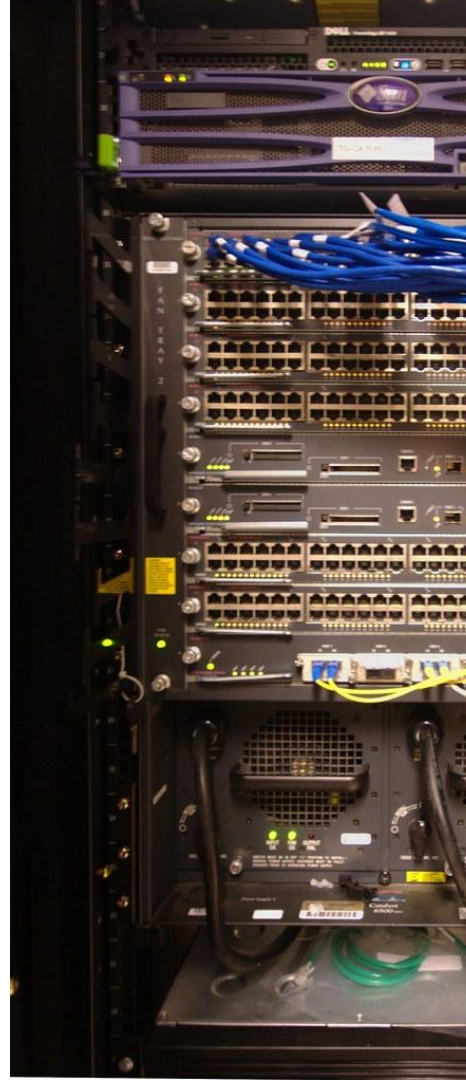




# CIT2114 - Redes de Datos

## Capítulo 4: Capa Enlace de Datos

Rodrigo Muñoz Lara



# Funciones de la capa de Enlace de Datos

# Funciones de la capa de Enlace de Datos

- Manejar los errores de transmisión
- Manejo del Framing o entramado
- Regular el flujo de datos para que receptores lentos no sean saturados por emisores rápidos.
- 

Para cumplir con estas metas, la capa de enlace de datos toma de la capa de red los paquetes y los **encapsula** en tramas para transmitirlos. Cada trama contiene un encabezado, un campo de carga útil (payload) para almacenar el paquete y un terminador o final

# Manejo de Errores en la transmisión

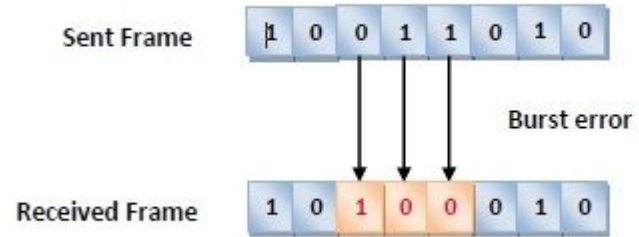
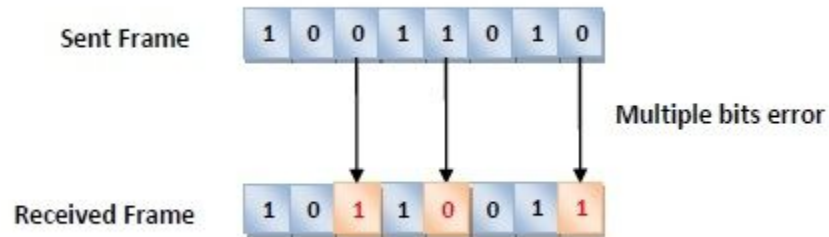
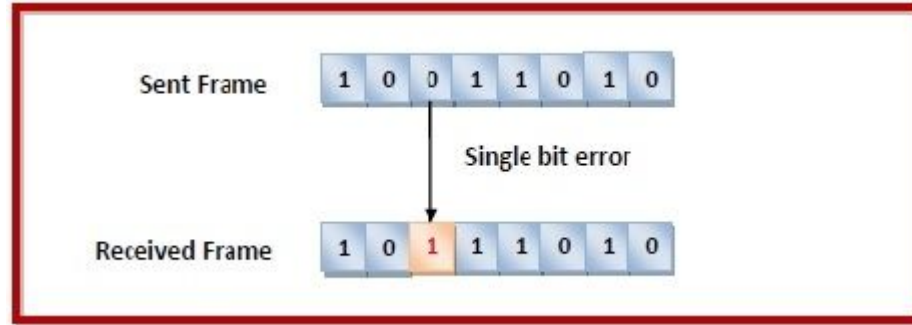
# Manejo de Errores en la transmisión

## Tipos de Errores

- Single bit error: En la trama recibida, solo se ha corrompido un bit, es decir, se cambió de 0 a 1 o de 1 a 0.
- Multiple bits error: En la trama recibida, más de un bit está dañado.
- Burst error: En la trama recibida, más de un bit *consecutivo* está dañado.

# Manejo de Errores en la transmisión

## Tipos de Errores



# Manejo de Errores en la transmisión

## Detección

Esta estrategia considera incluir suficiente redundancia para permitir que el receptor **sepa** que ha ocurrido un error (pero no qué error) y entonces solicite una retransmisión

## Corrección

En esta estrategia se considera incluir suficiente información redundante en cada bloque de datos transmitido para que el receptor pueda **deducir** lo que debió ser el carácter transmitido

**¿Detección o Corrección?**

# Manejo de Errores en la transmisión

En ambas estrategias **se agrega información adicional** llamada código. Existen dos grupos de códigos:

- Código de Detección de errores:
  - Usado para canales altamente confiables (fibra óptica).
  - En este tipo de canales, es más eficiente detectar el error y solicitar una retransmisión.
- Código de Corrección de errores:
  - Usado para canales que causan muchos errores (canales inalámbricos).
  - Es este tipo de canales es más eficiente corregir el error que solicitar una retransmisión que también puede venir con errores.
  - Método más usado: FEC (Forward Error Correction)



# Manejo de Errores en la transmisión

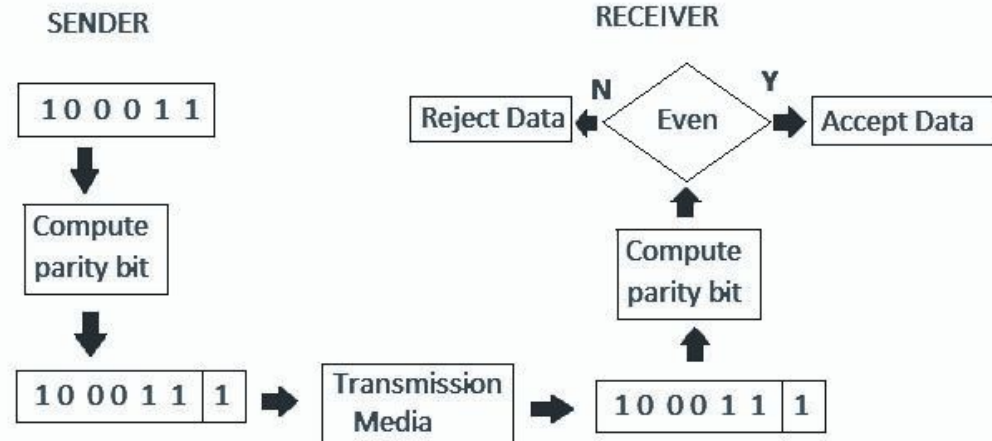
## Códigos de Detección de errores

- Paridad
- Checksum
- Cyclic Redundant Checks (CRC)

# Manejo de Errores en la transmisión

## Códigos de Detección de errores

- Paridad (unidimensional):
  - Se agrega un bit de paridad para detectar errores
  - La verificación de paridad es adecuada solo para la detección de errores de un solo bit.
  - Frame 1100100 □ 1100100**1**



# Manejo de Errores en la transmisión

## Códigos de Corrección de errores

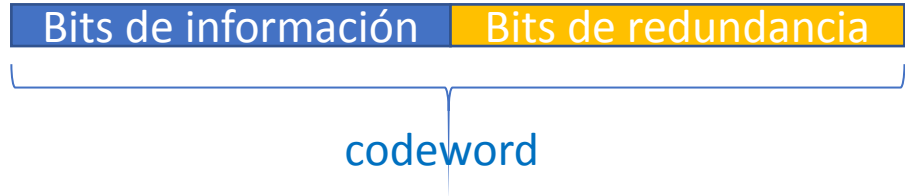
- Forward Error Correction (FEC)
  - Hamming Codes
  - Binary Convolution Code
  - Reed – Solomon Code
  - Low-Density Parity-Check Code

# Manejo de Errores en la transmisión

## Códigos de Corrección de errores

- Forward Error Correction (FEC)
  - **Hamming Codes:** Solo detecta y corrige el error en **un bit**
  - Definiciones:

- Codeword o palabra codificada
  - $m$  bits de información
  - $r$  bits de redundancia
  - $n$  bits de palabra de código
  -



$$n = m + r$$

- La cantidad de bits de Hamming cumple:

$$2^r \geq m + r + 1$$

# Manejo de Errores en la transmisión

## Códigos de Corrección de errores

Ejemplo: Sea la palabra de datos de 7 bits **0110101** ( $m = 7$ ).  $r = 4$  cumpliría la ecuación

$$2^r \geq m + r + 1$$

Para encontrar los bits de redundancia se siguen los siguientes pasos:

1. Crear un codeword de largo  $n = m + r$
2. Todos los bits cuya posición es potencia de dos se utilizan como bits de paridad (posiciones 1,2,4,8,16,32,64, etc.)
3. Los bits del resto de posiciones son usados como bits de datos (posiciones 3,5,6,7,9,10,11,12,13,14,15)

# Entramado o framing

# Entramado o framing

- **Problema:** ¿Cómo sabe el Receptor cuando comienza o finaliza una trama si el solo recibe un flujo de bits?
- Una solución podría ser introducir intervalos de tiempo entre las tramas.
- Sin embargo, las redes pocas veces ofrecen garantías sobre la temporización, por lo que es posible que estos intervalos sean eliminados o que puedan introducirse otros intervalos durante la transmisión.
- Métodos para manejar el entramado o framing:
  - Método de conteo de caracteres
  - Bandera con relleno de bytes

