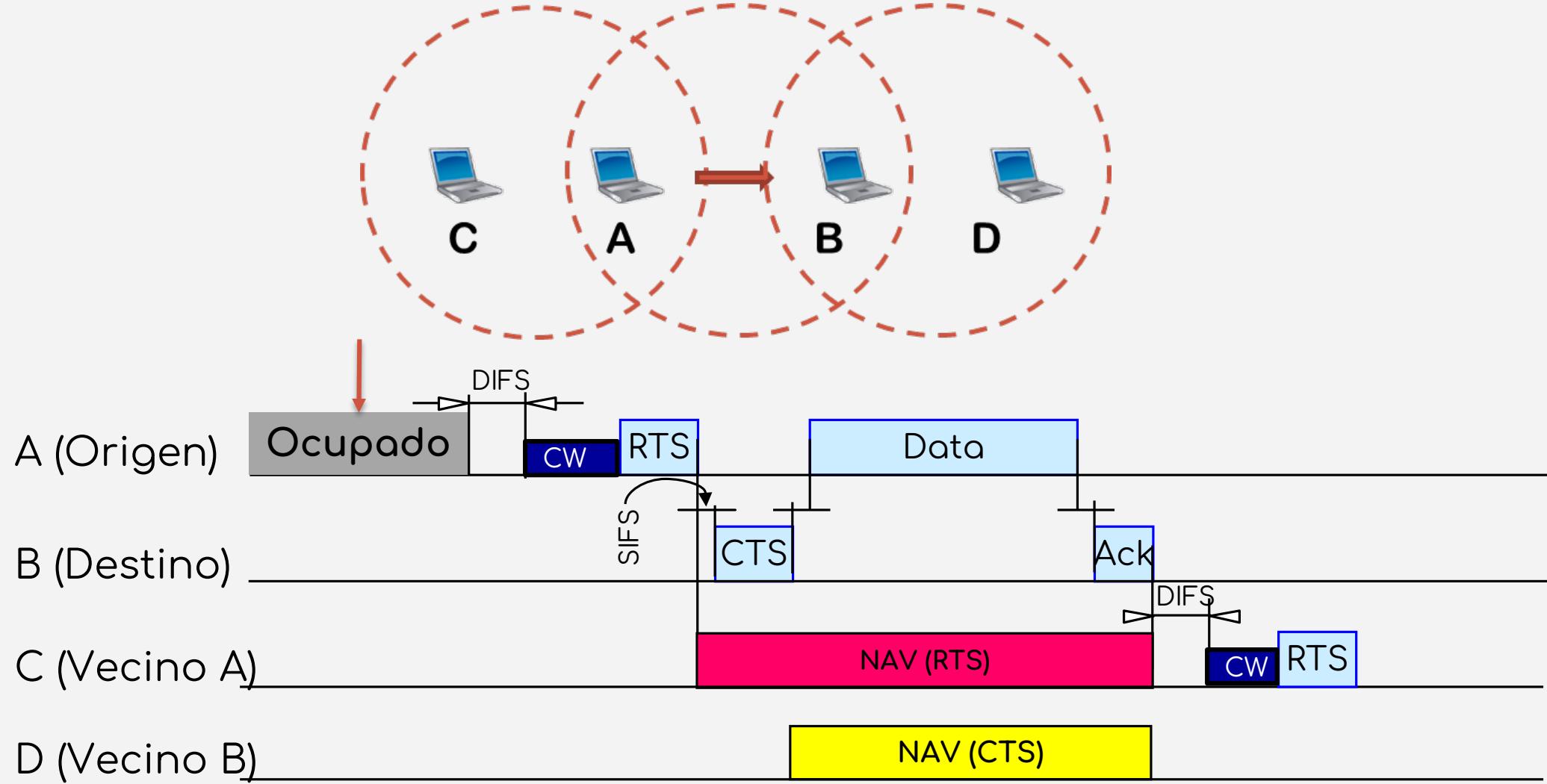
Entonces hay dos formas de consultar si el canal está ocupado:

- **Virtual Channel Sensing:** Mientras tengamos un NAV activo no se puede enviar aunque se detecte el canal sin ocupar
- **Physical Channel Sensing:** Consultar física del canal. Sólo se realiza si no tenemos un NAV activo

A veces el RTS/CTS está desactivado para mejorar la eficiencia

802.11: Capa de enlace: DCF: CSMA/CA

24



802.11: Capa de enlace: DCF: CSMA/CA

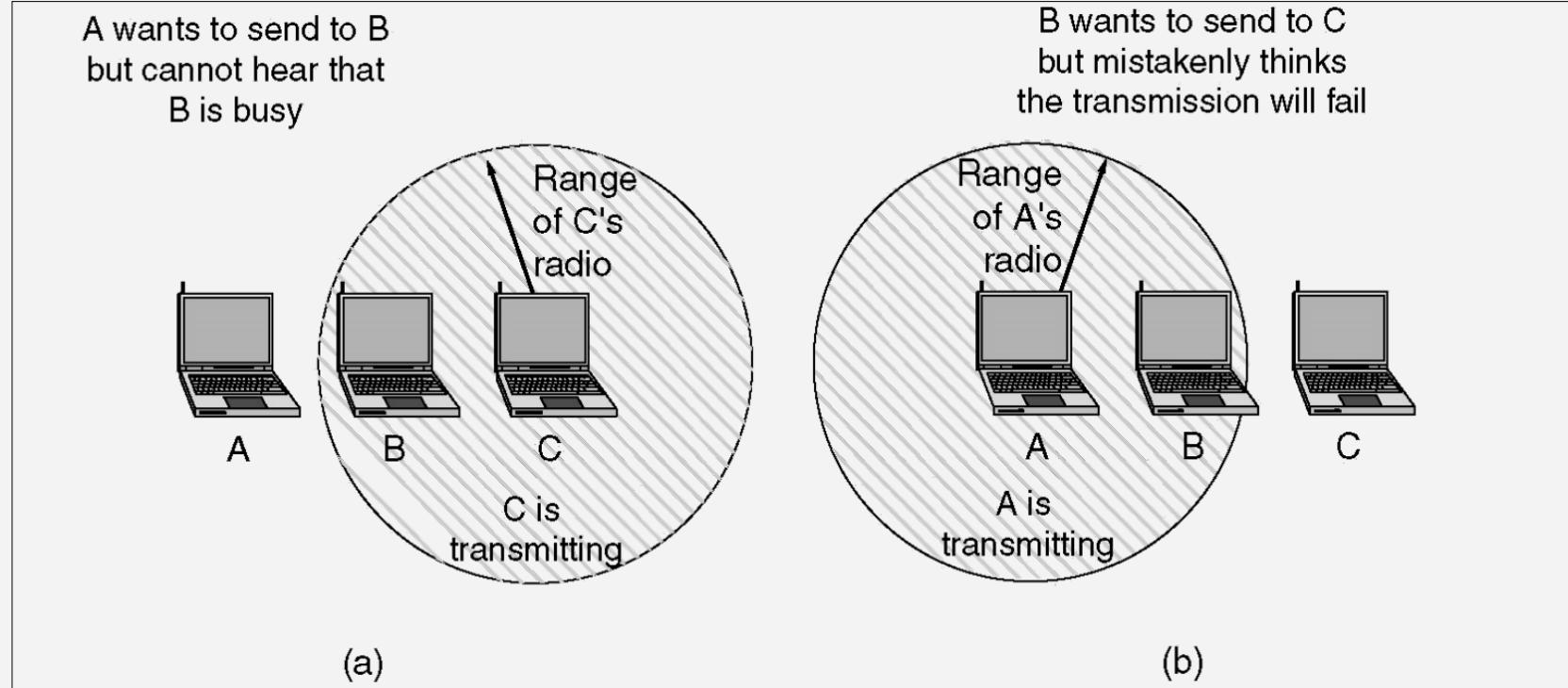
25

El problema de estación oculta (a)

