

Enlace de Datos



Problema de Asignación del Canal

- Redes
 - Punto a Punto: WANS
 - Broadcast: LANS
 - Broadcast => medio o canal compartido
 - conflictos
 - identificación
 - medio no siempre disponible
 - Capa 2 dividida: MAC y LLC

¿Cómo Resolver el Problema?

- Asignación estática
 - FDM
 - TDM
 - ▣No aplicables a redes broadcast
- Asignación dinámica
 - protocolos de contienda
 - generan los protocolos de acceso al medio que operan en la subcapa MAC

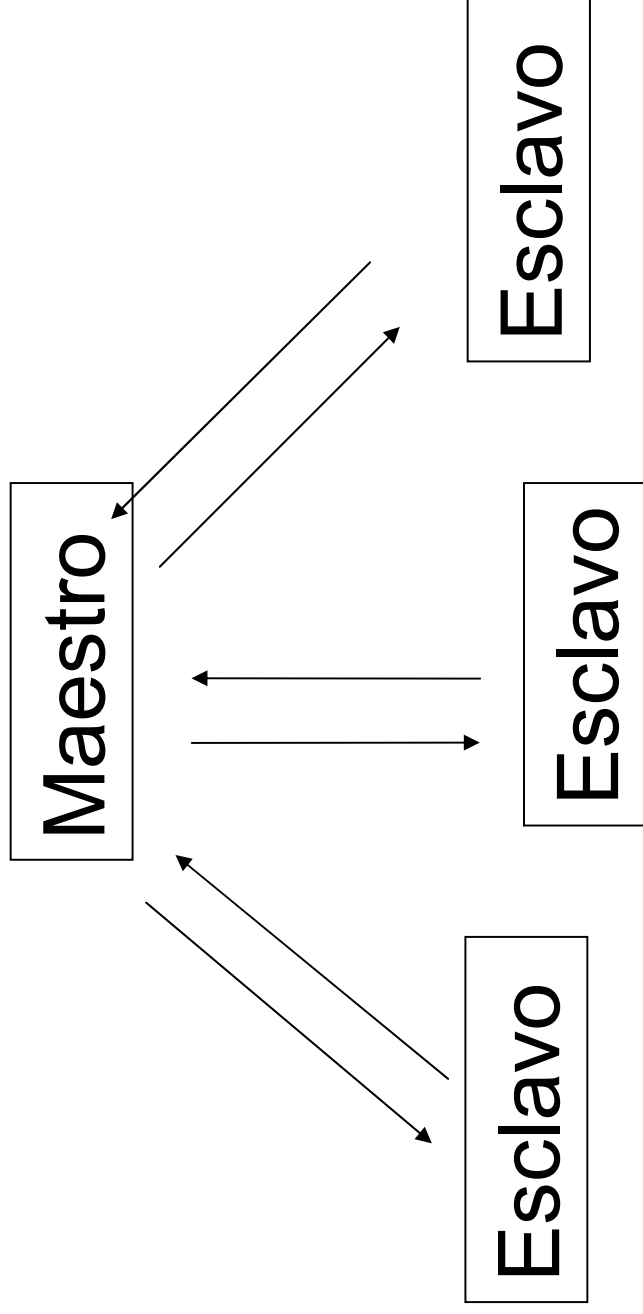
Tipos de Protocolos MAC

- Acceso múltiple sin detección de portadora
- Acceso múltiple con detección de portadora
- Libres de colisiones
- De contienda limitada
- Token Passing
- Inalámbricos

Acceso múltiple sin detección portadora

- Antecedentes
- 1970: Abramson crea Alohanet (Hawaii)
- Topología Maestro (1) Esclavo (3)
- Dos canales: descendente y ascendente
- Canales en la banda UHF:
 - Anchura: 100 KHz
 - Capacidad: 9.6 Kbps

Funcionamiento de Alohanet

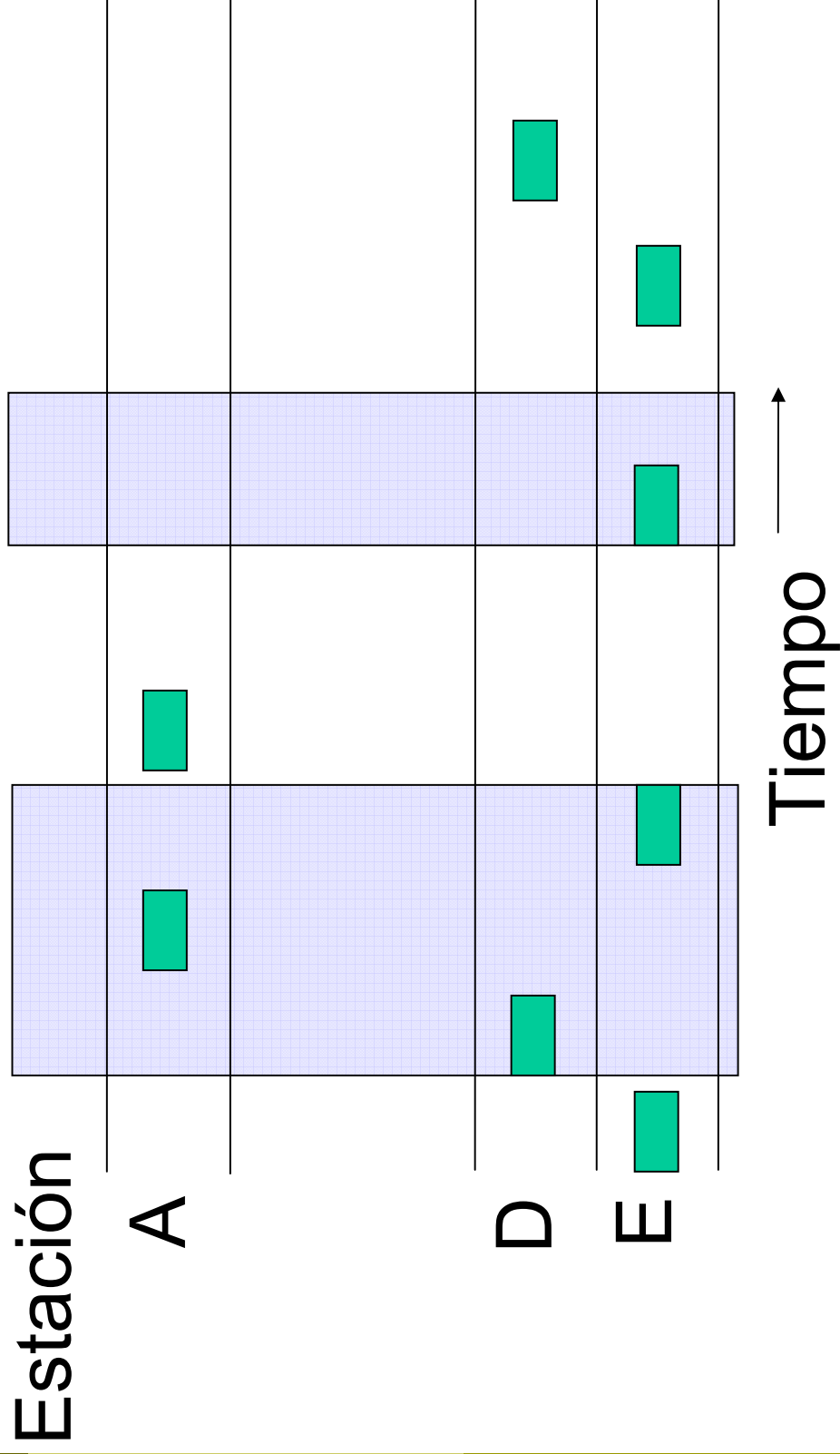


- Canal descendente: sin problemas
- Canal ascendente: si dos esclavos transmiten se crea un colisión
- Requiere protocolo MAC