# Entramado o framing

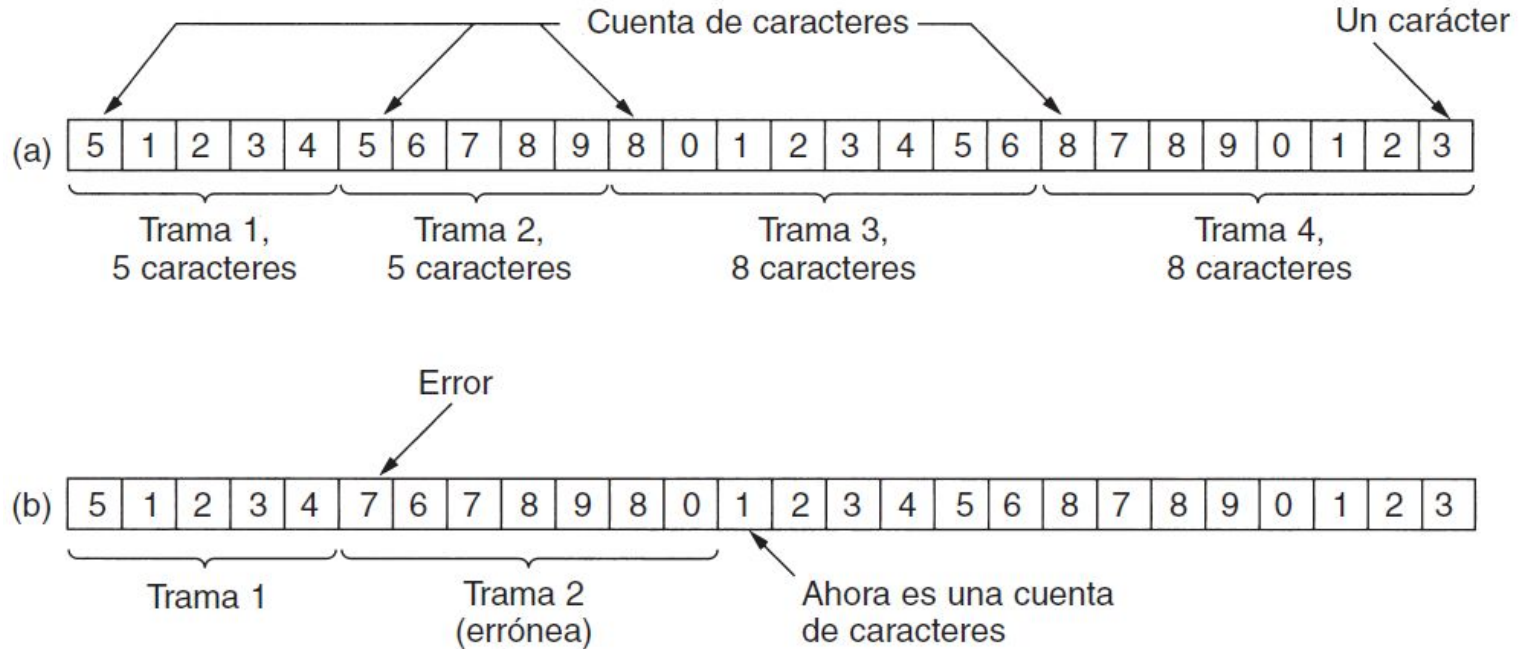
## Método de Conteo de caracteres:

- Campo en el encabezado para especificar el número de bytes en la trama.
- Cuando la capa de enlace de datos del destino ve la cuenta de bytes, sabe cuántos bytes siguen y, por lo tanto, dónde está el fin de la trama.
- **Problema:** el encabezado puede ser dañado y no sería posible determinar donde comienza la trama



# Entramado o framing

## Método de Conteo de caracteres:



**Figura 3-4.** Un flujo de caracteres. (a) Sin errores. (b) Con un error.

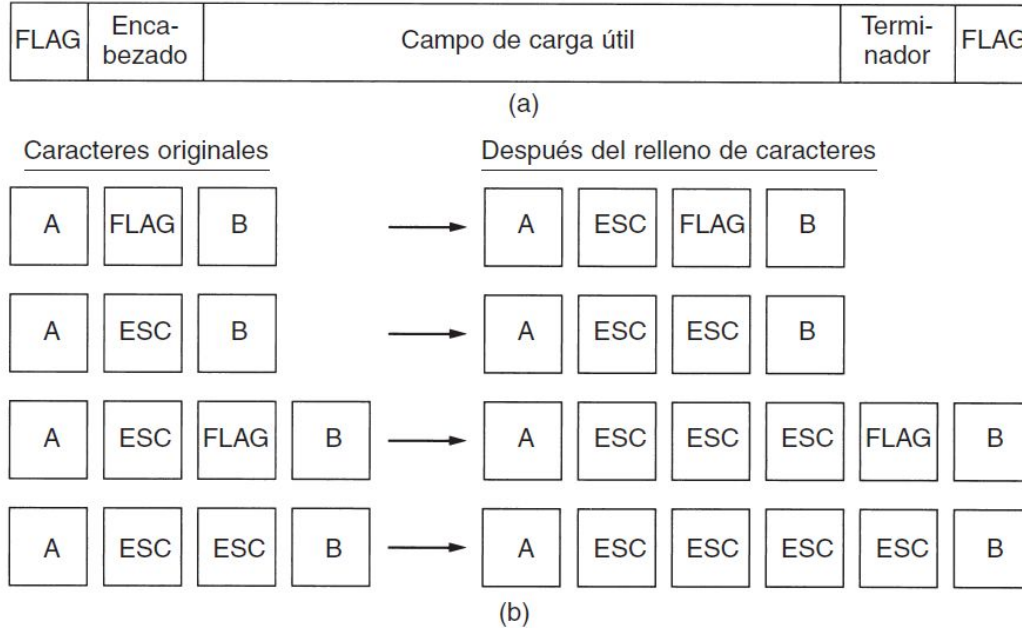
# Entramado o framing

## **Banderas, con relleno de bytes:**

- Trama inicia y termina con bytes especiales.
- Los bytes especiales se llaman Bandera o Flag
- Evita el problema de tener que sincronizar nuevamente después de un error.
- Problema: Se puede dar el caso de que el patrón de bits de la bandera aparezca en los datos (payload), lo que interferiría en el entramado.
- Solución: insertar relleno de bytes.

# Entramado o framing

## Banderas, con relleno de bytes:



**Figura 3-5.** (a) Una trama delimitada por banderas. (b) Cuatro ejemplos de secuencias de bytes antes y después del relleno de caracteres.

# Control de Flujo

# Control de Flujo

## ¿Por qué usar el control de Flujo?

El emisor puede querer transmitir tramas de manera sistemática y a mayor velocidad que aquella con que puede aceptarlos el receptor.

El control de flujo permite adaptar la velocidad de envío del transmisor a la velocidad de procesamiento del receptor.

# Control de Flujo

Dos métodos:

**control de flujo basado en retroalimentación (feedback-based):** el receptor regresa información al emisor autorizándolo para enviar más datos o indicándole su estado.

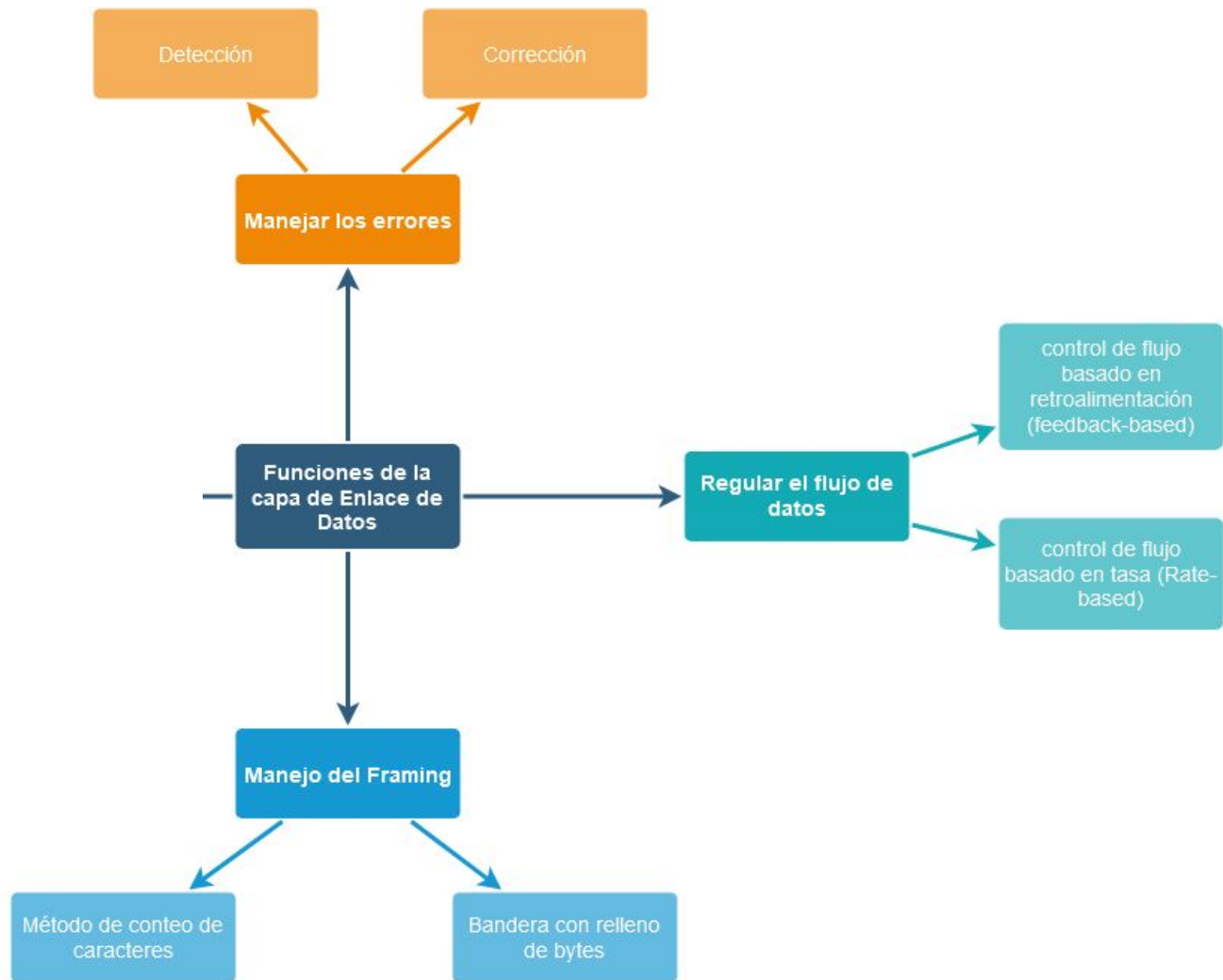
**control de flujo basado en tasa (Rate-based),** el protocolo tiene un mecanismo integrado que limita la tasa a la que el emisor puede transmitir los datos, sin recurrir a retroalimentación por parte del receptor.