- Se soluciona con RTS y CTS

El problema de la estación expuesta (b)

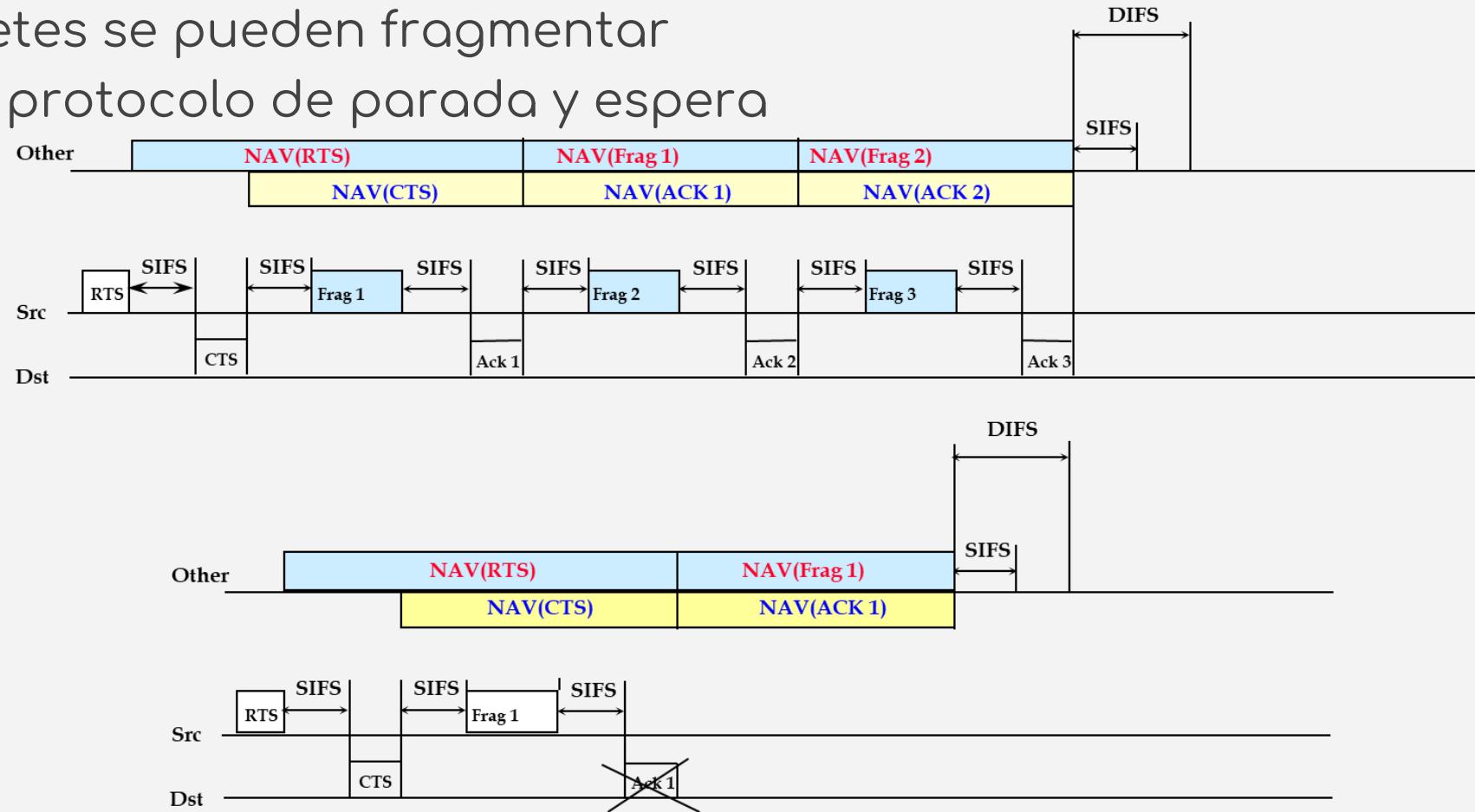
- ¿Solución?



802.11: Enlace: DCF: Fragmentación

En medios con gran cantidad de pérdidas:

- Los paquetes se pueden fragmentar
- Se usa un protocolo de parada y espera



802.11: Enlace: DCF: Protocolos

27

MACA (Multiple Access with Collision Avoidance):

- Incorpora el mecanismo de RTS/CTS

MACAW (MACA for Wireless):

- Añade las confirmaciones a los datos (ACKs)

CSMA/CA:

- Variante de MACAW con tiempos de espera basados en backoff
- Añade tiempos de espera fijos para dar prioridad (DIFS, SIFS...).

802.11: Enlace: PCF

28

Un nodo especial (el punto de acceso) toma el control del canal

- Usa un tiempo de espera (PIFS) < DIFS

Envía un paquete (Beacon) para reservar el canal

- Usa NAV y lo va actualizando.

Envía información a cada nodo para el que tiene y le da el turno:

- Los paquetes van confirmados pero llevando datos (piggybacking)

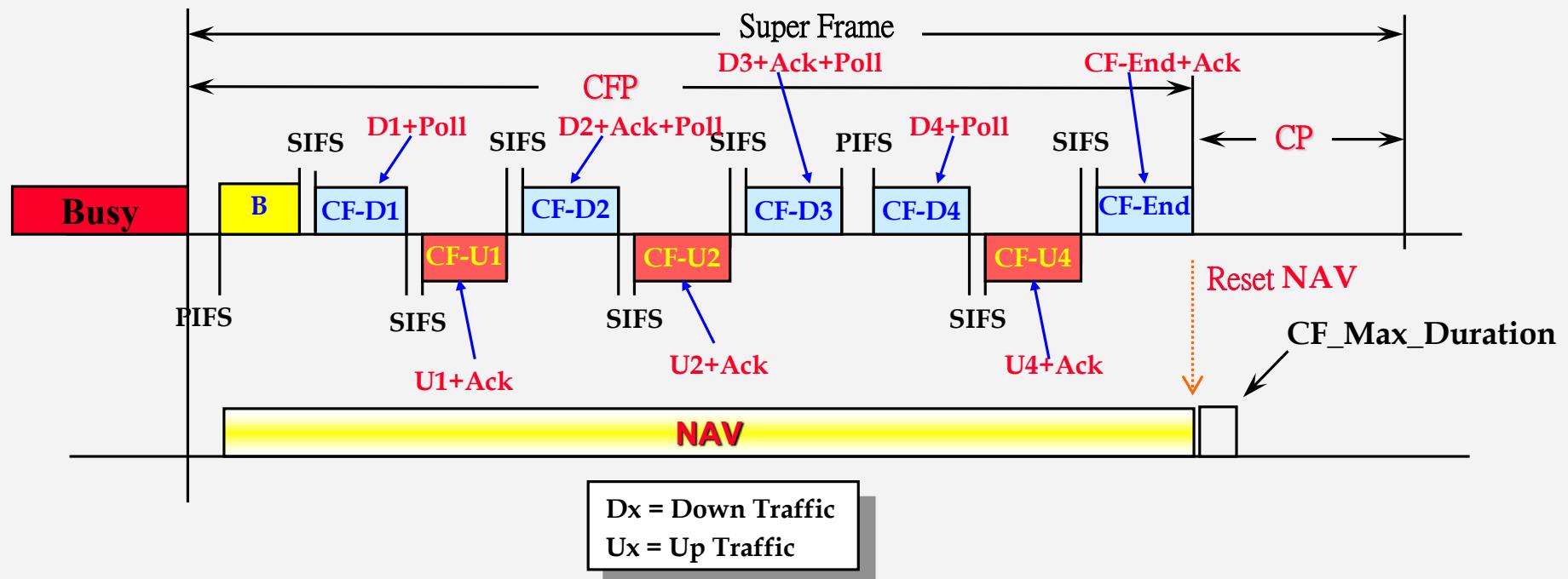
Debe alternarse con DCF ya que PCF es opcional y quizás no todos los nodos lo tengan disponible

802.11: Enlace: PCF

29

Útil para cierto tipo de tráfico donde se requiera cierta calidad de servicio (voz, multimedia, ...)