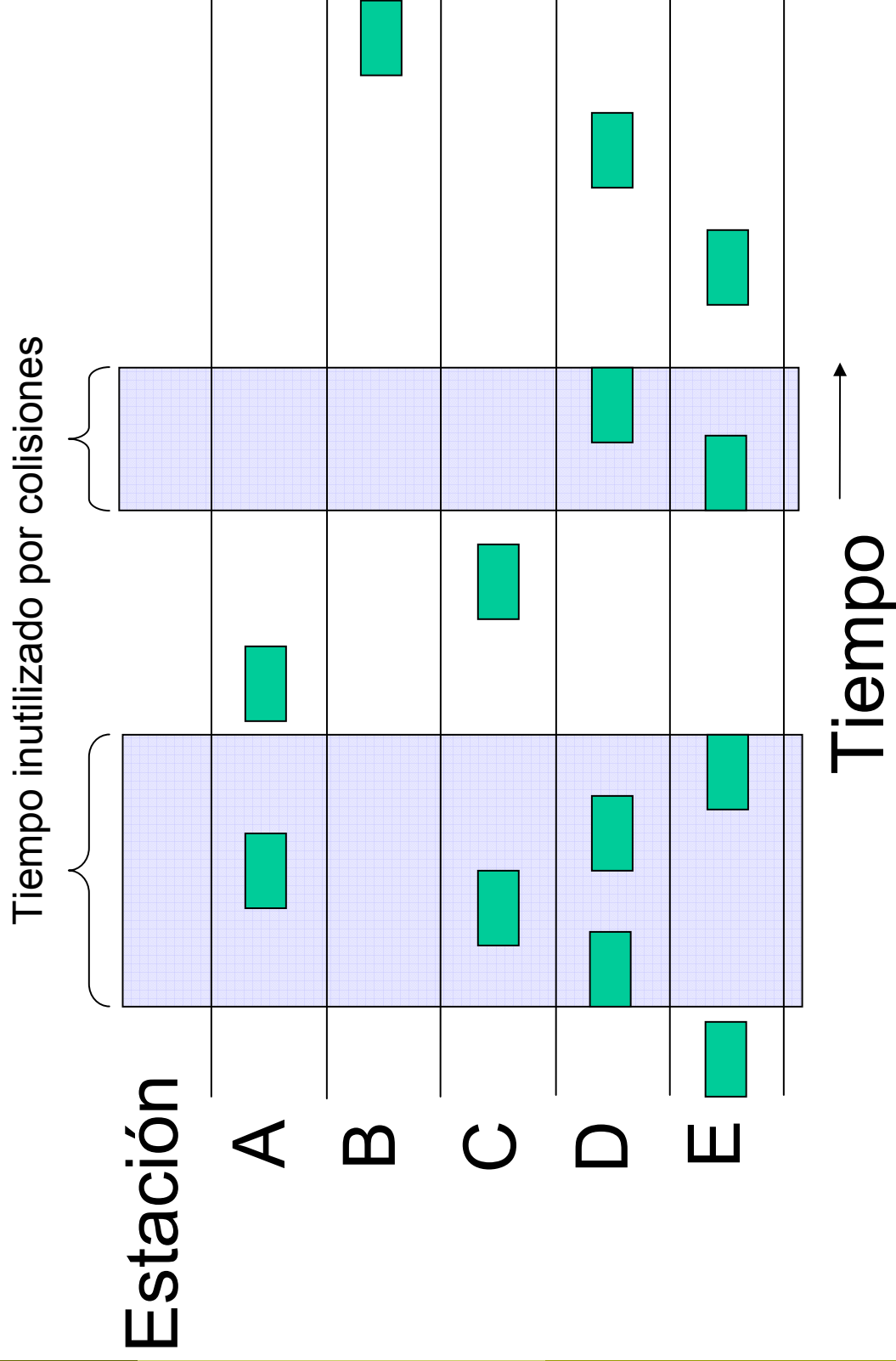
Protocolo MAC Aloha

- Funcionamiento básico:
Estación transmite frame y espera ACK; si esto no se produce dentro del timeout) se retransmite el frame.
- Solapamiento de un bit entre dos nodos produce un conflicto de **transmisión**.
- A este conflicto se le llama **colisión**.
- En Aloha los tiempos de transmisión son aleatorios.

Emisión de frames en ALOHA puro



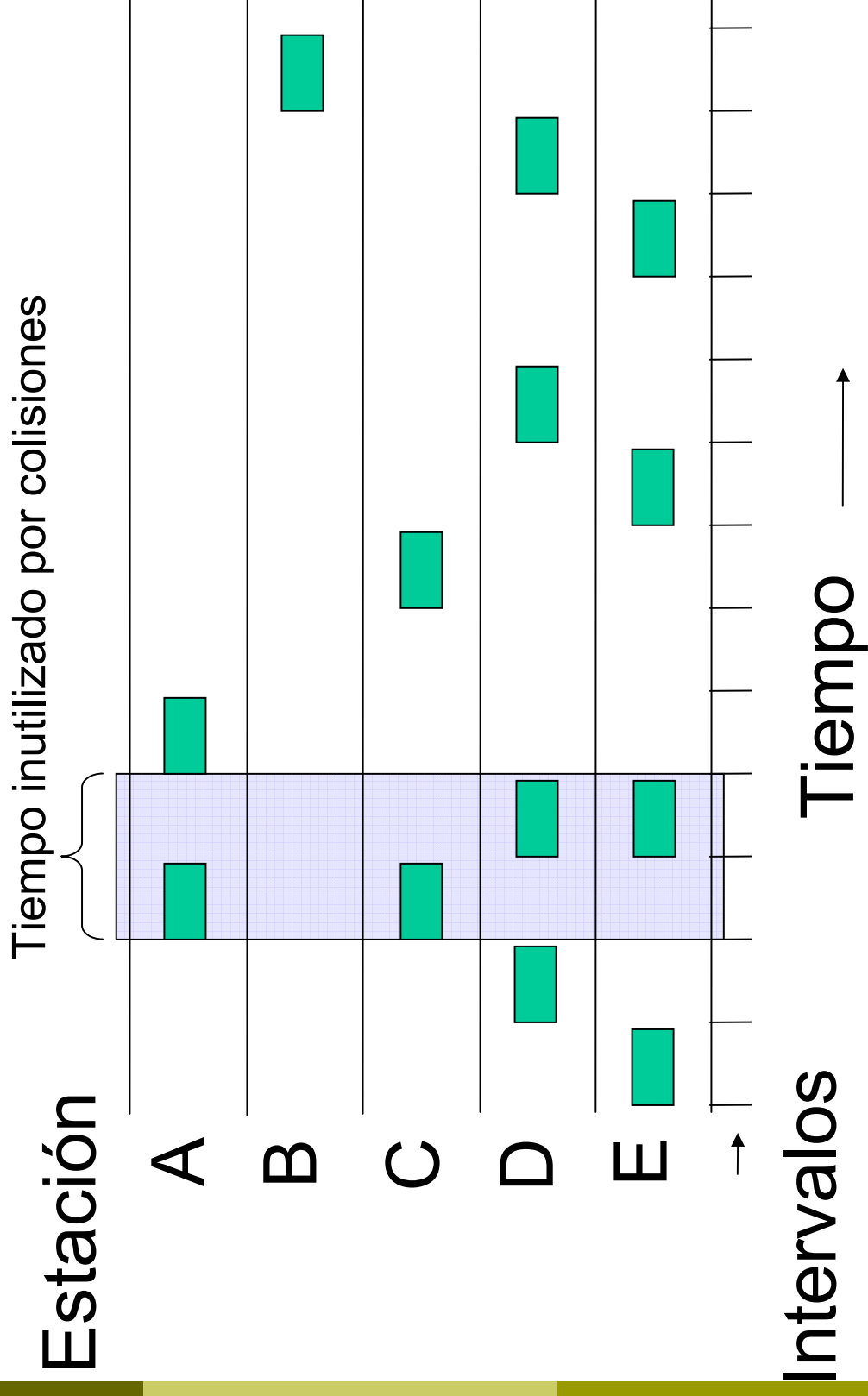
Emisión de frames en ALOHA puro



Slotted Aloha

- Funcionamiento básico:
Estación transmite frame y espera ACK; si esto no se produce dentro del timeout) se retransmite el frame.
- En Slotted Aloha los intervalos de inicio de transmisión son múltiplos de un frame.
- Requiere sincronización entre todos los nodos