# Control de Flujo

## control de flujo basado en retroalimentación

Puedes enviarme n tramas ahora, pero una vez que lo hagas, no envíes nada más hasta que te indique que continúes

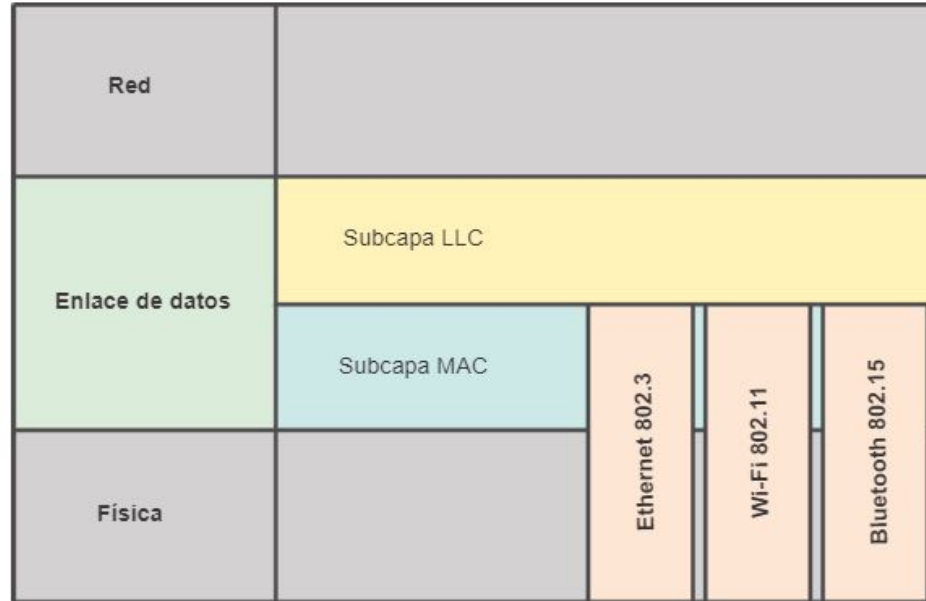
```
[-] Ethernet II, Src: 42networ_30:41:50 (00:0f:5d:30:41:50), Dst: Spanning-tree-(for-bridges)_01 (01:80:c2:00:00:01)
  [-] Destination: Spanning-tree-(for-bridges)_01 (01:80:c2:00:00:01)
    Address: Spanning-tree-(for-bridges)_01 (01:80:c2:00:00:01)
    .... ..1 .... = IG bit: Group address (multicast/broadcast)
    .... ..0. .... = LG bit: Globally unique address (factory default)
  [-] Source: 42networ_30:41:50 (00:0f:5d:30:41:50)
    Address: 42networ_30:41:50 (00:0f:5d:30:41:50)
    .... ..0 .... = IG bit: Individual address (unicast)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    Type: MAC Control (0x8808)
[-] MAC Control
  Pause: 0x0001
  Quanta: 65535
```





# Subcapa de control de acceso al medio o Media Access Control Layer

# Introducción



# Subcapa MAC

Las redes pueden dividirse en dos categorías:

- las que utilizan conexiones **punto a punto**
- y las que utilizan **canales de difusión o broadcast**.

Este capítulo trata las redes de difusión y sus protocolos.

En cualquier red de difusión, **el asunto clave es la manera de determinar quién puede utilizar el canal cuando hay competencia por él.**

# Subcapa MAC

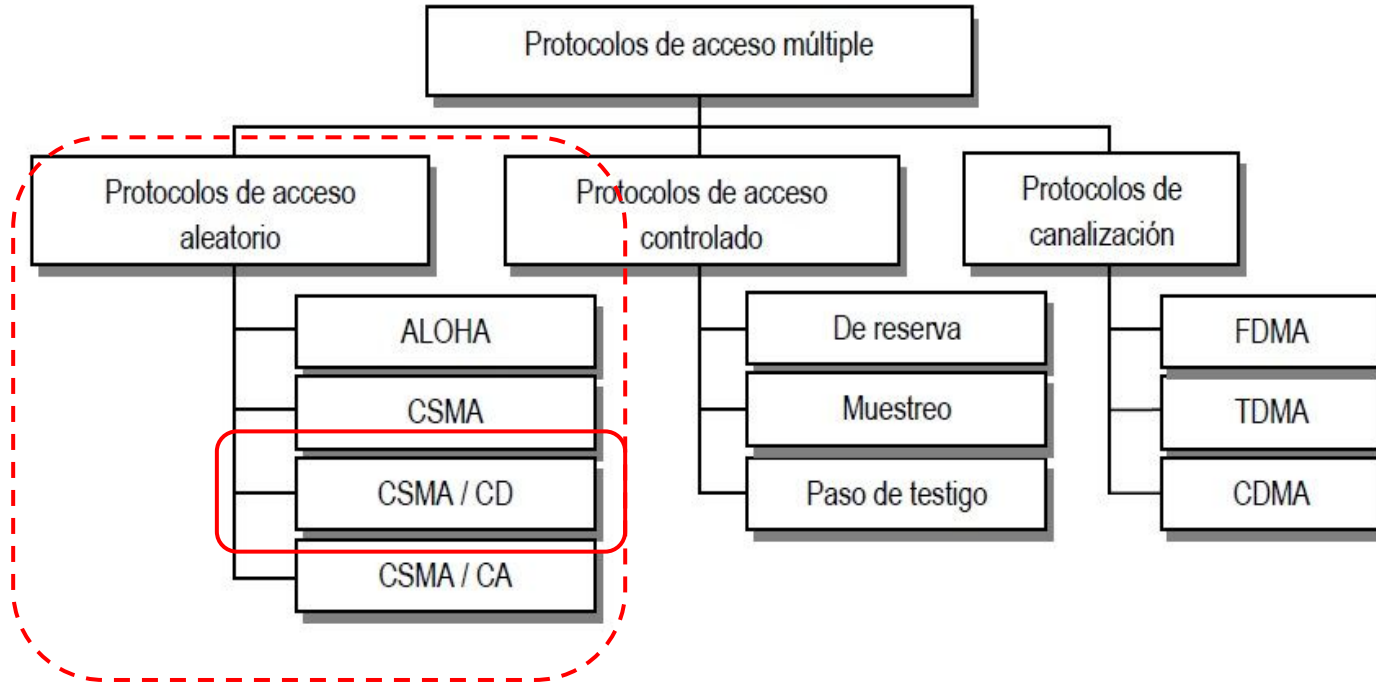
Los protocolos encargados de manejar el acceso en un canal de difusión se llaman **Protocolos de Acceso Múltiple**.

Existen tres tipos de Protocolos de Acceso Múltiple:

- Protocolos de acceso aleatorio
- Protocolos de acceso controlado
- Protocolos de canalización

En este curso revisaremos los **protocolos de acceso aleatorio**.

# Subcapa MAC



# Subcapa MAC

## Colisiones

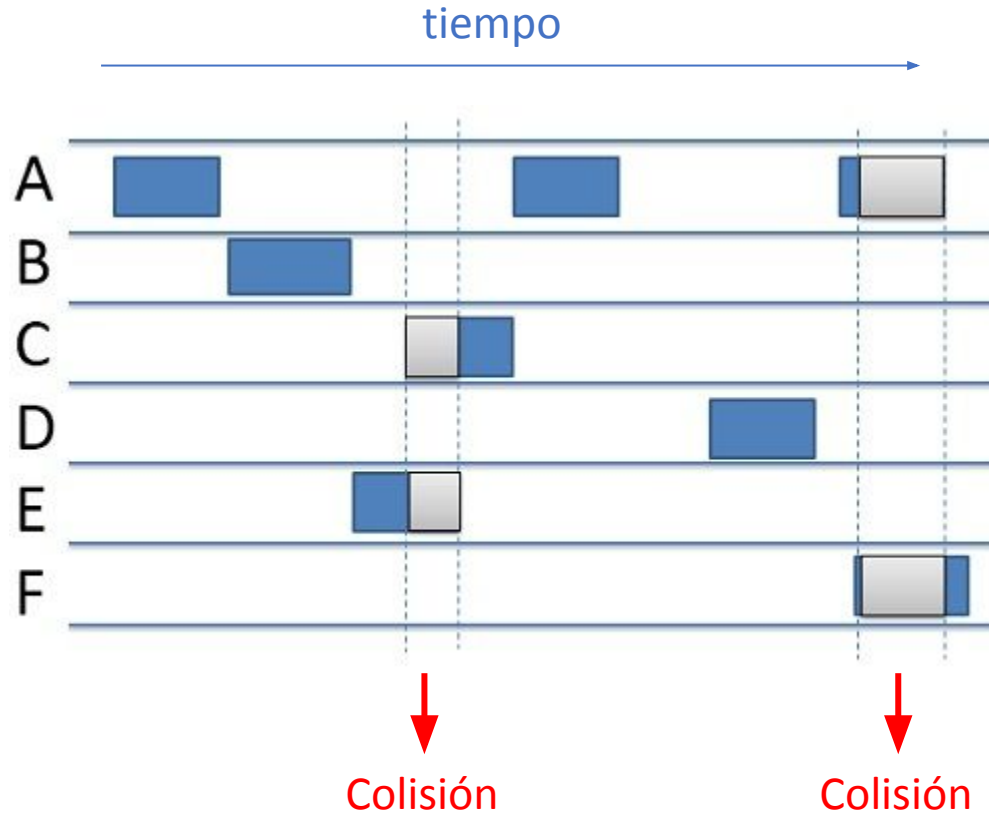
Para detectar si se va a producir una colisión, la estación comprueba si la señal transmitida es idéntica a la del medio de transmisión.