No habitual: no es obligatoria su implementación



Estándar IEEE 802.11: Capa enlace: IFS

30

IFS InterFrame Space

EIFS > **DIFS** > **PIFS** > **SIFS** > 0

Adquisición del canal:

- **EIFS**: IFS extendido: se ha recibido una trama no legible => para asegurar posibles respuestas esperamos más tiempo.
- **DIFS**: IFS para DCF
- **PIFS**: IFS para PCF

Mantenimiento del canal:

- **SIFS**: IFS corto para respuestas
- **RIFS**: Reemplaza algunos **SIFS** (solo en 802.11n)
- 0: Reemplaza **RIFS** en 802.11ac y posteriores

Estándar IEEE 802.11: Capa enlace: IFS

31

Estándar	SIFS (μ s)	Slot time (μ s)
802.11 (FHSS)	28	50
802.11 (DSSS)	10	20
802.11b	10	20
802.11a	16	9
802.11g	10	9 o 20
802.11n (2.4 GHz)	10	9 o 20
802.11n (5 GHz)	16	9
802.11ac	16	9

$$\text{DIFS} = \text{SIFS} + 2 * \text{Slot}$$

$$\text{PIFS} = \text{SIFS} + \text{Slot}$$

$$\text{EIFS} = \text{SIFS} + \text{DIFS} + t_{\text{trans_ack}}$$

$$\text{RIFS} = 2 \mu\text{s}$$

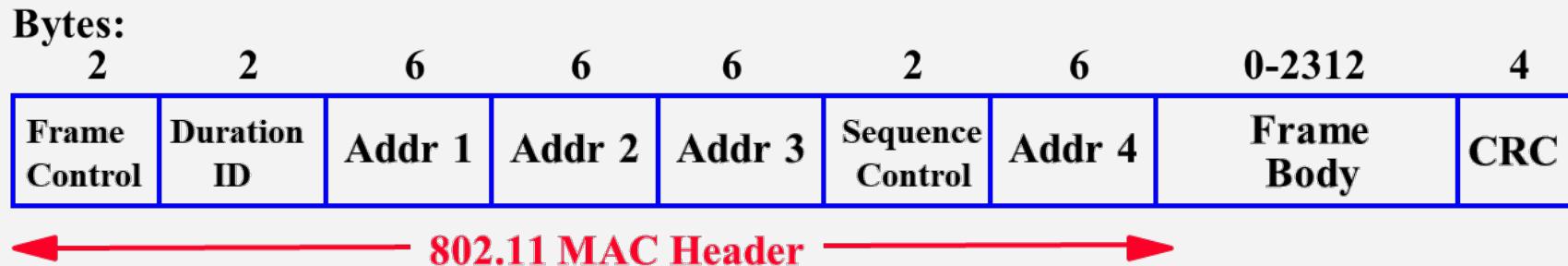
Estándar IEEE 802.11: Capa enlace: Trama

32

Tres tipos de tramas:

- **Datos**
- **Control:** RTS, CTS, ACK, CF-X, ...
- **Gestión:** Authentication, Beacon, Probe, ...

Según el tipo de trama se pueden omitir campos:



Bits: 2 2 4 1 1 1 1 1 1 1 1

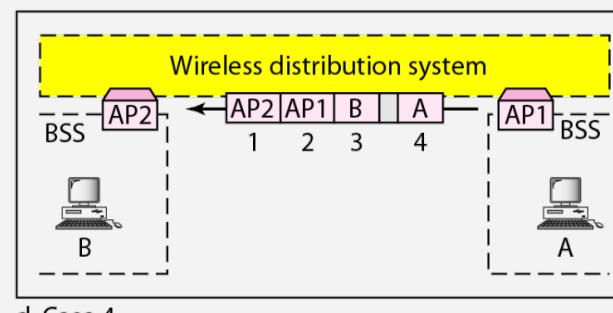
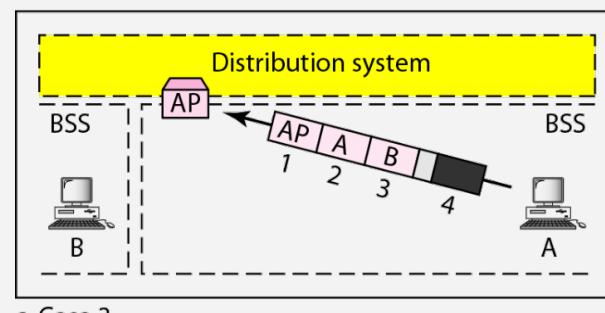
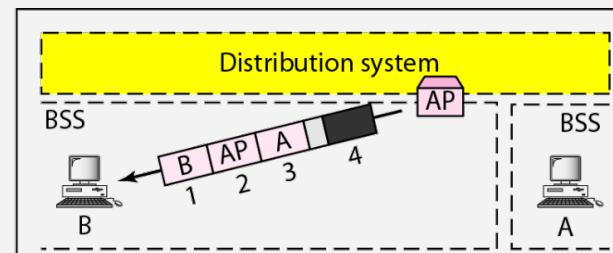
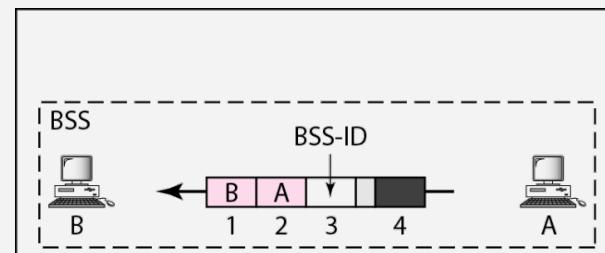
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order / rsrv
------------------	------	---------	-------	---------	-----------	-------	---------	-----------	-----	--------------

Campos de control de trama

Estándar IEEE 802.11: Capa enlace: Trama

33

A DS	DE DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	0	Destino	Origen	ID de BSS	N/A
0	1	Destino	AP emisor	Origen	N/A
1	0	AP receptor	Origen	Destino	N/A
1	1	AP receptor	AP emisor	Destino	Origen