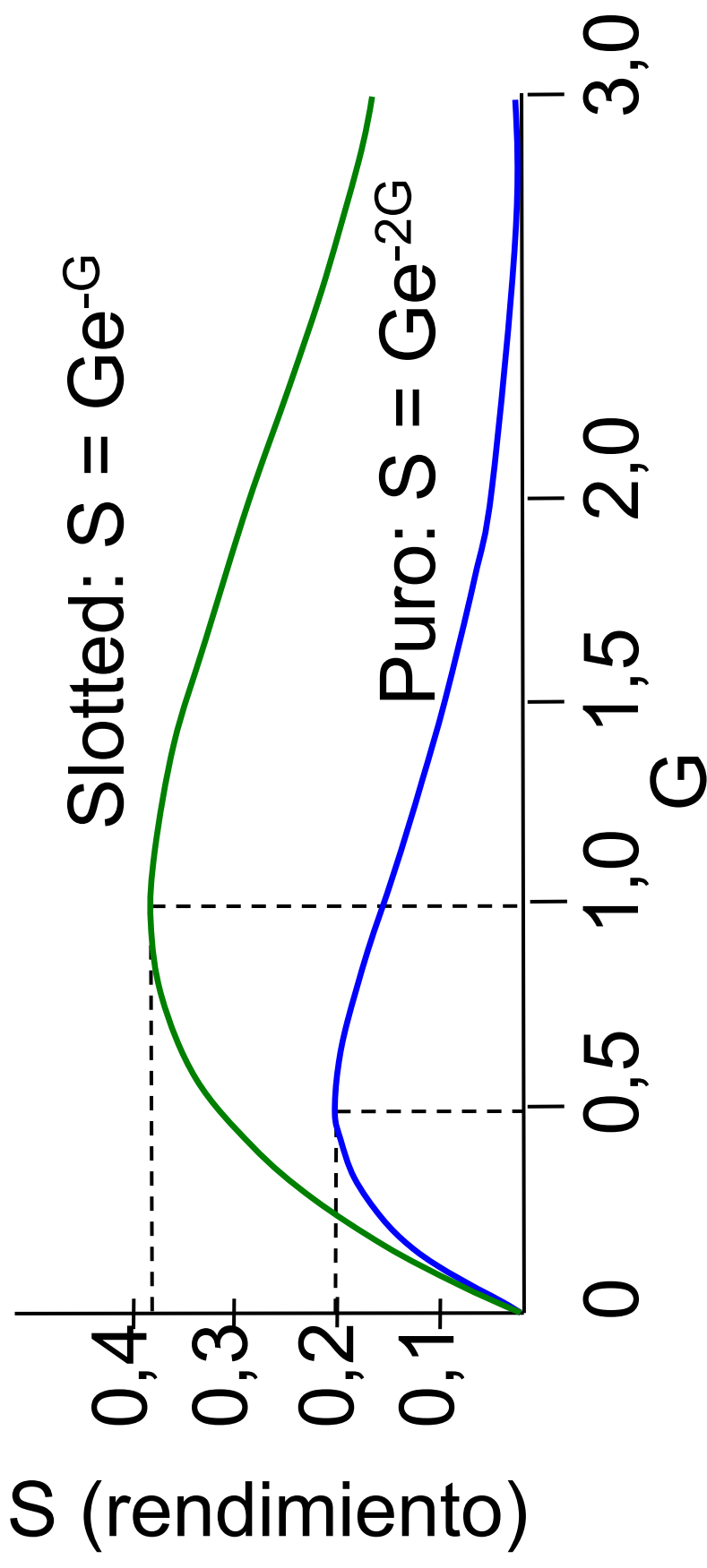
Emisión de frames en Slotted ALOHA



Rendimiento de Aloha

- Suponiendo distribución de Poisson:
 - Aloha puro: max. 18,4% al 50% de utilización
 - Aloha ranurado: 36,8% al 100% de utilización
- Pero el tráfico es auto-similar o fractal
=> en la práctica: imás rendimiento!
- Slotted Aloha es usado actualmente en redes GSM y comunicaciones vía satélite.

Rendimiento de Aloha y Slotted Aloha

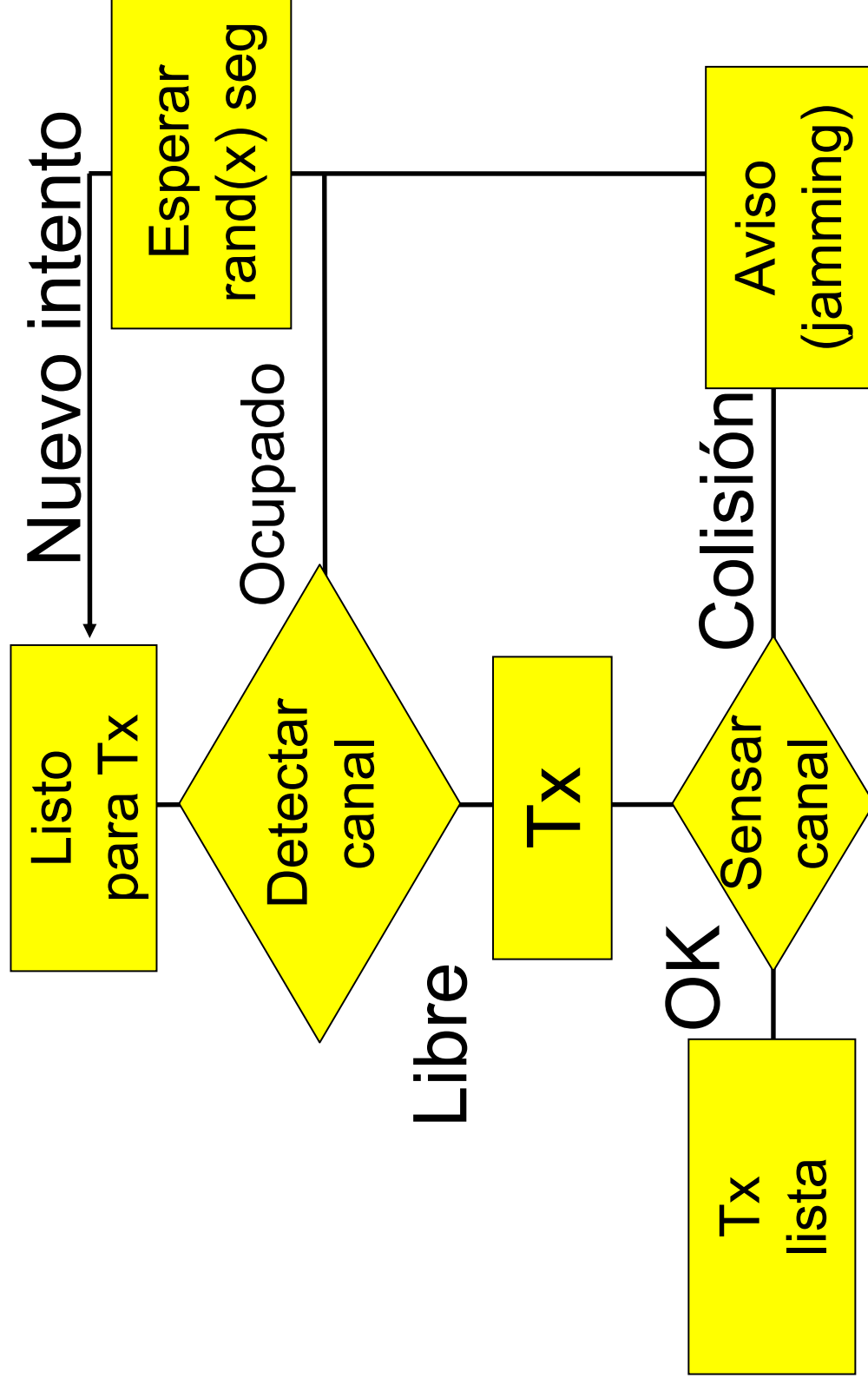


(densidad de tráfico
inyectado en la red)

Carrier Sense Multiple Access con Detección Colisión

- Funcionamiento básico:
Estación sensa el canal, si está libre transmite frame; caso contrario se espera un tiempo aleatorio y se vuelve a sensar repitiendo el algoritmo. Una vez transmitido el frame se sensa el canal para detectar colisiones. En caso de existir una, se avisa con una señal
- ¡Ahora existe seguridad si hubo colisiones!