Si no fuera así, otra estación transmitiría al mismo tiempo, distorsionando así la señal del Bus.

## ¿Qué es un dominio de colisión?

Un dominio de colisión es un **segmento físico de una red** en el que las estaciones comparten un medio de transmisión y pueden colisionar

# Subcapa MAC



# Protocolos de acceso aleatorio

## Carrier Sense Multiple Access (CSMA)

El número de colisiones de los sistemas Aloha se puede reducir detectando la portadora antes de la transmisión.

CSMA es un protocolo de **control de acceso al medio** en el cual un **nodo verifica la ausencia de tráfico antes de transmitir** en un medio compartido.

Si al verificar el medio antes de transmitir una señal es detectada, el nodo **espera a que la transmisión en progreso finalice** antes de iniciar su propia transmisión.



# Protocolos de acceso aleatorio

## Carrier Sense Multiple Access (CSMA)

- CSMA indica que si el transmisor desea enviar datos pero detecta una transmisión en curso, este debe esperar para el envío de estos.
- Problema: Ya que varias estaciones pueden haber detectado la transmisión y estar a la espera para transmitir cuando el canal esté desocupado, pueden colisionar ya que todas ellas desean transmitir a la vez
- Solución: Hacer que la espera para volver a transmitir despues que el canal está desocupado sea aleatoria (con algun grado de probabilidad)

# Protocolos de acceso aleatorio

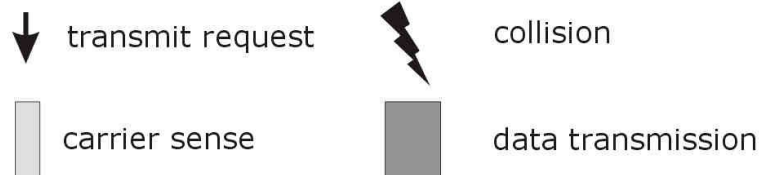
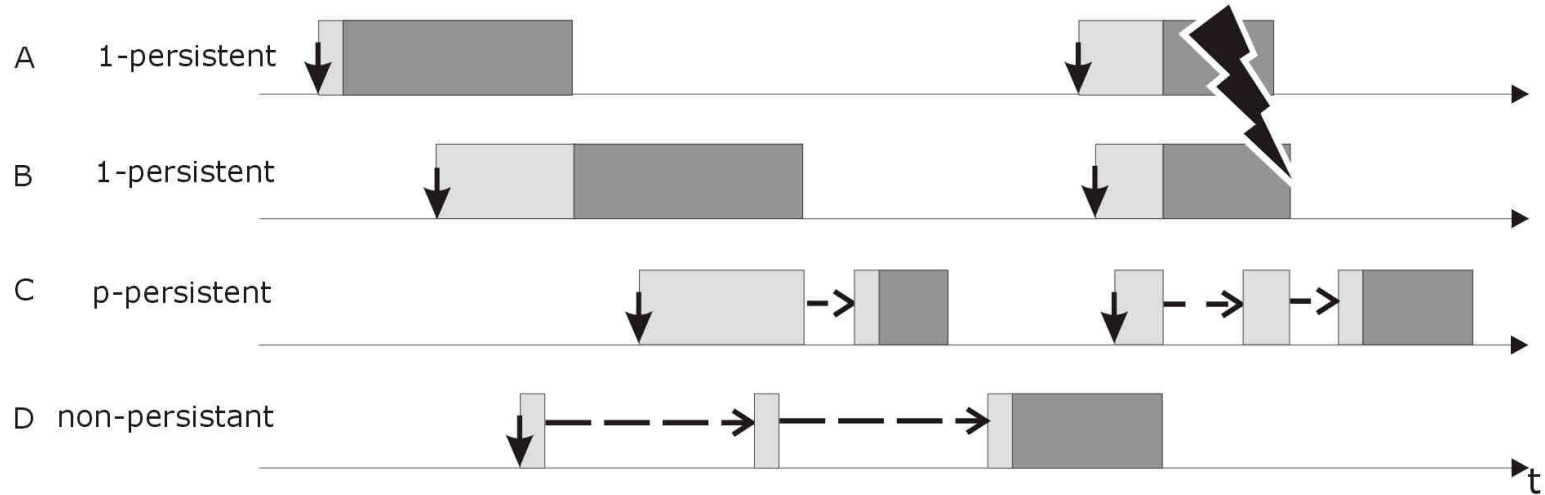
## Carrier Sense Multiple Access (CSMA)

Variantes de CSMA:

- CSMA persistente-1: estación transmite inmediatamente cuando encuentra que el canal está inactivo (escucha continua)
- CSMA persistente-p: La estación transmite con una probabilidad de  $p$  cuando encuentra que el canal está inactivo. Cuando el canal está activo, espera tiempo aleatorio con probabilidad  $q=1-p$
- CSMA no persistente: el nodo detecta el canal, si está inactivo, envía los datos; de lo contrario, verifica el medio después de una cantidad de tiempo aleatoria (no continuamente) y transmite cuando se encuentra inactivo.

# Protocolos de acceso aleatorio

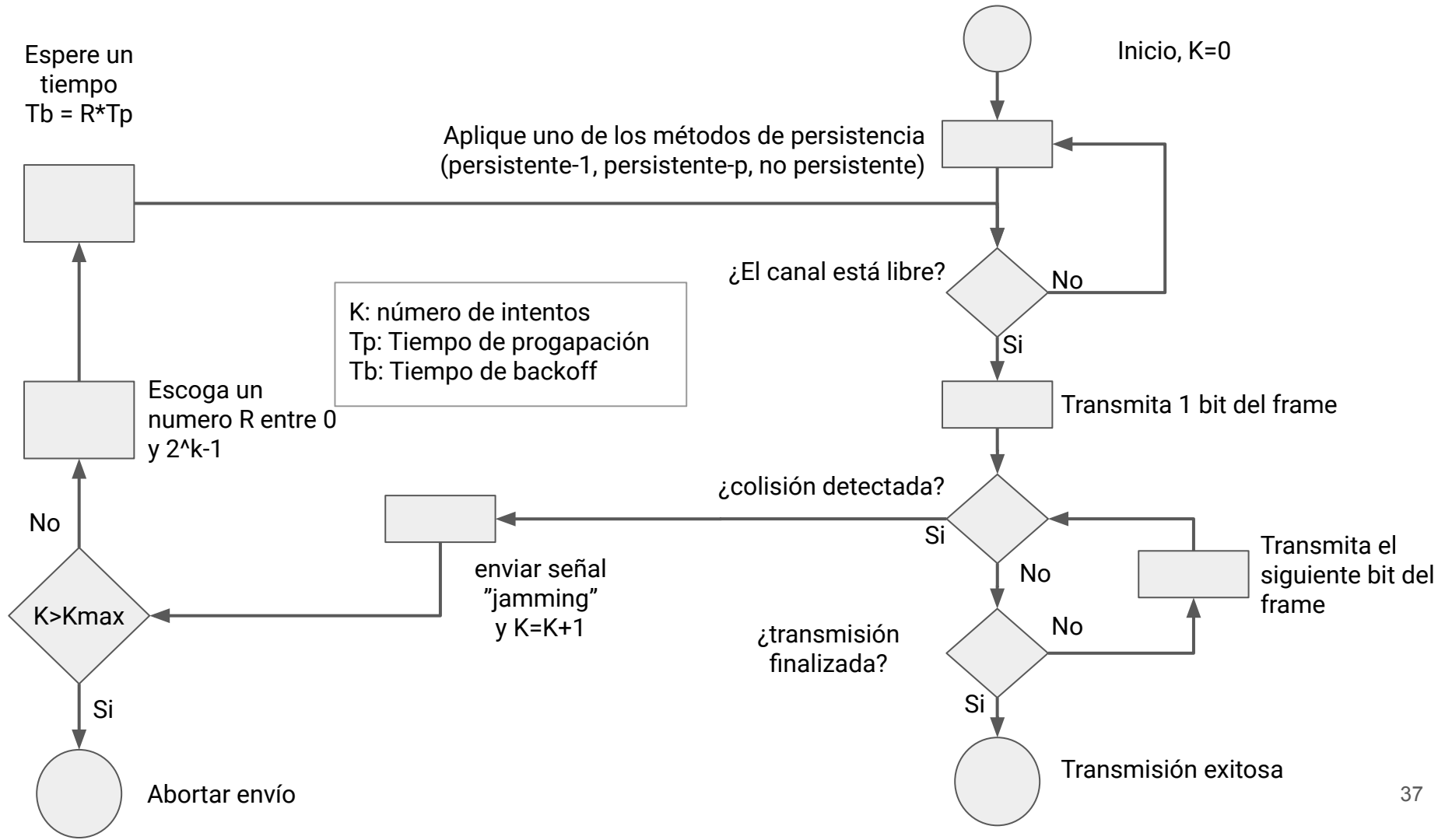
## Carrier Sense Multiple Access (CSMA)



# Protocolos de acceso aleatorio

## Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

- El método CSMA **no dice** qué hacer en caso de que haya una colisión mientras el nodo está transmitiendo un mensaje.
- En **CSMA/CD**, la técnica consiste en escuchar el medio mientras se transmite
- Si la señal escuchada es diferente a la que se transmite, se sabe que hay una colisión
- Ante la presencia de colisión se pasa a una fase de contención