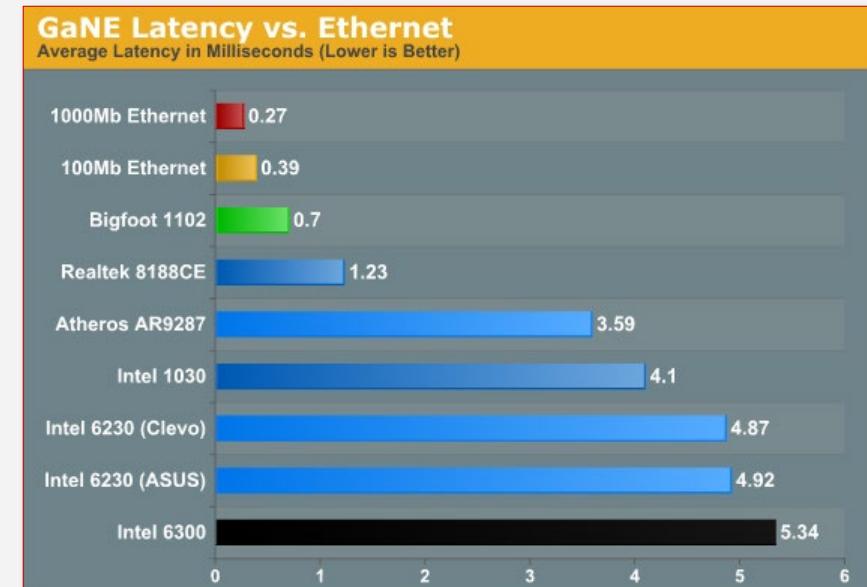
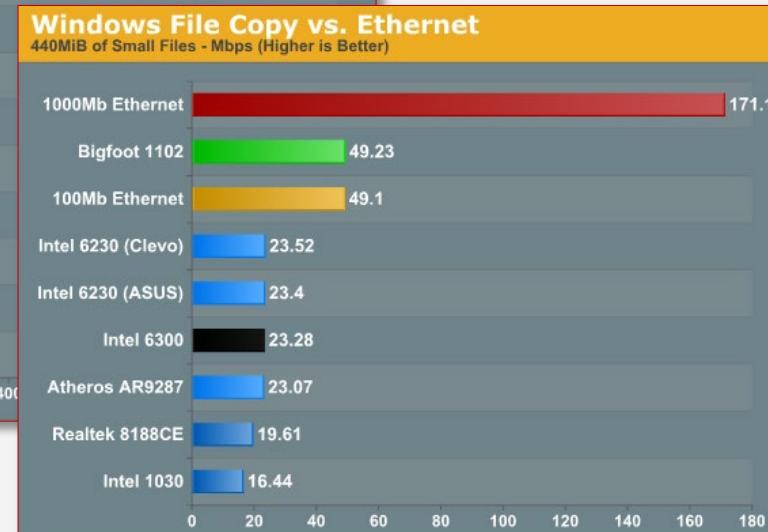
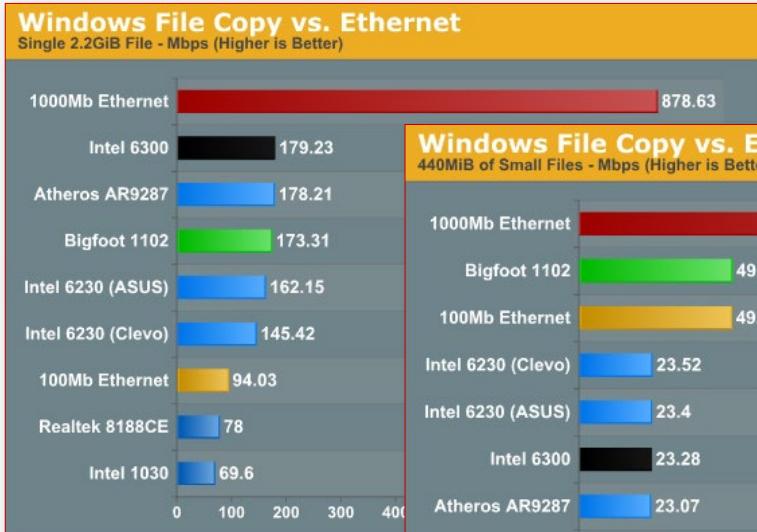


Redes IEEE 802.11: Aspectos prácticos

“Wifis normales” usan **infraestructura** (todos los mensajes pasan por el AP - no hay comunicación cliente a cliente)

¿Cable o Wifi?

- Cable en lo posible (rendimiento, latencia, distancia...)
- Wifi para movilidad (smartphones, tablets...)

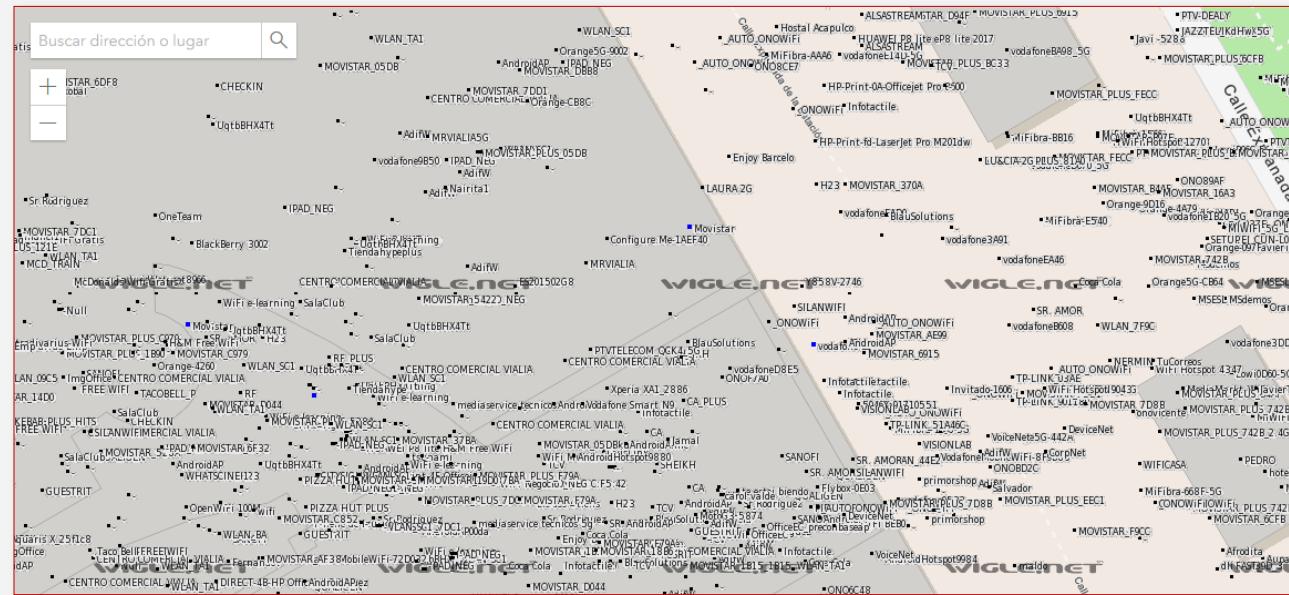


Redes IEEE 802.11: Aspectos prácticos

35

¿Cómo se identifica una Wifi?

- **SSID (Service Set Identifier):** Texto de 32 caracteres (máximo)



SSIDs recogidos en **wigle.net** en la estación de tren María Zambrano.

¿Ocultar el SSID?

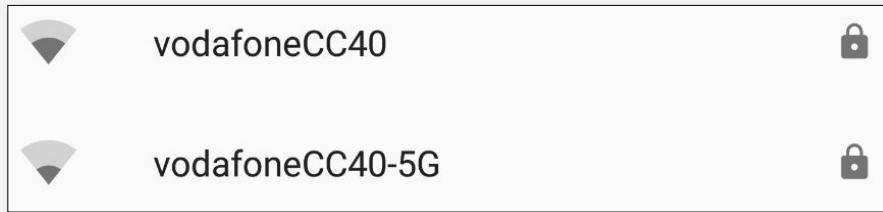
- Añade cierta seguridad, pero fácilmente obtenible con ciertos conocimientos

Redes IEEE 802.11: Aspectos prácticos

36

¿2.4 GHz o 5 GHz?