CSMA/CD



CSMA/CD

- Una colisión se producirá si dos o más nodos Tx al mismo tiempo o separados un instante de tiempo tal que la señal Tx no haya llegado al otro nodo (Período de Contienda)
- Los estados de una red CSMA/CD son entonces: libre, transmisión y colisión

Protocolos Libres de Colisión

- Antecedentes
- Las colisiones reducen el desempeño de la red
- A medida que aumenta el tráfico aumentan las colisiones (¿qué pasa con poco tráfico?)
- Solución:
- Eliminar las colisiones
- Con esto se obtendrá un mayor desempeño a alto tráfico

Protocolos Libres de Colisión

- ❑ Protocolo Bit Map
- ❑ Protocolo de Cuenta Regresiva

Protocolos de Contención Limitada

- Antecedentes
- Las colisiones reducen el desempeño de la red en alto tráfico
- Eliminar colisiones introduce latencia en una red con bajo tráfico
- Solución:
- Llegar a un esquema híbrido y dinámico entre ambos casos

Protocolos de Contención Limitada - II

- Si la red tiene poco tráfico, comportarse como protocolos con colisiones
- Si la red tiene alto tráfico, comportarse como protocolos sin colisiones
- Solución práctica:
- Identificar el nodo o grupo de nodos que generan gran tráfico y a ellos otorgarle intervalos propios de transmisión

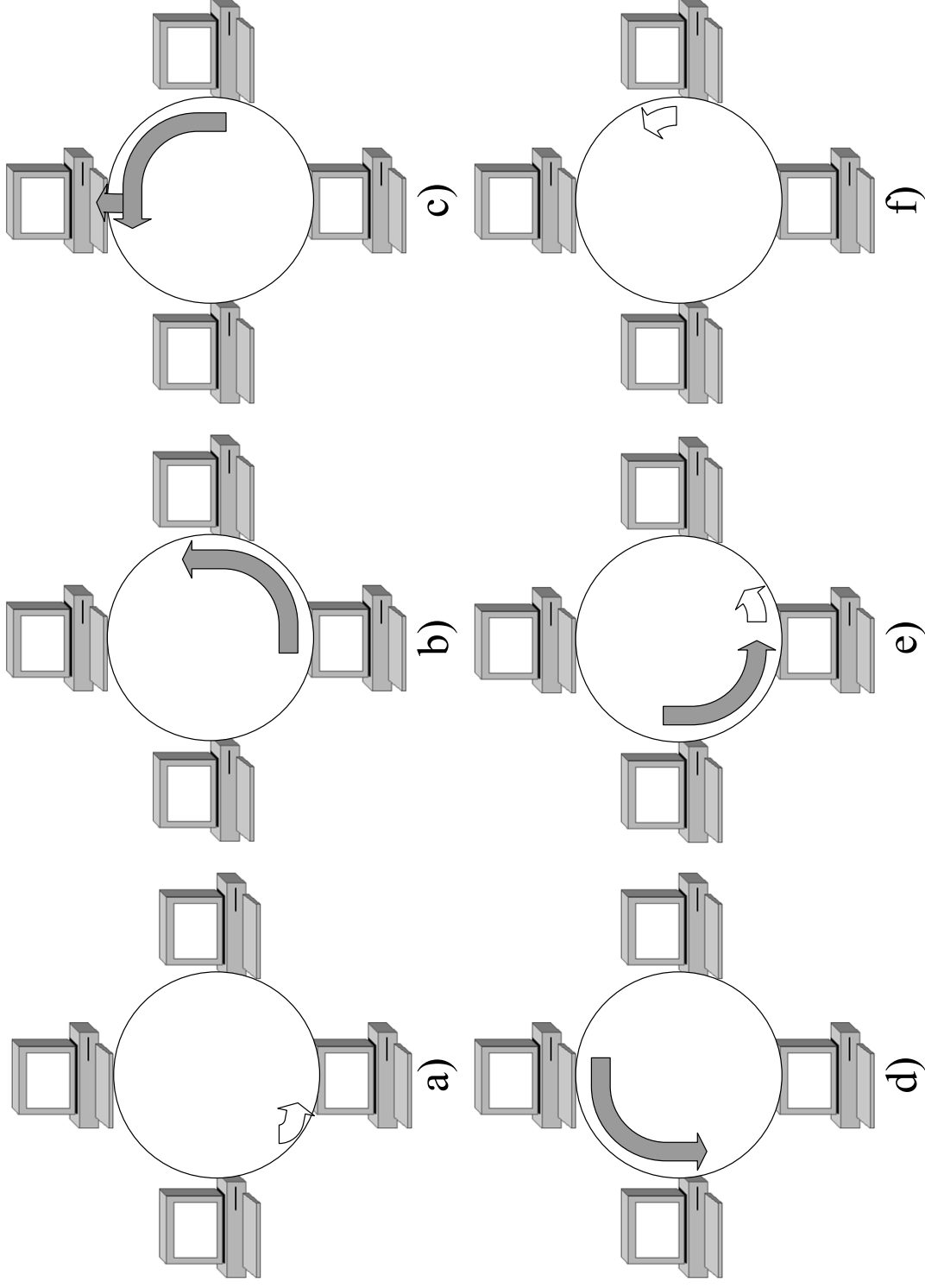
Protocolos Token Passing

- Antecedentes
- Los protocolos anteriores son no deterministas
- En redes de control de procesos se requiere tener una garantía de tiempo máximo de retardo
- Solución:
- Otorgar el medio a los nodos un tiempo máximo y luego reasignarlo.

Protocolos Token Passing

- Funcionamiento básico:
Por la red siempre circula un token. Si un nodo desea Tx debe esperar hasta recibir el token, entonces se apodera de él y Tx frames hasta un cierto tiempo máximo, para luego liberar el token a la red.
- Control de acceso flexible, eficiente y equitativo a carga elevada.
- Permite generar prioridades y BW garantizados

Operación Token Passing



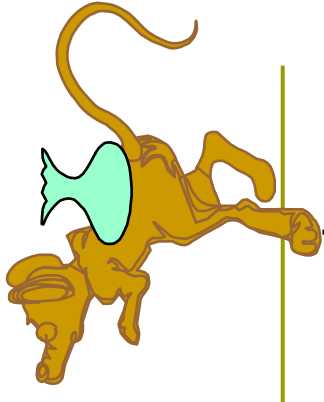
Protocolos Token Passing

- Token holding time: máximo período de tiempo en el que un nodo puede transmitir
- Este protocolo no produce colisiones
- ¿qué sucede si se pierde el token?
- ¿qué sucede si se corta el anillo?
- ¿el anillo debe ser físico, lógico o ambos?

Capa de Enlace en IEEE 802

| |
|--------------|
| Aplicación |
| Presentación |
| Sesión |
| Transporte |
| Red |
| Enlace |
| Física |

| |
|-----------------------------------|
| Aplicación |
| Presentación |
| Sesión |
| Transporte |
| Red |
| LLC: 802.2 |
| MAC: 802.3, 802.4, 802.5, etc. |
| Física |



La capa de enlace

- ❑ La principal función de la capa de enlace es comprobar que los datos enviados están libres de error. Para ello se utiliza el CRC (Cyclic Redundancy Check)
- ❑ Cuando se detecta un error se pueden hacer tres cosas:
 - Intentar corregirlo (no es posible con el CRC)
 - Descartar el paquete erróneo y pedir reenvío
 - Descartar el paquete erróneo y no decir nada
- ❑ En todos los casos habituales se procede de la tercera forma (se descarta y no se dice nada). Será normalmente la capa de transporte (en el host de destino) la que se encargue de solicitar la retransmisión de los datos al emisor. Pero no siempre es así, hay protocolos que no reenvían.