# Ethernet

# Subcapas en Ethernet

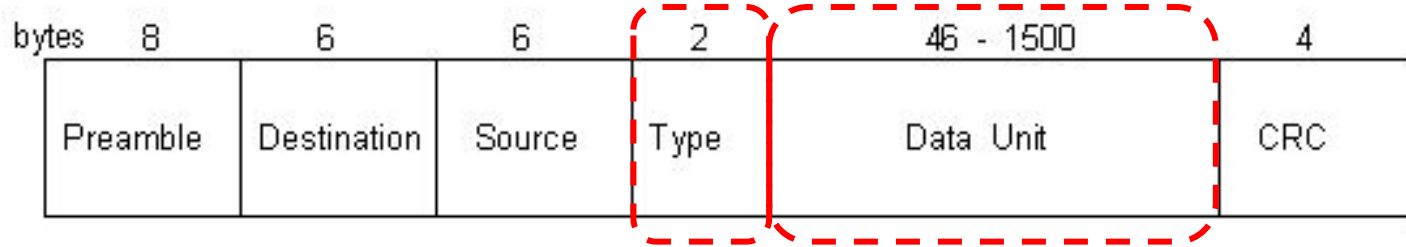
Data Link Layer	LLC Sublayer	Ethernet	IEEE 802.2				
	MAC Sublayer		IEEE 802.3 (Ethernet)	IEEE 802.3u (FastEthernet)	IEEE 802.3z (GigabitEthernet)	IEEE 802.3ab (GigabitEthernet over Copper)	Token Ring/IEEE 802.6
Physical Layer	Physical Layer		FDDI				

# Subcapa Media Access Control (MAC)

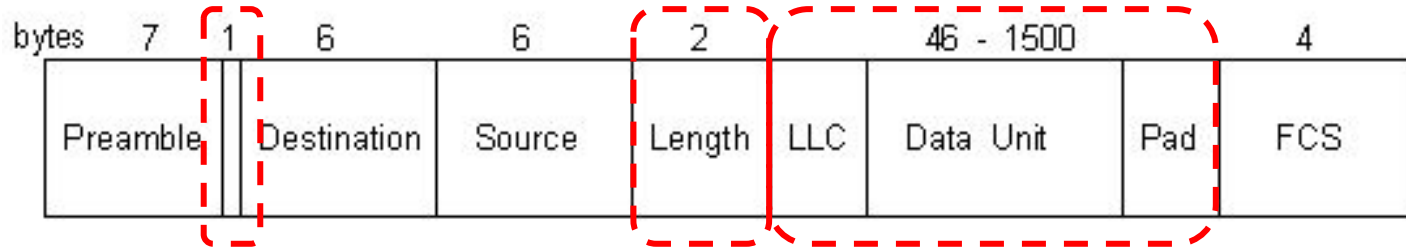
<b>Original IEEE</b>	<b>IEEE Shorthand Name</b>	<b>Informal Name(s)</b>	<b>Speed</b>	<b>Typical Cabling</b>
802.3i	10BASE-T	Ethernet	10 Mbps	UTP
802.3u	100BASE-T	Fast Ethernet (Fast E)	100 Mbps	UTP
802.3z	1000BASE-X	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	Fiber
802.3ab	1000BASE-T	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	UTP
802.3ae	10GBASE-X	10 GbE	10 Gbps	Fiber
802.3an	10GBASE-T	10 GbE	10 Gbps	UTP
802.3ba	40GBASE-X	40GbE (40 GigE)	40 Gbps	Fiber
802.3ba	100GBASE-X	100GbE (100 GigE)	100 Gbps	Fiber



# Trama Ethernet y IEEE 802.3



DIX Ethernet Packet



IEEE 802.3 Frame

# Direcciones Física o MAC Address

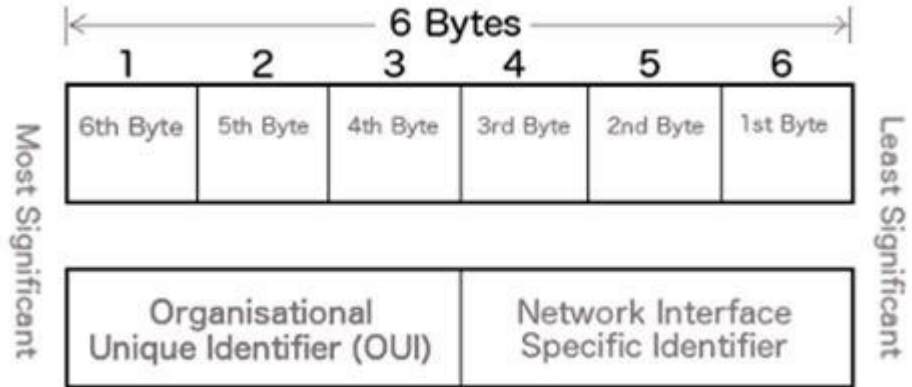
48 bits o 6 bytes de largo

Compuesta por dos partes

- 24 bits llamados OUI: identifica quien es el fabricante del hardware
- 24 bits llamados NSI: numero de serie que identifica al dispositivo fabricado

<https://macvendors.com/>

Dirección ÚNICA en el mundo



# Direccionamiento Ethernet

Cuando un host A desea comunicarse con un host B dentro de la misma subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del host B para la MAC de destino.

Cuando un host A desea comunicarse con un host B que esta fuera de la subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del default gateway para la MAC de destino.

SIEMPRE la MAC de destino corresponde a un host que está en la misma subred que el host de origen



# Direccionamiento Ethernet

Existe una dirección MAC llamada dirección Broadcast que permite enviar una trama a todos los equipos en una subred, siempre y cuando no pasen a través de un router.

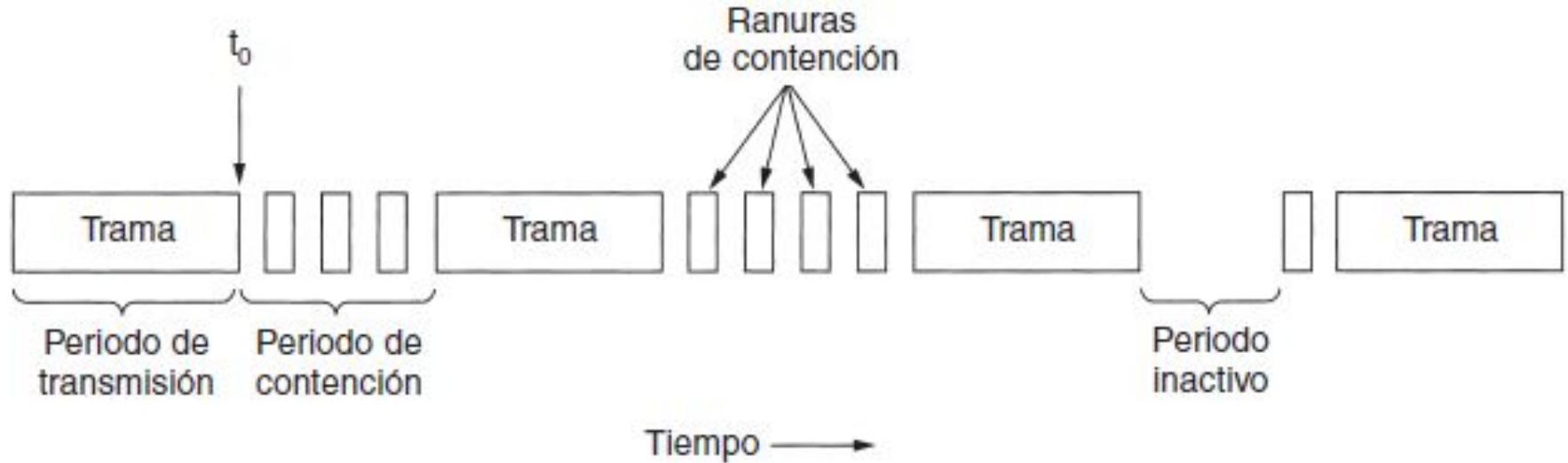
La dirección Broadcast ethernet es FF:FF:FF:FF:FF:FF

Este tipo de comunicación es llamada: **Broadcast de capa 2**

# Algoritmo de retroceso exponencial binario

- Después de una colisión, el tiempo es dividido en ranuras de tiempo o *timeslots*, igual al tiempo de propagación ida y vuelta del segmento ethernet. Esto corresponde al tiempo de 512 bits o  $51,2 \mu s$
- Después de la primera colisión, cada estación espera 0 ó 1 *timeslot* antes de intentar el envío nuevamente.
- Después de una segunda colisión, cada estación espera 0, 1, 2 ó 3 *timeslot* antes de intentar el envío nuevamente.
- Después de la **n-ésima** colisión, cada estación espera entre 0 y  $(2^n - 1)$  *timeslot* antes de intentar el envío nuevamente.
- Después de 10 colisiones el numero de espera siempre es entre 0 y 1023 *timeslots*
- Después de 16 colisiones se da por fallida la transmisión

# Algoritmo de retroceso exponencial binario



# Address Resolution Protocol (ARP)

# Address Resolution Protocol (ARP)

**¿Qué dirección de capa 2 pondría en un frame que va desde su PC a un computador en China?**

Imposible tener una tabla con TODAS las direcciones de capa 2 de todos los computadores del mundo.

Todos los computadores que sean alcanzables colocando la dirección de capa 2 de destino en el frame están dentro del dominio de broadcast.