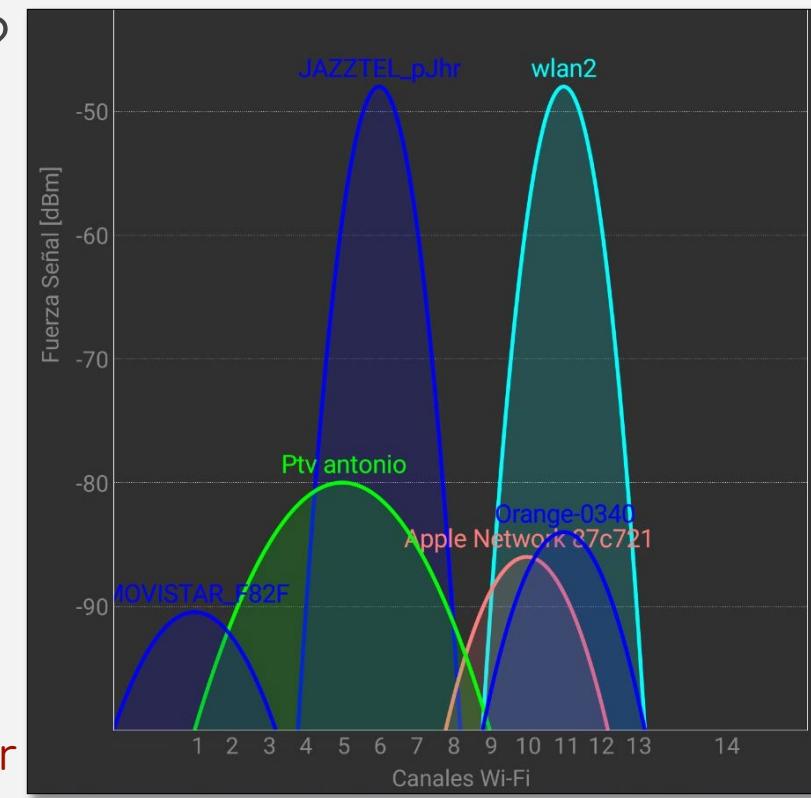
- 2.4 GHz mayor cobertura y compatibilidad... pero muy poblada
- 5 GHz menos usada y mayor rendimiento... pero menor cobertura
- Usar ambas ("dual band") ¿mismo SSID?



¿Canal?

- Canales solapados
- Ocupación variable
- Dependiente del lugar
- Modo "auto"

Wifi Analyzer



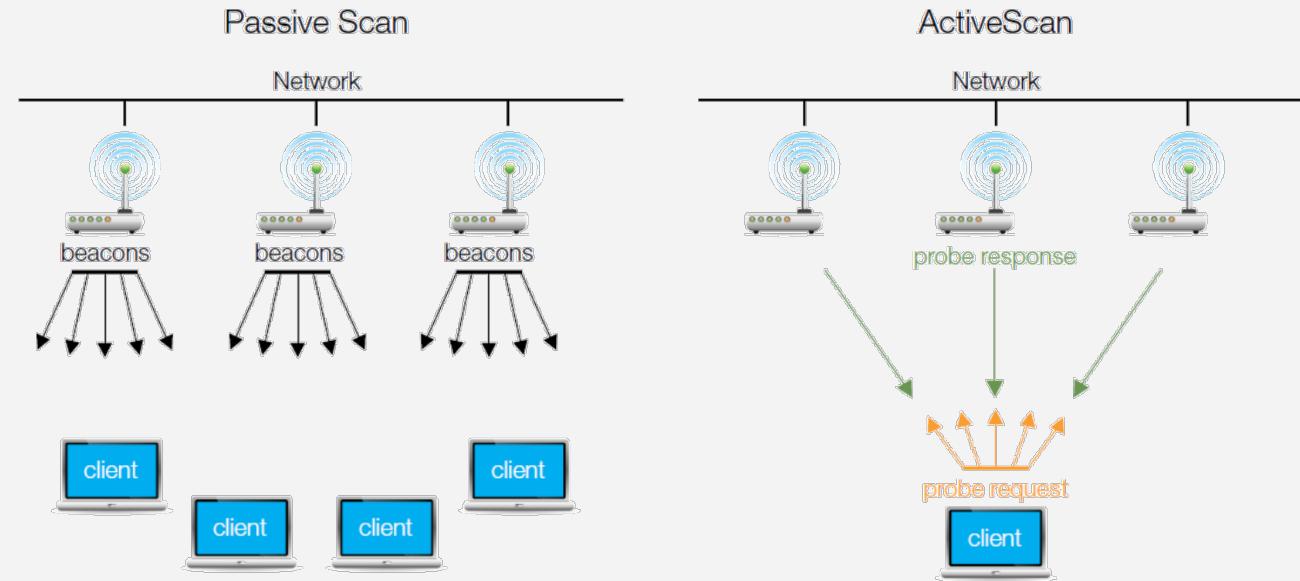
Redes IEEE 802.11: Aspectos prácticos

¿Cómo se sabe las wifis cercanas?

Mensajes especiales. Dos modos:

- **Pasivo:** el AP se anuncia (“Beacons”)
 - Monitorizar todos los canales constantemente
- **Activo:** el cliente pregunta las wifis (“Probe request”)
 - Problemas de privacidad (MAC, redes conocidas...)

	DIRECT-5LMSlmsON	
	wlan2	
	wlan2_5G	
	vodafoneCC40	
	vodafoneCC40-5G	



Redes IEEE 802.11: Aspectos prácticos

¿Cómo se encuentra y conecta a una wifi?

El cliente busca "martinet3" en el canal 8. No respuesta (activo)

Siemens_41:bd:6e	Broadcast	Beacon frame, SN=549, FN=0, Flags=....., BI=100, SSID=martinet3
NokiaDan_3d:aa:57	Broadcast	Probe Request, SN=55, FN=0, Flags=....., SSID=martinet3
NokiaDan_3d:aa:57	Broadcast	Probe Request, SN=56, FN=0, Flags=....., SSID=martinet3
Siemens_41:bd:6e	NokiaDan_3d:aa:57	Probe Response, SN=550, FN=0, Flags=....., BI=100, SSID=martinet3

El AP informa de su SSID y propiedades (pasivo)

- > IEEE 802.11 Beacon frame, Flags:
- ▼ IEEE 802.11 wireless LAN

 ▼ Fixed parameters (12 bytes)

 Timestamp: 0x000000026c2da183

 Beacon Interval: 0.102400 [Seconds]

 > Capabilities Information: 0x0411

 ▼ Tagged parameters (74 bytes)

 > Tag: SSID parameter set: martinet3

 > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]

 > Tag: DS Parameter set: Current Channel: 11

 ▼ Capabilities Information: 0x0411

 1 = ESS capabilities: Transmitter is an AP

 0. = IBSS status: Transmitter belongs to a BSS

 0. 00.. = CFP participation capabilities: No point coordinator at AP (0x00)

 1 = Privacy: AP/STA can support WEP

 0. = Short Preamble: Not Allowed

 0.. = PBCC: Not Allowed

El cliente busca "martinet3" en canal 11
Y el AP da información sobre su red

En los Probe Request se
puede usar sin indicar el
SSID y es una petición
a todos

Redes IEEE 802.11: Aspectos prácticos

39

¿Mejorar la cobertura?

Posición:

Centrado respecto a dispositivos

Evitar la atenuación

Evitar interferencias

Parámetros:

canal, frecuencia...

Extensores:

Los wifis (WDS) reducen el rendimiento (~ 50%):

STA -> REP -> AP -> REP -> STA

vs STA -> AP -> STA

Lo ideal son los extensores Ethernet (¿PLC? ¿MoCA?) o ¿Mesh?