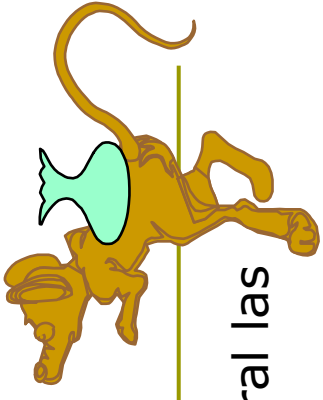
Capa de enlace: tipos de enlaces

- Un enlace puede ser:
 - **Simplex**: transmisión en un solo sentido. Ej.: emisión de TV
 - **Semi-dúplex o half-duplex**: transmisión en ambos sentidos, pero no a la vez. Ej.: walkie-talkies, redes WiFi (inalámbricas)
 - **Dúplex o full-duplex**: transmisión simultánea en ambos sentidos. Ej.: conversación telefónica. Ethernet, ADSL
- En el caso dúplex y semi-dúplex el enlace puede ser:
 - **Simétrico** (misma velocidad ambos sentidos). Ej.: Ethernet
 - **Asimétrico** (diferente velocidad). Ej: ADSL

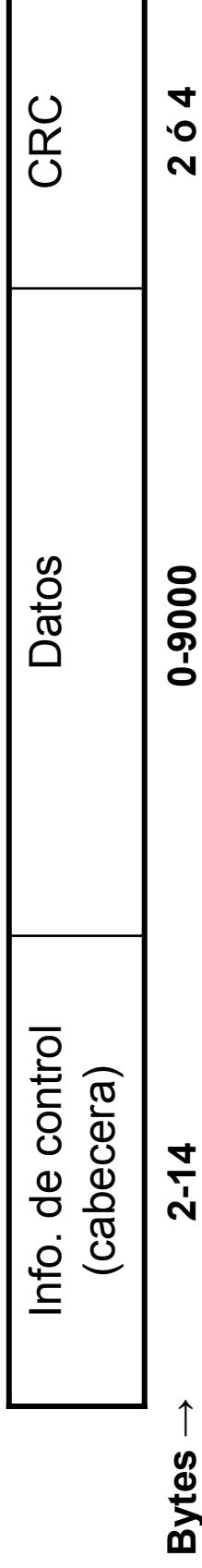
Velocidad de un enlace

- La velocidad se especifica en bits por segundo (no bytes!) usando los prefijos métricos: bps, Kbps, Mbps, Gbps, Tbps, ... pero OJO, con el significado métrico (1000), no informático (1024):
 - **1 Kbps = 1.000 bps (no 1.024 bps)**
 - **1 Mbps = 1.000.000 bps (no 1.024*1.024 bps)**
- Ej.: conexión ADSL 320/1024 Kbps (asc./desc.):
 - Envía: 320.000 bits/s = 40.000 Bytes/s = 39,1 KBytes/s
 - Recibe: 1.024.000 bits/s = 128.000 Bytes/s = 125 Kbytes/s

Capa de enlace: las tramas



- ❑ La capa de enlace transmite tramas. De forma general las tramas suelen tener la estructura siguiente:



- ❑ ¿Como sabe el receptor cuando termina una trama?
 - Porque el emisor ha dejado de enviar datos. Ej.: LANs
 - Porque la longitud va escrita en la cabecera. Ej.: Ethernet
 - Porque aparece un delimitador de fin de trama que nunca aparece en los datos (01111110 con bit stuffing). Ej.: HDLC, PPP, Frame Relay, etc.
 - Porque las tramas tienen una longitud constante. Ej.: ATM

Subcapa MAC

Estandarización 802.3

- ❑ 1983: 802.3 aprueba CSMA/CD con una modificación respecto a Ethernet DIX:

Campo **Ethertype** reemplazado por **longitud**

- ❑ Xerox desplaza campo Ethertype a valores >1536 para que pueda coexistir DIX con 802.3
- ❑ En 802.3 el tipo es especificado en LLC
- ❑ Por lo tanto, iexisten dos especificaciones!

Frames Ethernet/802.3 (1, 10 y 100 Mbps)

| | | | | | | | |
|-----------|-------------|-----------------|----------------|------|----------|---------|-----|
| 7 B | 1 B | 6 B | 6 B | 2 B | 0-1500 B | 0-46 B | 4 B |
| Preámbulo | S O F | Dir. Destino | Dir. Fuente | Tipo | Datos | Relleno | CRC |

Ethernet

| | | | | | | |
|-----------|-----------------|----------------|-------|----------|---------|-----|
| 8 B | 6 B | 6 B | 2 B | 0-1500 B | 0-46 B | 4 B |
| Preámbulo | Dir. Destino | Dir. Fuente | Largo | Datos | Relleno | CRC |

802.3

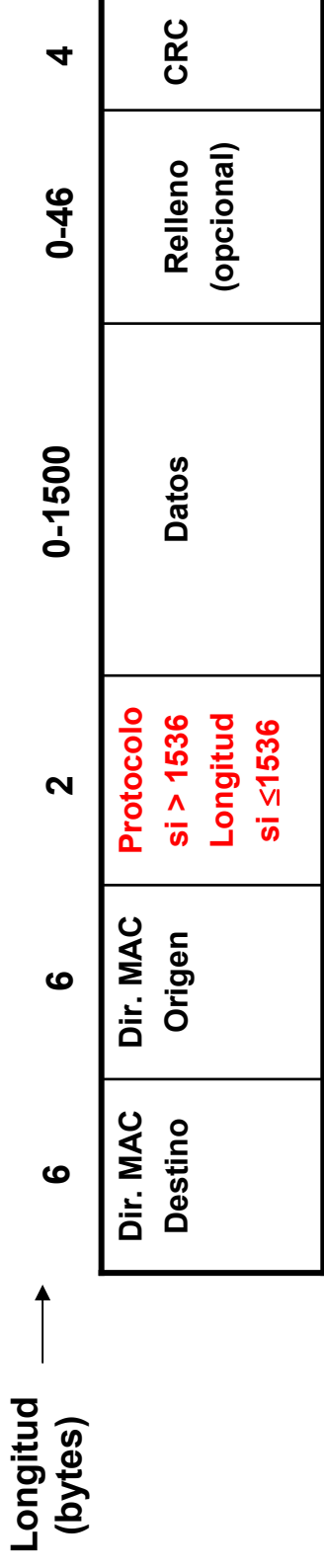
- Tipo especifica protocolo nivel 3
- Largo especifica el largo del campo datos

Frames Ethernet/802.3

| Especificación | Formato DIX | Formato 802.3 |
|-----------------------------|---|-------------------------------------|
| Protocolo de red | Campo Tipo en frame MAC | Campo DSAP/SSAP en encabezado 802.2 |
| Longitud si ≥ 64 bytes | Implícita por longitud del frame | Explícita en campo longitud |
| Longitud si < 64 bytes | En campo longitud de paquete (nivel de red) | Explícita en campo longitud |

Estructura de la Trama Ethernet

- ❑ La detección de colisiones de Ethernet requiere que las tramas tengan una longitud mínima de 64 bytes.
- ❑ La longitud máxima es de 1518 bytes (1500 bytes de datos una vez descontada la cabecera y el CRC)



El relleno solo está cuando es preciso para llegar al mínimo de 64 bytes

Diferencias Ethernet II/IEEE 802.3

- IEEE 802.3 introdujo una modificación respecto a DIX: el campo *protocolo* fue reemplazado por *longitud*
- Por compatibilidad Xerox desplazó el campo protocolo a valores por encima de 1536 para que DIX pudiera coexistir con IEEE 802.3
- En 802.3 el protocolo de red se especifica en un nuevo encabezado LLC (802.2) en la parte de datos.

Formatos DIX y 802.3

- En 1997 el IEEE aprobó el doble significado (tipo/longitud) siguiendo el uso habitual de distinguir según el valor del Etherbyte. La asignación de Ethertypes pasó entonces de Xerox a IEEE
- DIX: TCP/IP, DECNET Fase IV, LAT (Local Area Transport), IPX
- 802.3/LLC: Appletalk Fase 2, NetBIOS, IPX

LLC (Logical Link Control 802.2)

- Interfaz entre nivel de red y el subnivel MAC.
- Tres tipos de servicio:
 - LLC Tipo 1: Datagramas sin acuse de recibo (como PPP pero sin comprobar CRC).
 - LLC Tipo 2: Servicio CONS con ACK y numeración.
 - LLC Tipo 3: datagramas con ACK y numeración.

LLC

- Dada la elevada confiabilidad de las LANs se usa LLC Tipo 1
- Si existen errores/problemas (colisiones excesivas o no detectadas) el rendimiento decae con rapidez.
- Ethernet II la subcapa LLC no existe.
- En IEEE 802.3 y otras LANs (Token Ring, FDDI, etc.) la subcapa LLC da el soporte multiprotocolo.