Para almacenar las direcciones de capa 2 de los computadores de mi dominio de broadcast el computador usa la Tabla ARP



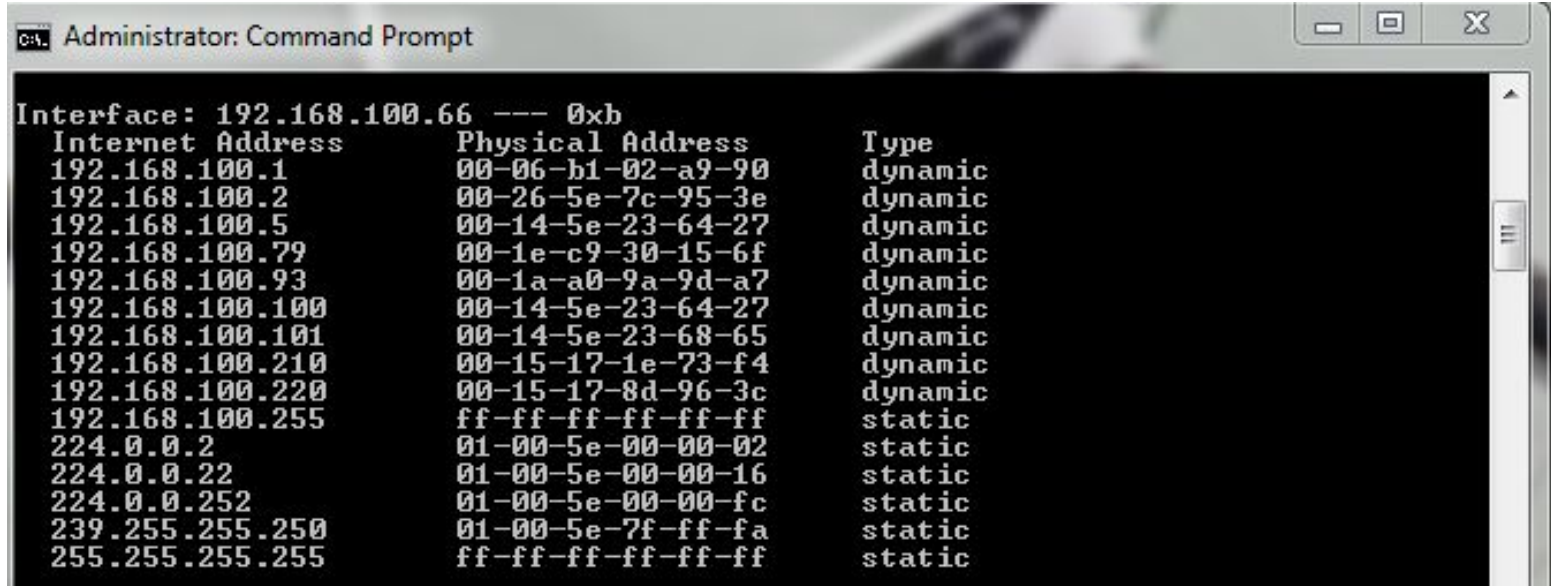
# Address Resolution Protocol (ARP)

Para completar la tabla ARP, cada computador utiliza el protocolo ARP (Address Resolution Protocol) para obtener a partir de una dirección IP (capa 3) su correspondiente dirección MAC (capa 2)

La Tabla ARP:

- Se puede llenar por monitoreo de tramas en el medio
- Se puede llenar por medio de una solicitud ARP
- Tabla contiene entradas uno a uno entre IP y MAC
- Entradas tienen un TTL o tiempo de vida, depende de SO

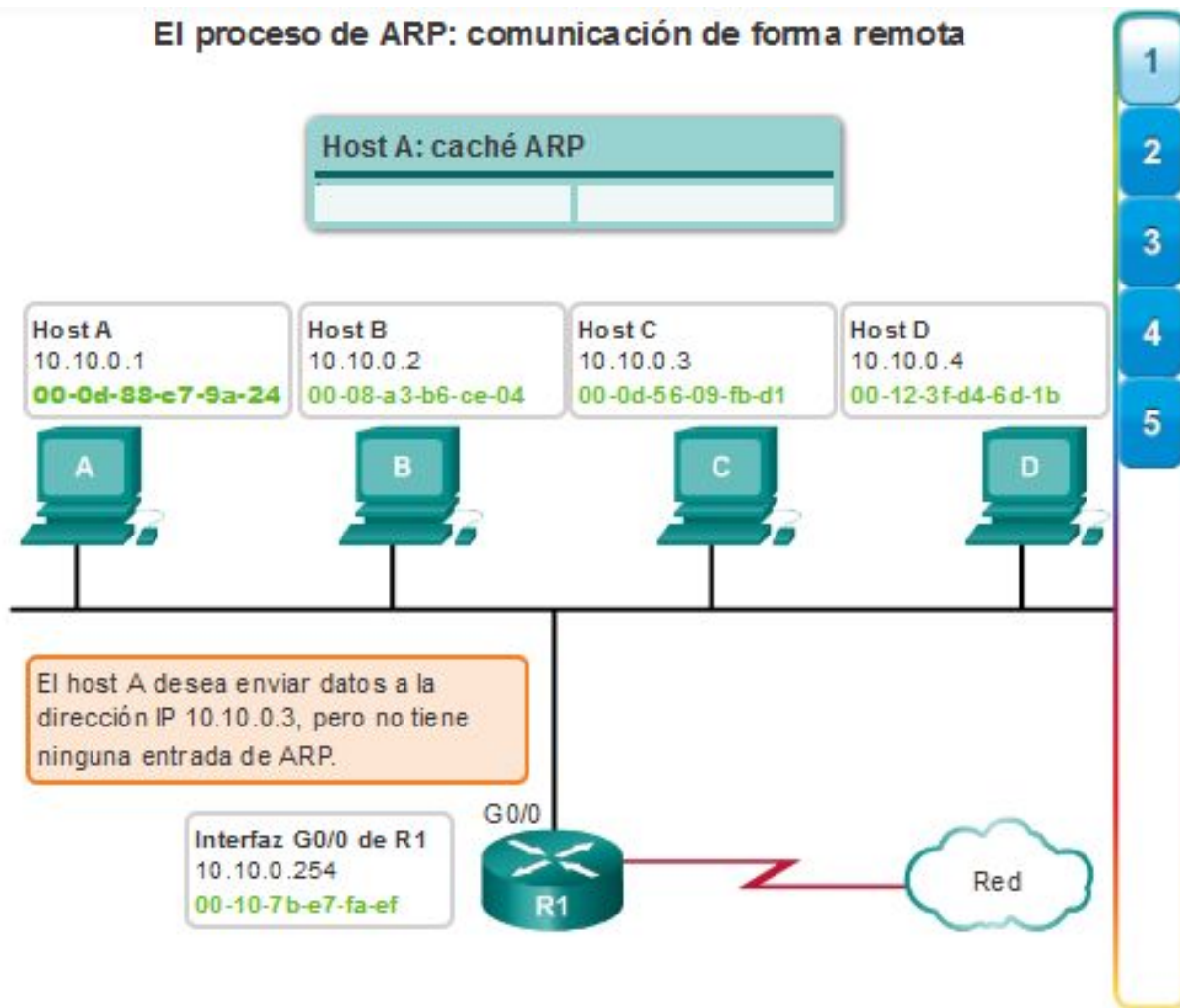
# Address Resolution Protocol (ARP)