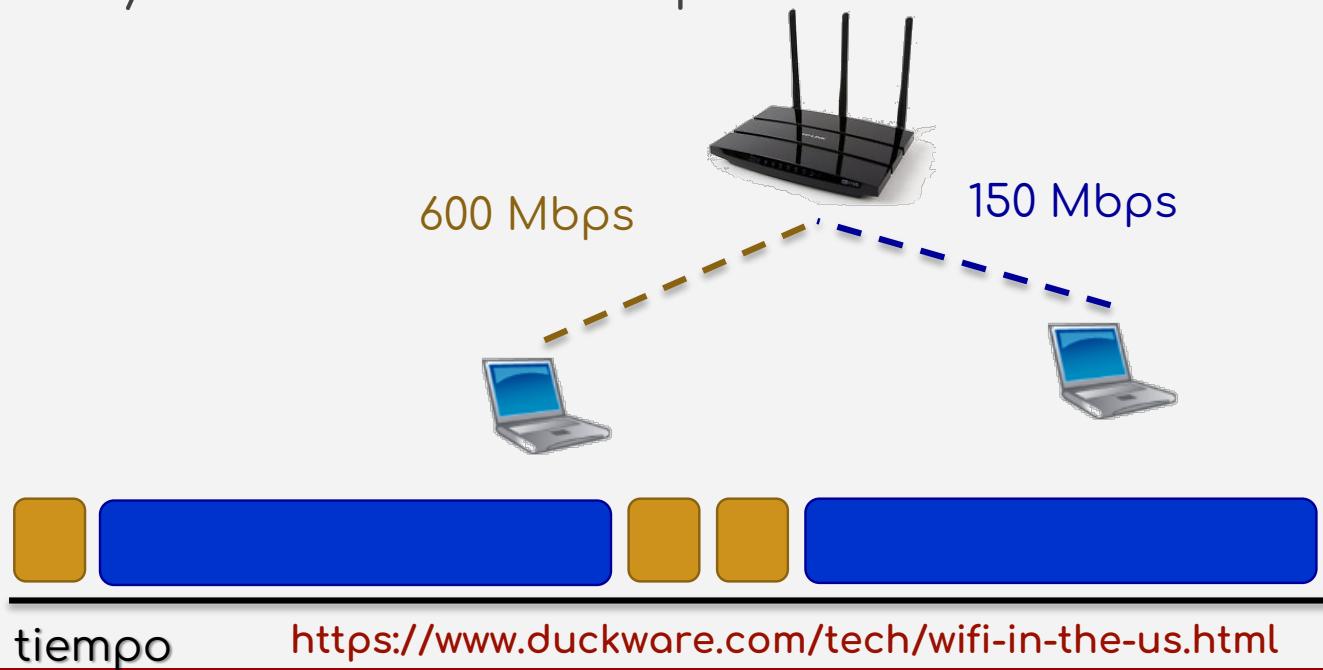
Material	Atenuación	Ejemplo
Cristal simple	Baja	Ventana
Madera	Baja	Puerta
Cristal tintado	Baja-Media	Ventana
Ladrillo	Baja-Media	Pared
Agua	Media	Acuario
Organismos	Media	Personas
Cartón Yeso	Media	Pladur
Yeso	Media	Pared
Cerámica	Media-Alta	Suelo / pared
Hormigón	Alta	Suelo / pared
Cristal anti-balas	Alta	Ventana
Metal	Alta	Puerta/Pared

Redes IEEE 802.11: Aspectos prácticos

40

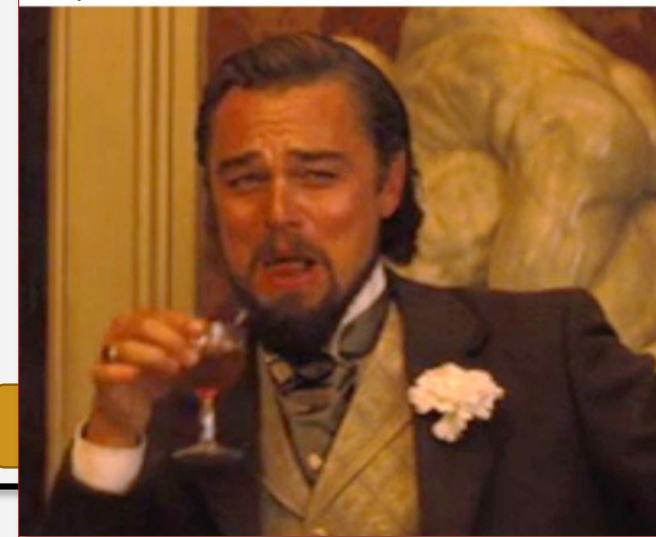
¿Estar a la última?

- Son retro-compatibles y con un acceso al medio “justo” y eso produce situaciones anómalas con equipos que usan diferentes
- Los APs (caro) cambiarlos cuando los de usuario mayoritariamente acepten el nuevo estándar



Yo: Me he gastado 500 euros en un router wifi mega tocho con 8x8 MIMO 802.11ax

Tu portátil/móvil/tele con 2x2-MIMO 802.11ac:



Redes IEEE 802.11: Aspectos prácticos

41

Seguridad

- No usar **redes abiertas** (sin esquemas adicionales)
- **Sistemas antiguos:** WEP ofrece tanto autenticación como cifrado.
Actualmente muy vulnerable (...ARP...)
- **Autenticación:** WPA/WPA2/WPA3 (2018)
 - Enterprise (MGT): servidor de autenticación (RADIUS)
 - Personal (PSK): clave pre-compartida
- **Requiere servicio de cifrado:** TKIP, AES...
- **WPS:** Mecanismo para compartir credenciales de forma automática (PIN, Botón, NFC o conexión USB). La versión con PIN es vulnerable en la actualidad

Redes IEEE 802.11: Aspectos prácticos

42

WIFI Direct, TLDS, Miracast y DLNA

- **WIFI Direct** permite crear de forma sencilla una red inalámbrica donde un equipo actúa de AP (implementa un AP software y servicios adicionales)

- **TLDS (Tunneled Direct Link Setup)**: adicción/corrección 802.11z para permitir comunicar directamente cliente en una red con infraestructura
- **Miracast (Screen Mirroring, AllShare cast...)**: “HDMI” inalámbrico (usa WIFI Direct)

- **DLNA (Digital Living Network Alliance)**: Servicio de comunicación, gestión, control y descubrimiento de recursos multimedia (independiente de los anteriores)


Tema 2: Capa de Enlace

Clase del 21/2/2023

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)



Organización del tema y la clase

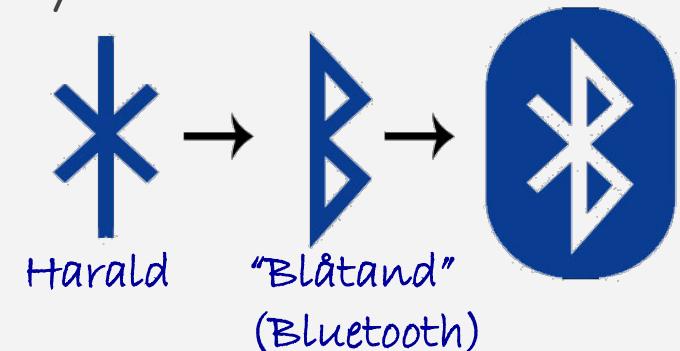
- **Funcionalidad** de la capa:
Comunicación directa entre equipos conectados directamente
- **Principales servicios:**
 - Fiabilidad (**control de error**),
 - saturación (**control de flujo**),
 - difusión: **direcccionamiento** y **acceso al medio**,
 - gestión
- **Casos concretos:**
 - **Ethernet** (802.3),
 - **Wifi** (802.11),
 - **Bluetooth** (802.15.1) (802.15.1)
 - **PPP** (RFC 1661)

LANs inlámbricas de área personal (PAN)

3

Bluetooth:

- Tecnología de LAN inalámbrica de área personal
- Permite la conexión de dispositivos variados: teléfonos, portátiles, cámaras, impresoras...
 - Reemplazar cables en conexión de teclados, impresoras...
 - Sensores de monitorización para control de salud
- Originalmente, proyecto de compañía Ericsson
 - Posteriormente se estandarizó como IEEE 802.15.1
- Red ad hoc: se forma de manera espontánea y sin acceso externo
 - Dispositivos se encuentran unos a otros
 - Forman una picorred