Frame LLC SAP

| 1 B | 1 B | 1-2 B | Variable |
|------|------|-------------|----------|
| DSAP | SSAP | Control LLC | Datos |

- DSAP: Destination Service Access Point
- SSAP: Source Service Access Point
- En DSAP y SSAP los dos primeros bits tienen el significado Individual/Grupo y Local/Global. Esto deja solo 6 bits para el protocolo (64 posibilidades).

Frame LLC SNAP SAP

| 1 B | 1 B | 1 B | 3 B | 2 B | Variable |
|------|------|----------------|-----|------|----------|
| DSAP | SSAP | Control LLC | OUI | Tipo | Datos |

- **OUI: Organizationally Unique Identifier.**
Un prefijo que identifica el fabricante del protocolo (coincide con el de las direcciones MAC).
- **Tipo: el protocolo para un OUI dado**
- **Si el OUI es X 000000 el significado de Tipo es Ethernet**

Comparación de Ethernet DIX y 802.2/LLC

DIX

| | | | | |
|------------|------------|------------|------------------------|--|
| 6 | 6 | 2 | 46-1500 | |
| Dir. Dest. | Dir. Orig. | Ether-type | Paquete a nivel de red | |

Encabezado MAC

802.2/LLC

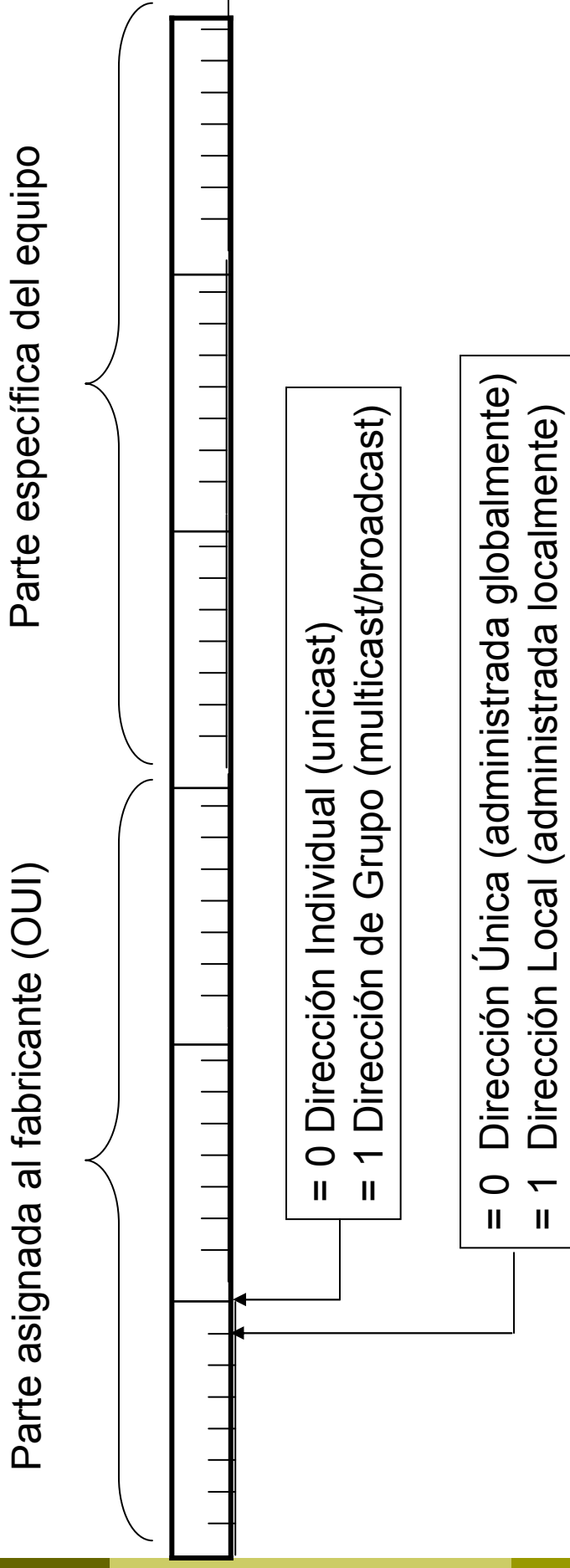
| | | | | | | | | | |
|------------|------------|----------|------|------|------|----------|---|------------|------------------------|
| 6 | 6 | 2 | 1 | 1 | 1 | 1 | 3 | 2 | 38-1492 |
| Dir. Dest. | Dir. Orig. | Longitud | 'AA' | 'AA' | '03' | '000000' | X | Ether-type | Paquete a nivel de red |

Encabezado MAC

Encabezado LLC

Para protocolo IP Ethertype = 0800h

Direcciones MAC



Las direcciones se expresan en hexadecimal. Ej.: 0030.A43C.0CF1

Los OUIs (Organizationally Unique Identifier) los asigna el IEEE a cada fabricante (un OUI cuesta US\$ 1250)

Tipos de Direcciones IEEE de 48 bits

Broadcast

| | | |
|---|---|-------------------------------|
| 1 | 1 | 111111111111...11111111111111 |
|---|---|-------------------------------|

Multicast Local

| | | |
|---|---|---------------------------------|
| 1 | 1 | Grupo Multicast local (46 bits) |
|---|---|---------------------------------|

Multicast Global

| | | | |
|---|---|------------|------------------------|
| 1 | 0 | Fab (22 b) | Grupo Multicast (24 b) |
|---|---|------------|------------------------|

Unicast Local

| | | |
|---|---|---------------------------|
| 0 | 1 | Dirección local (46 bits) |
|---|---|---------------------------|

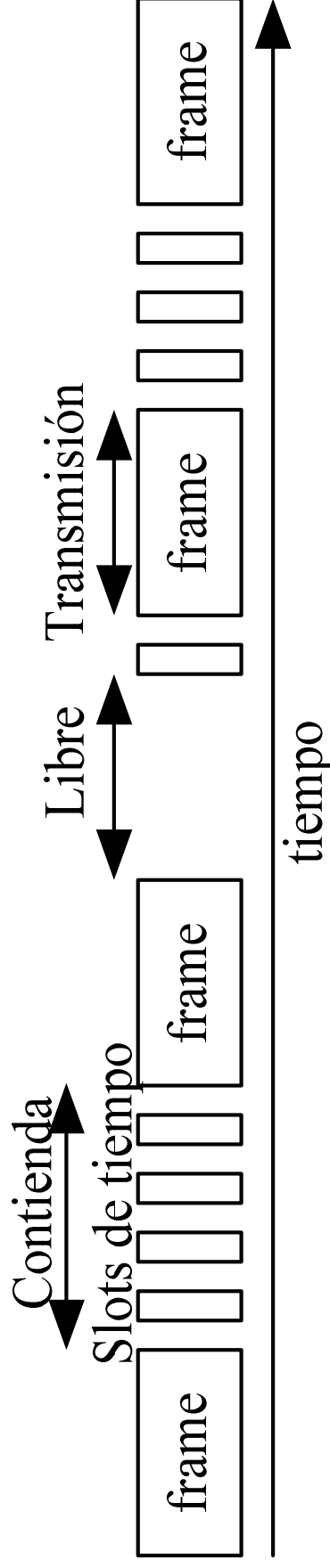
Unicast Global

| | | | |
|---|---|------------|------------------|
| 0 | 0 | Fab (22 b) | Dir. Nodo (24 b) |
|---|---|------------|------------------|