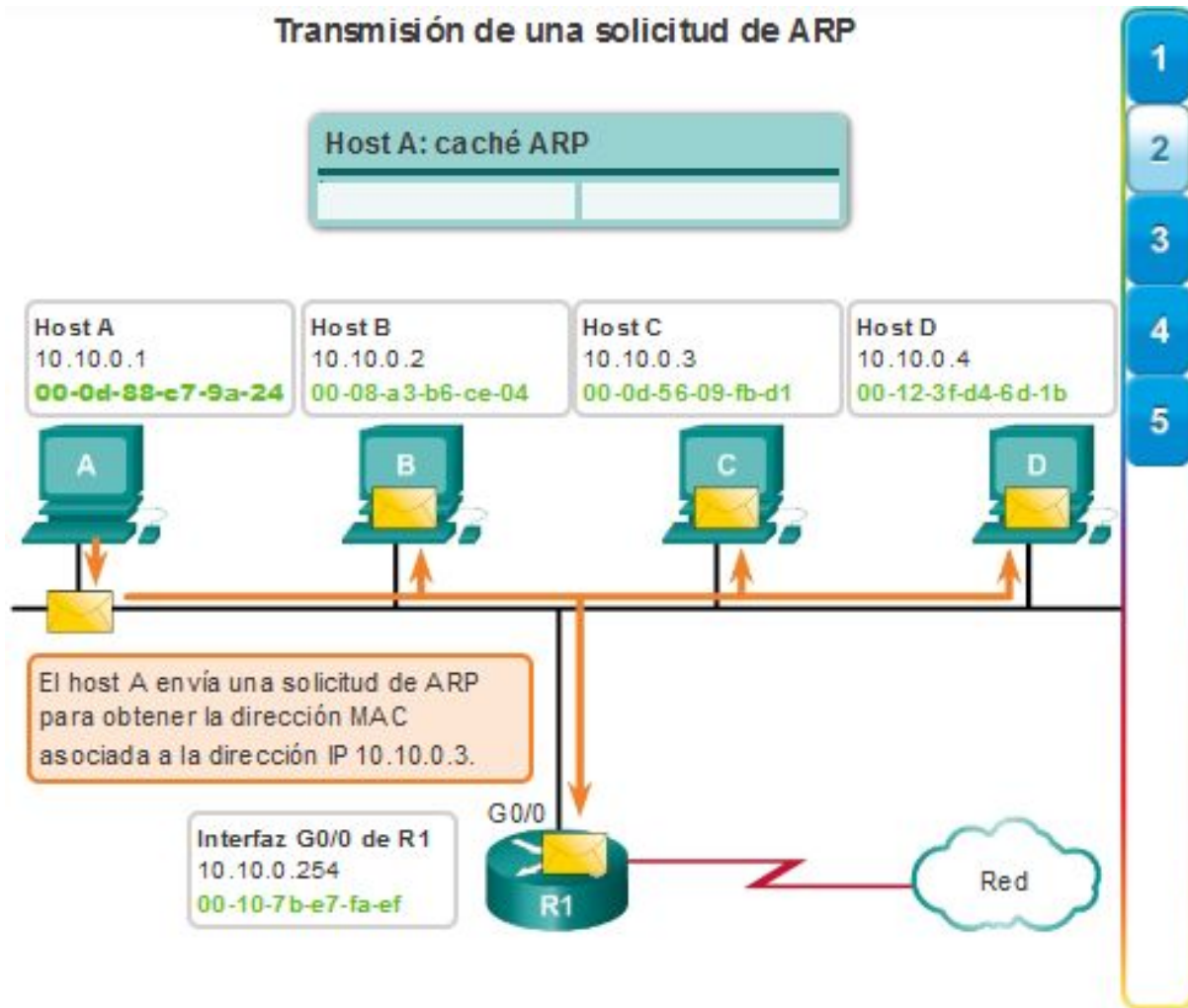
```
C:\> Administrator: Command Prompt

Interface: 192.168.100.66 --- 0xb
Internet Address      Physical Address      Type
192.168.100.1         00-06-b1-02-a9-90     dynamic
192.168.100.2         00-26-5e-7c-95-3e     dynamic
192.168.100.5         00-14-5e-23-64-27     dynamic
192.168.100.79        00-1e-c9-30-15-6f     dynamic
192.168.100.93        00-1a-a0-9a-9d-a7     dynamic
192.168.100.100       00-14-5e-23-64-27     dynamic
192.168.100.101       00-14-5e-23-68-65     dynamic
192.168.100.210       00-15-17-1e-73-f4     dynamic
192.168.100.220       00-15-17-8d-96-3c     dynamic
192.168.100.255       ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

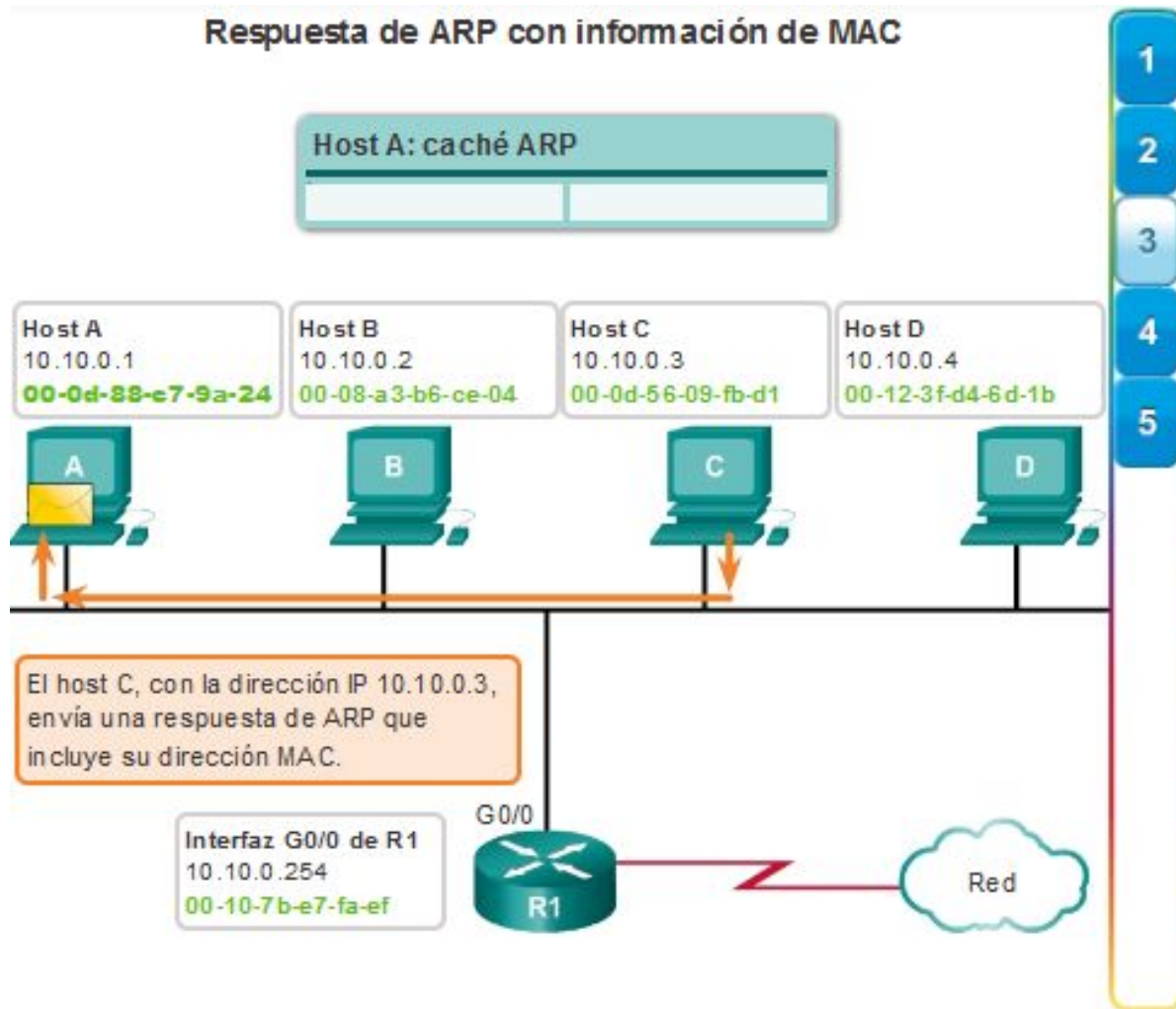
## El proceso de ARP: comunicación de forma remota



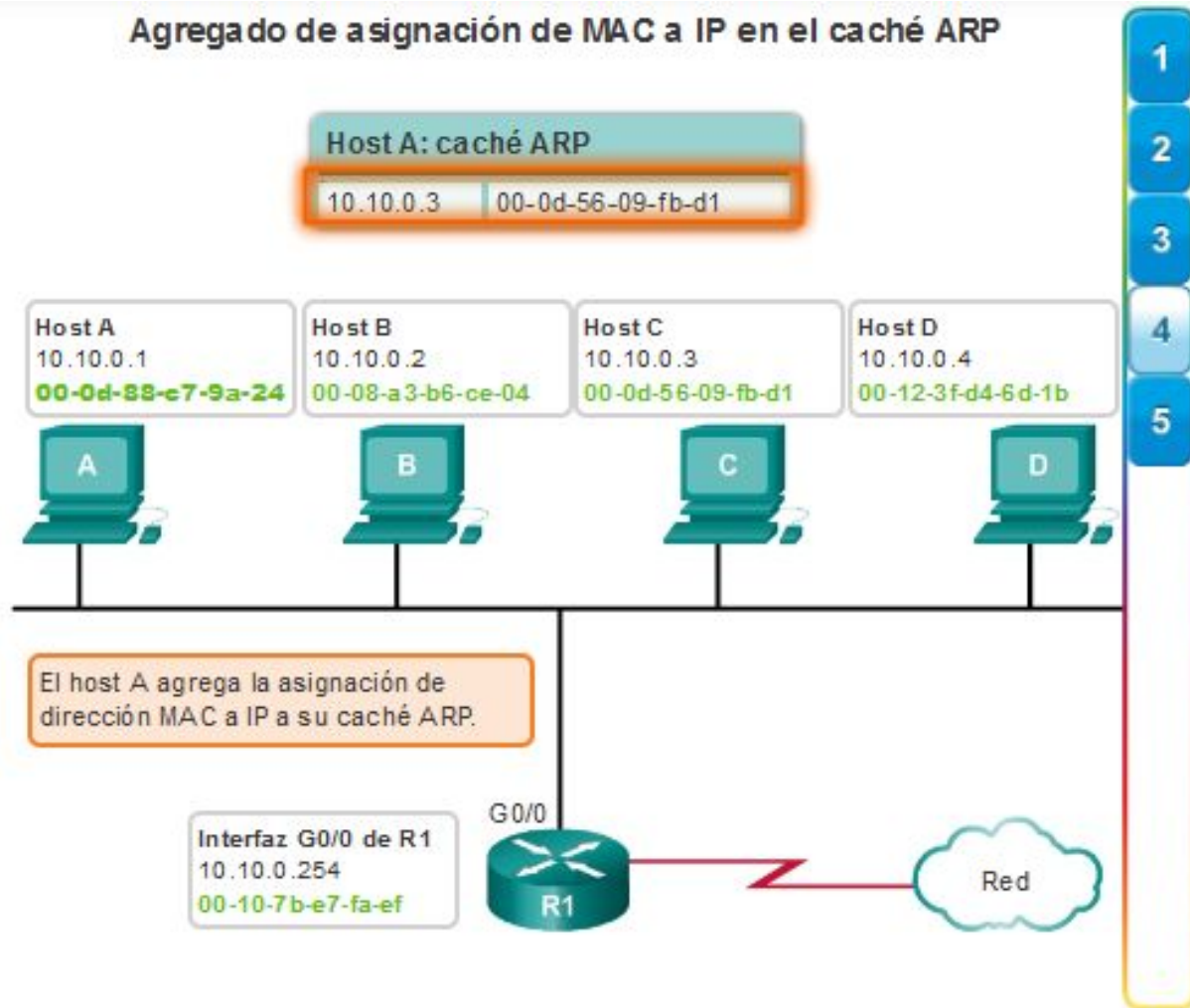
## Transmisión de una solicitud de ARP



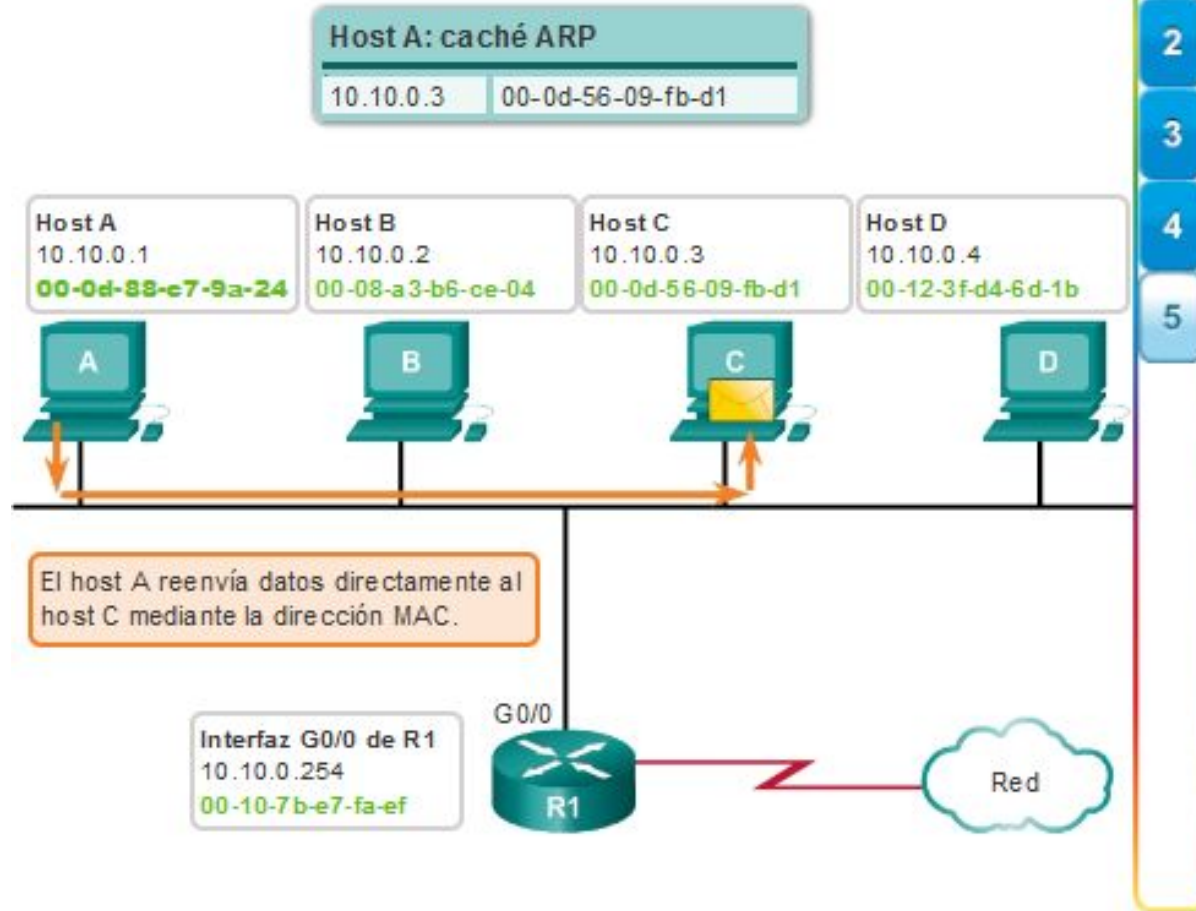
## Respuesta de ARP con información de MAC



## Agregado de asignación de MAC a IP en el caché ARP

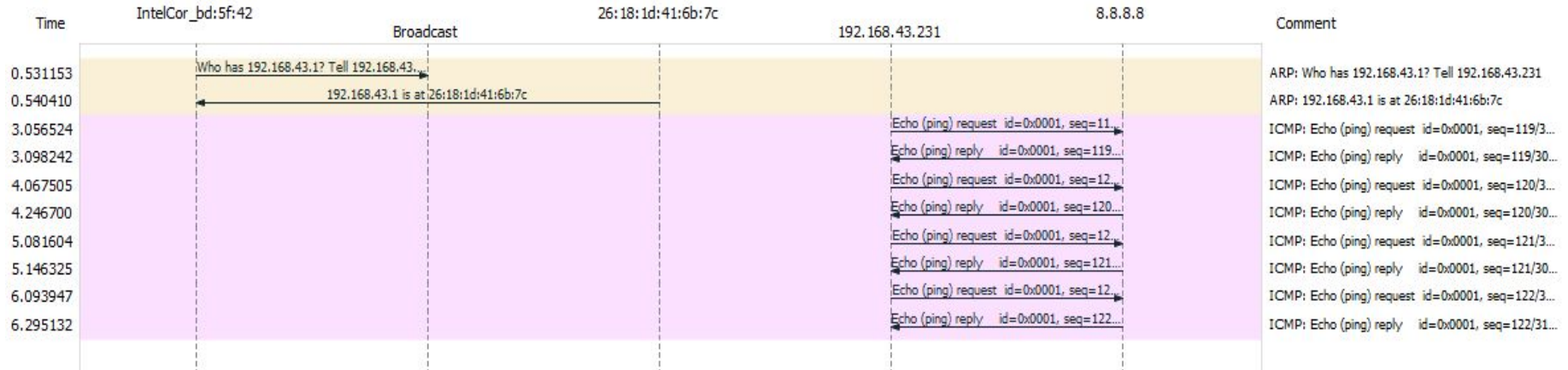
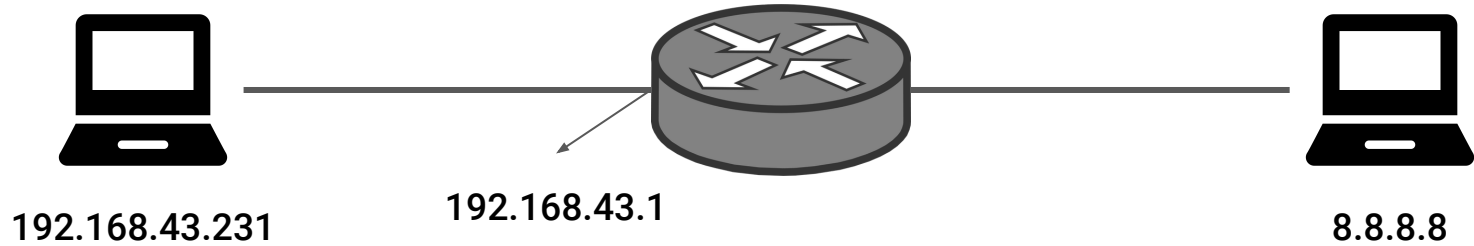


## Reenvío de datos con información de dirección MAC



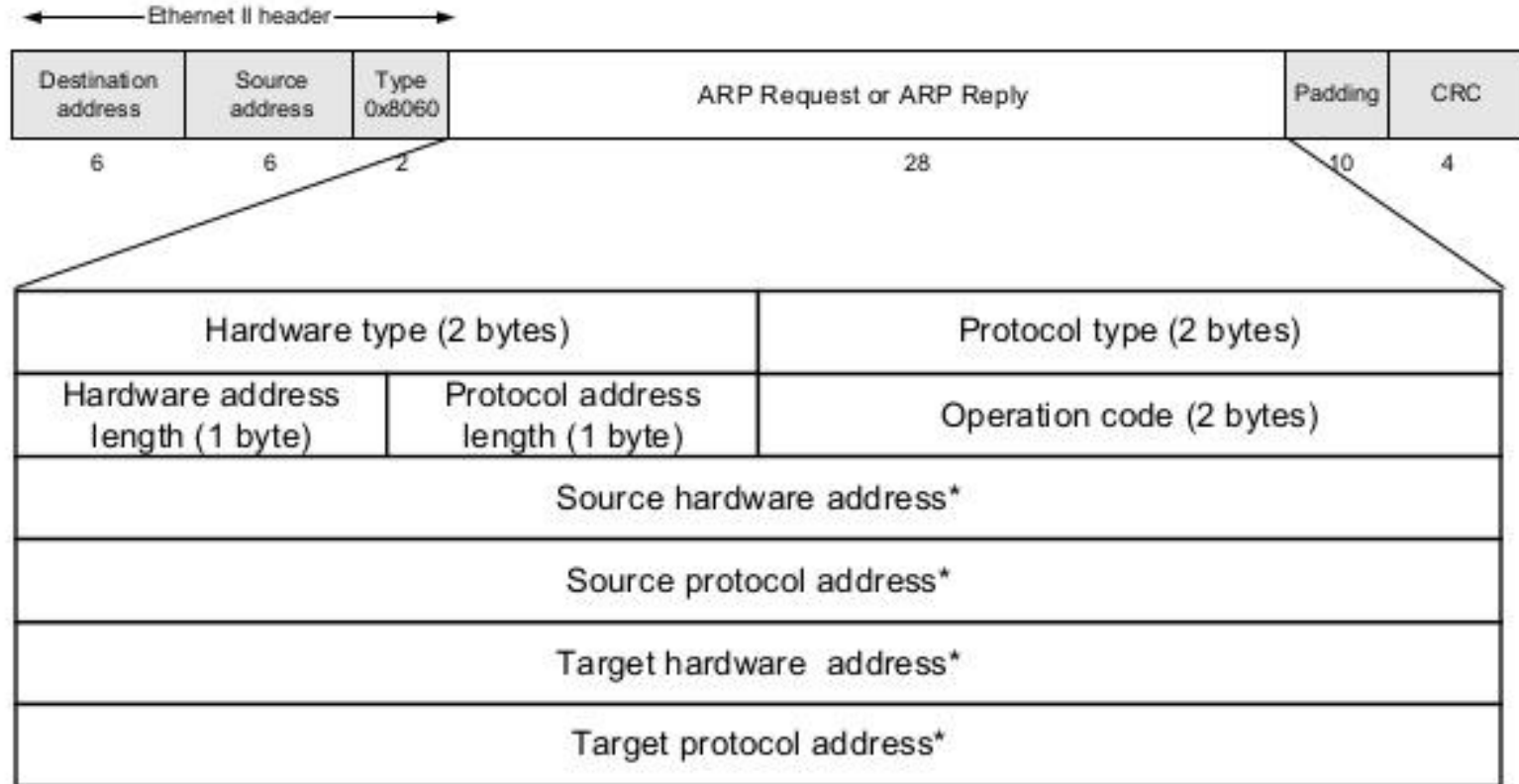