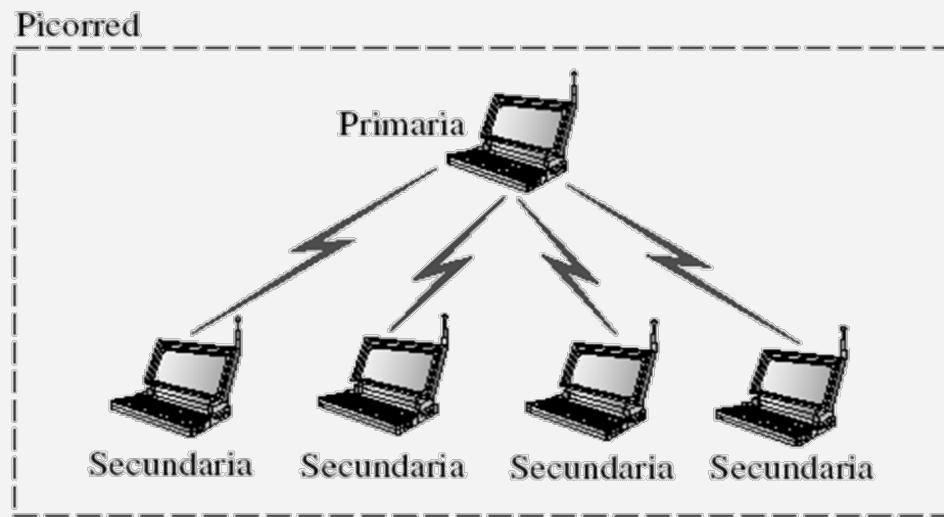


Bluetooth: arquitecturas

4

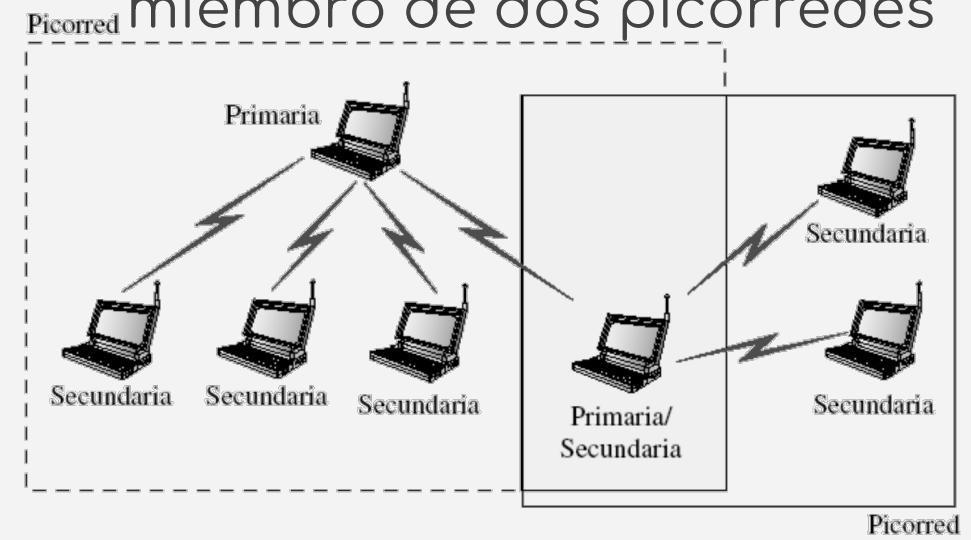
Arquitectura Picorred:

- Máximo 8 estaciones
- 1 estación actúa de primaria, el resto secundarias.



Arquitectura Red dispersa:

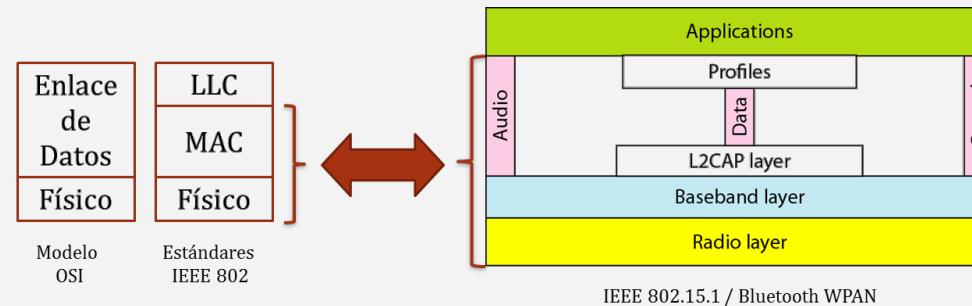
- Combinación de picorredes
- Una estación secundaria en una picorred actúa de primaria en otra
- Una estación puede ser miembro de dos picorredes



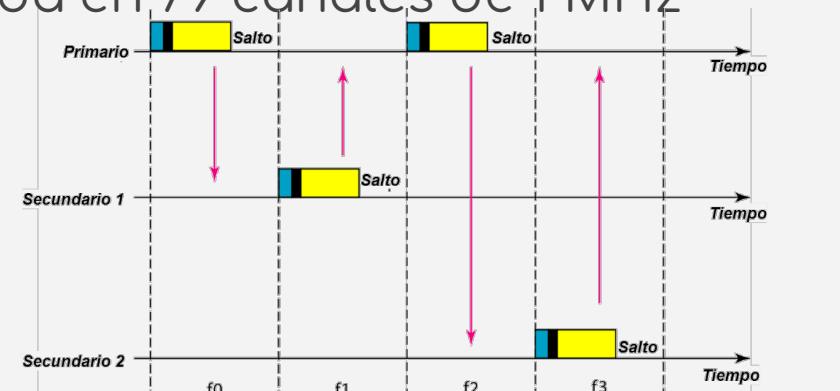
Bluetooth: Capas

Niveles en Bluetooth

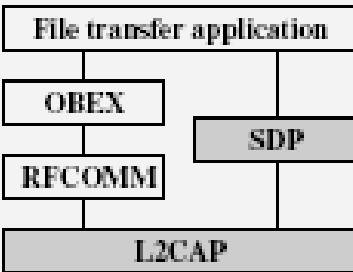
- No se corresponden exactamente con el modelo de Internet



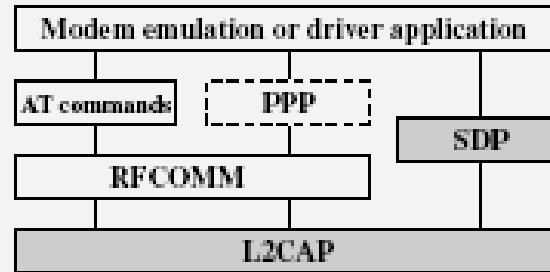
- Físico:**
 - Emplea banda ISM de 2.4 GHz, dividida en 79 canales de 1 MHz
- MAC:**
 - TDMA** (Acceso Múltiple por División en el Tiempo)
 - La comunicación ocurre **SÓLO** entre el **primario** y el **secundario**
 - Centralizado
- Niveles superiores: Bluetooth define protocolos específicos para cada propósito (**perfiles Bluetooth**)