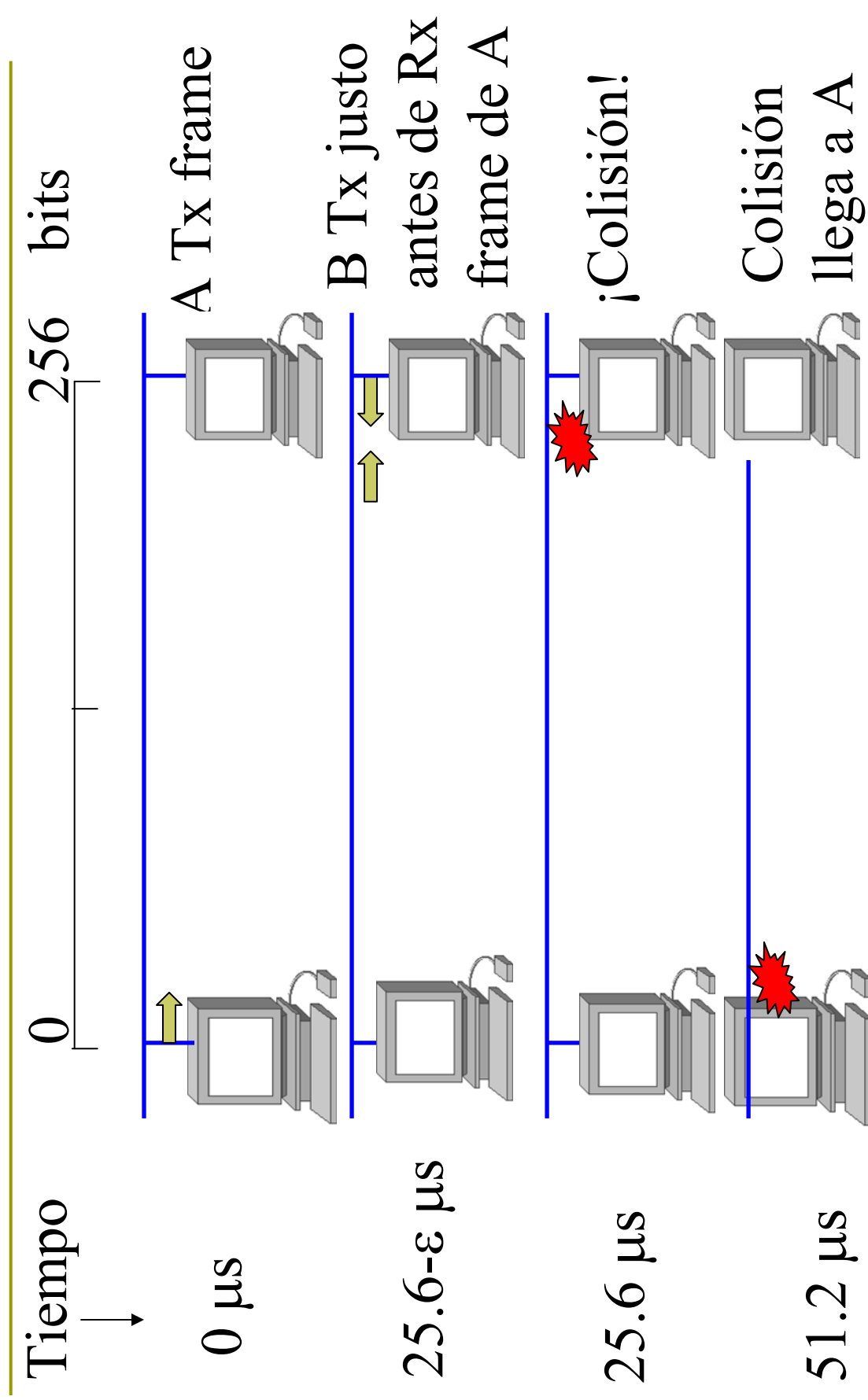
Funcionamiento de Ethernet/802.3

Una red Ethernet tiene tres estados:

- **Red libre:** no hay transmisión
- **Red en contienda:** existe riesgo de colisión
(sólo ocurre los primeros 51.2 μ s de Tx)
- **Red en Transmisión:** no existe riesgo de colisión



Cronología de una colisión a 10 Mbps



Tamaño del frame Ethernet

- ❑ En Ethernet/802.3 es fundamental detectar una colisión
- ❑ Para ello existe un tiempo máximo que un nodo debe quedar censando el canal en espera de recibir una señal jam

Campo Protocolo/longitud de Ethernet

- ❑ Por razones históricas este campo tiene dos posibles significados. Para saber si es uno u otro hay que averiguar su valor
- ❑ Cuando representa el protocolo del paquete que contiene se suele llamar 'Ethertype'
- ❑ Algunos Ethertypes comunes (en hexadecimal):
 - IP: 0x0800
 - ARP: 0x0806
 - Appletalk: 0x809b

Dispositivos LAN

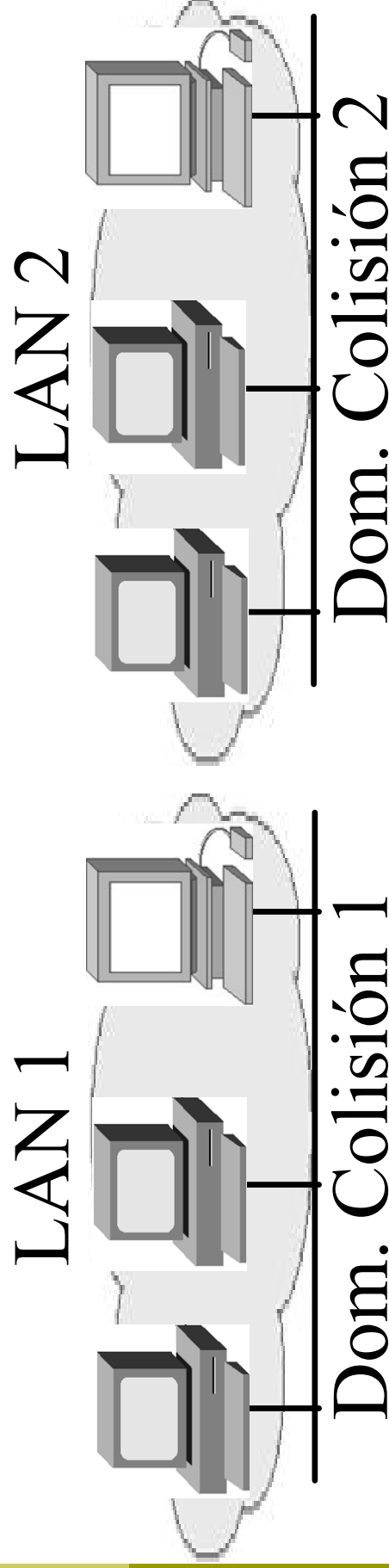
- ❑ Repetidores (Físico)
- ❑ Hubs (Físico)
- ❑ Bridges (Físico)
- ❑ Switch (Físico)

Repetidores



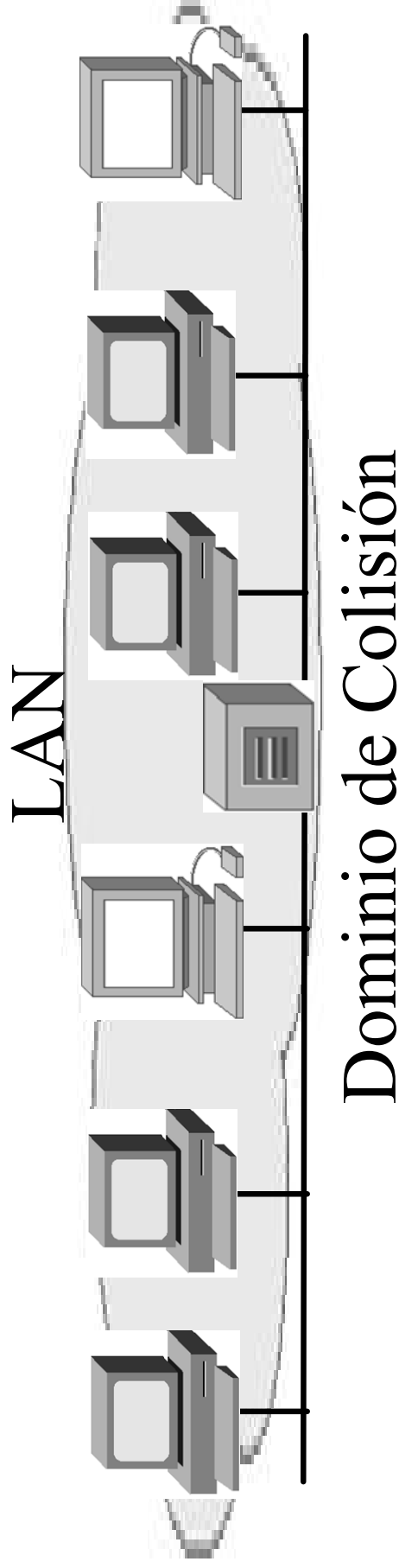
Dominios de Colisión

- Un *dominio de colisiones*: zona o distancia física en la que es probable que ocurra una colisión producto del funcionamiento de CSMA/CD.