# Address Resolution Protocol (ARP)





# Address Resolution Protocol (ARP)



# Address Resolution Protocol (ARP)

- **Tipo de hardware o Hardware Type (HTYPE):** este campo especifica el tipo de protocolo de enlace. Ejemplo: Ethernet es 1.
- **Tipo de protocolo o Protocol Type (PTYPE):** este campo especifica el protocolo de interconexión de redes para las que se destina la petición ARP. Para IPv4, esto tiene el valor 0x0800.
- **Longitud Hardware (HLEN):** longitud (en octetos) de una dirección de hardware. En Ethernet el tamaño de direcciones es de 6.
- **Longitud del Protocolo (PLEN):** longitud (en octetos) de direcciones utilizadas en el protocolo de capa superior. El protocolo de capa superior especificado en PTYPE. IPv4 tamaño de la dirección es de 4.

# Address Resolution Protocol (ARP)

- **Operación:** especifica la operación que el emisor está realizando: 1 para la petición, 2 para la respuesta.
- **Dirección de hardware del remitente (SHA):** dirección de capa 2 del remitente.
- **Remitente dirección de protocolo (SPA):** dirección de capa 3 del remitente.
- **Dirección de hardware de destino (THA):** dirección de capa 2 del destino.  
Este campo se ignora en las solicitudes.
- **Dirección de protocolo target (TPA):** dirección de capa 3 del destino.