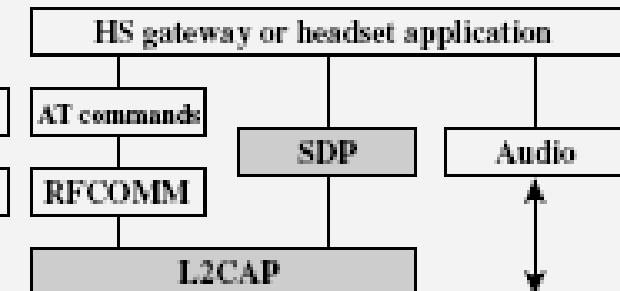
Bluetooth: Perfiles



(a) File transfer

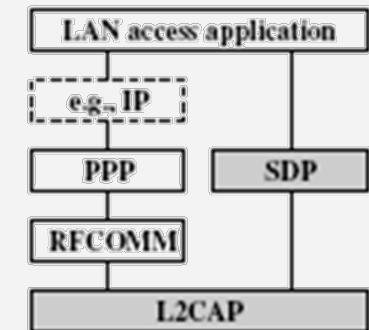


(b) Dial-up networking

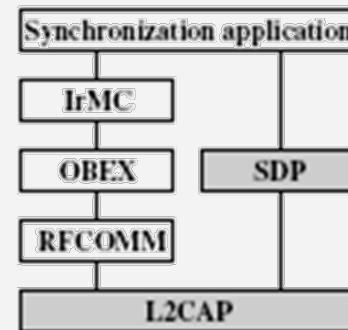


(c) Cordless phone and intercom

(f) Headset



(e) LAN access



(d) Synchronization

Bluetooth Low Energy (BLE)

Versión para IoT (Internet of the Things)

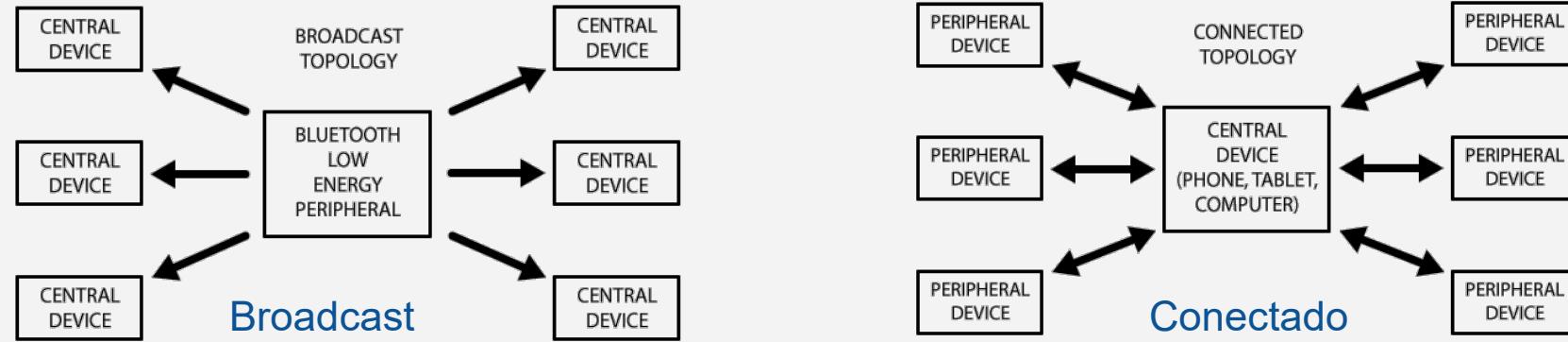
- Ventaja: facilidad de comunicación con dispositivos móviles (Android, iOS...)

Dos roles principales:

- Periféricos: Nodos de baja potencia y recursos (sensores)
- Central: Nodo con mayores recursos (móviles, tablets...)

Dos modos de comunicación:

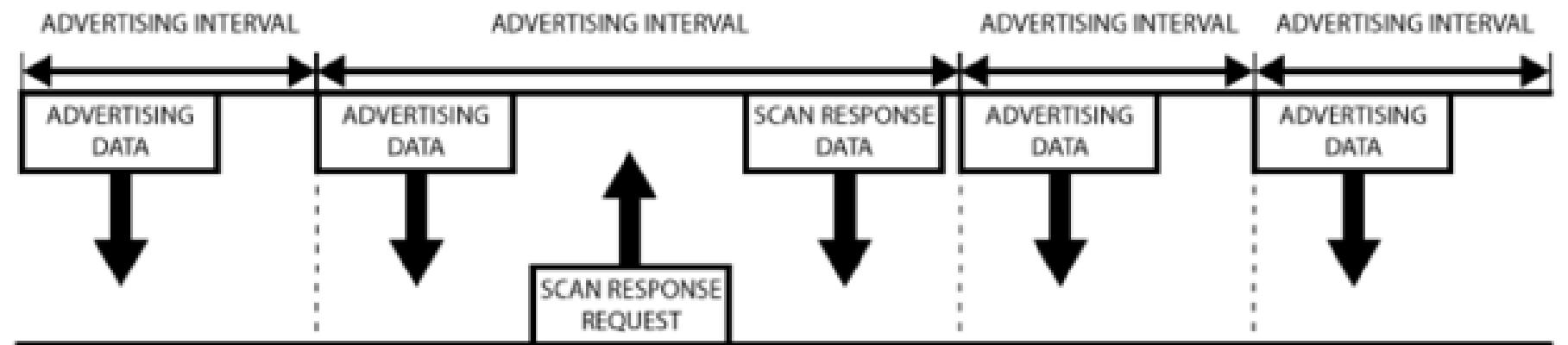
- Broadcast (perfil GAP)
- Conectado (perfil GATT)



BLE: Broadcast

Broadcast (advertising)

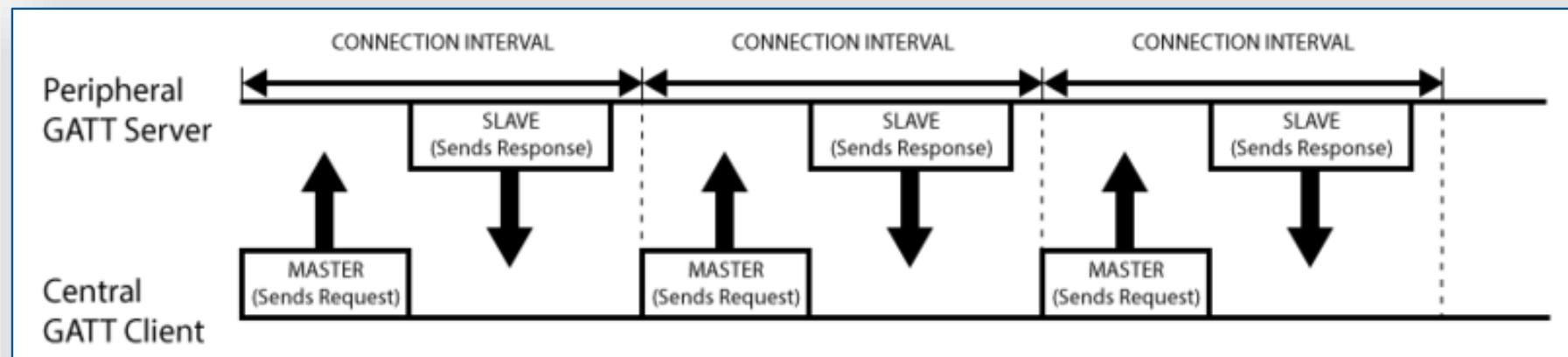
- Los periféricos emiten mensajes de **advertising** a intervalos regulares
- Ahorro de **energía** según el **intervalo** seleccionado
- El central puede solicitar información con un mensaje de **scan**. Puede que el periférico no soporte estos mensajes (es opcional)
- Poca información (31 B) **unidireccional** (sensor -> central)



BLE: Conectado

Conectado

- Los periféricos actúan de servidor a los que el central (cliente) hace peticiones
- Se basa en transacciones
- Todas las transacciones son iniciadas por el dispositivo maestro en intervalos fijos
- Comunicación bidireccional



Bluetooth: Transacciones

Heart Rate Service

	Handle	UUID	Permissions	Value
Service	0x0021	SERVICE	READ	HRS
Characteristic	0x0024	CHAR	READ	NOT 0x0027 HRM
	0x0027	HRM	NONE	bpm
Descriptor	0x0028	CCCD	READ/WRITE	0x0001
Characteristic	0x002A	CHAR	READ	RD 0x002C BSL
	0x002C	BSL	READ	<i>finger</i>