Dominios de Colisión y Repetidores

- ▣ Se extiende el dominio de colisiones al usar repetidores.

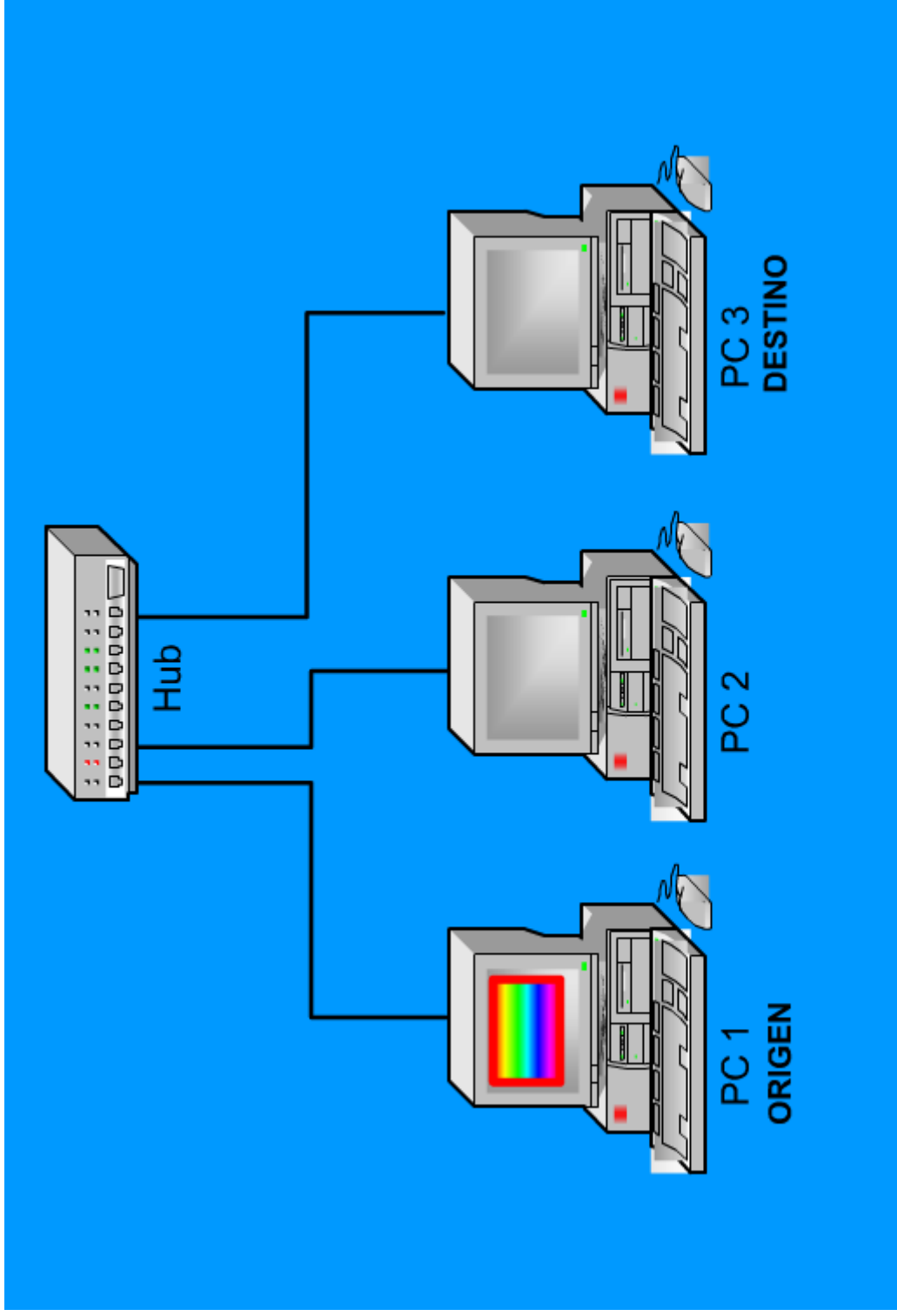


Hubs

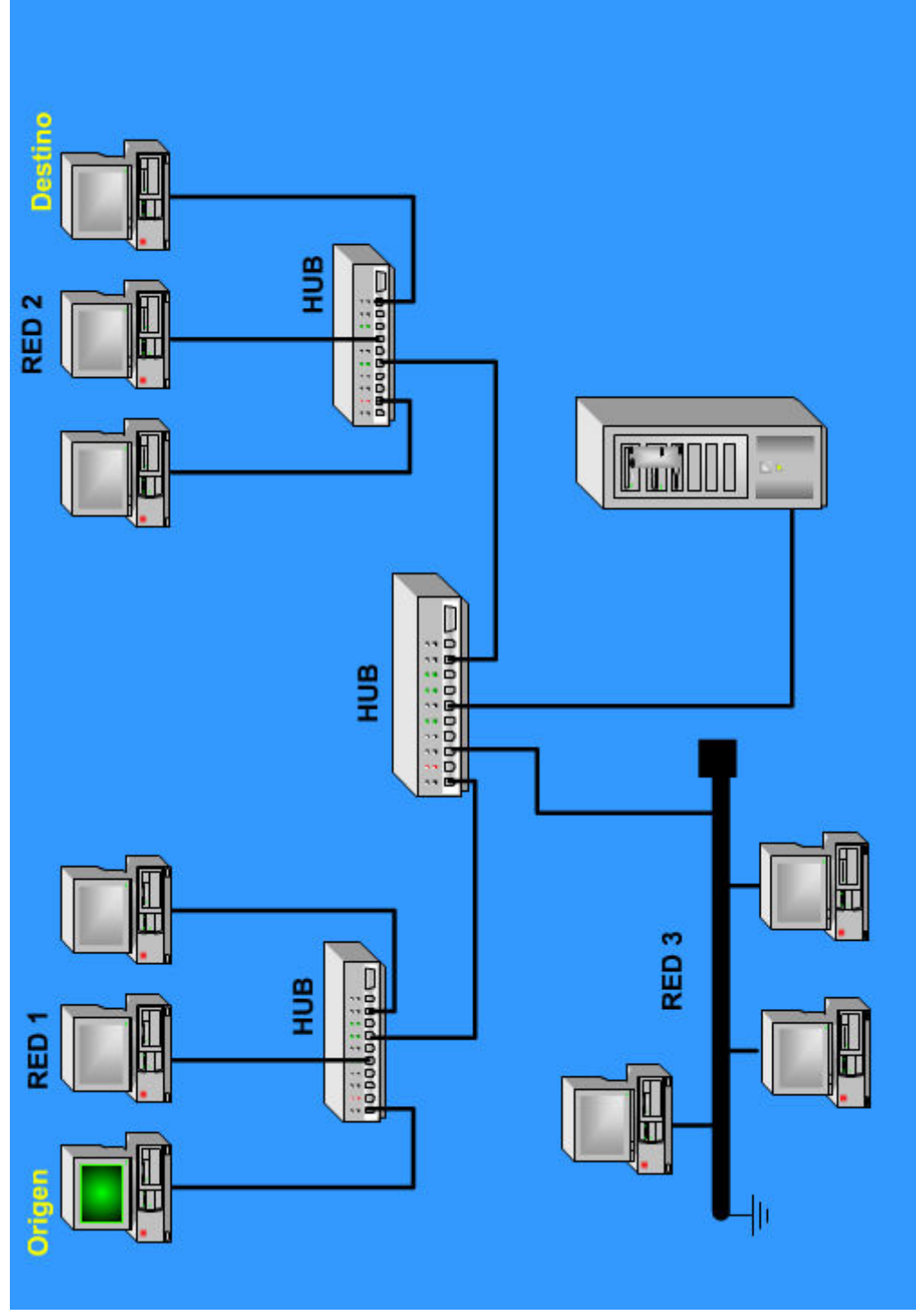
- ❑ Repetidores Multipuertas
- ❑ ¿Stackeables? ¿Managed? ¿SNMP? ¿Uplink?



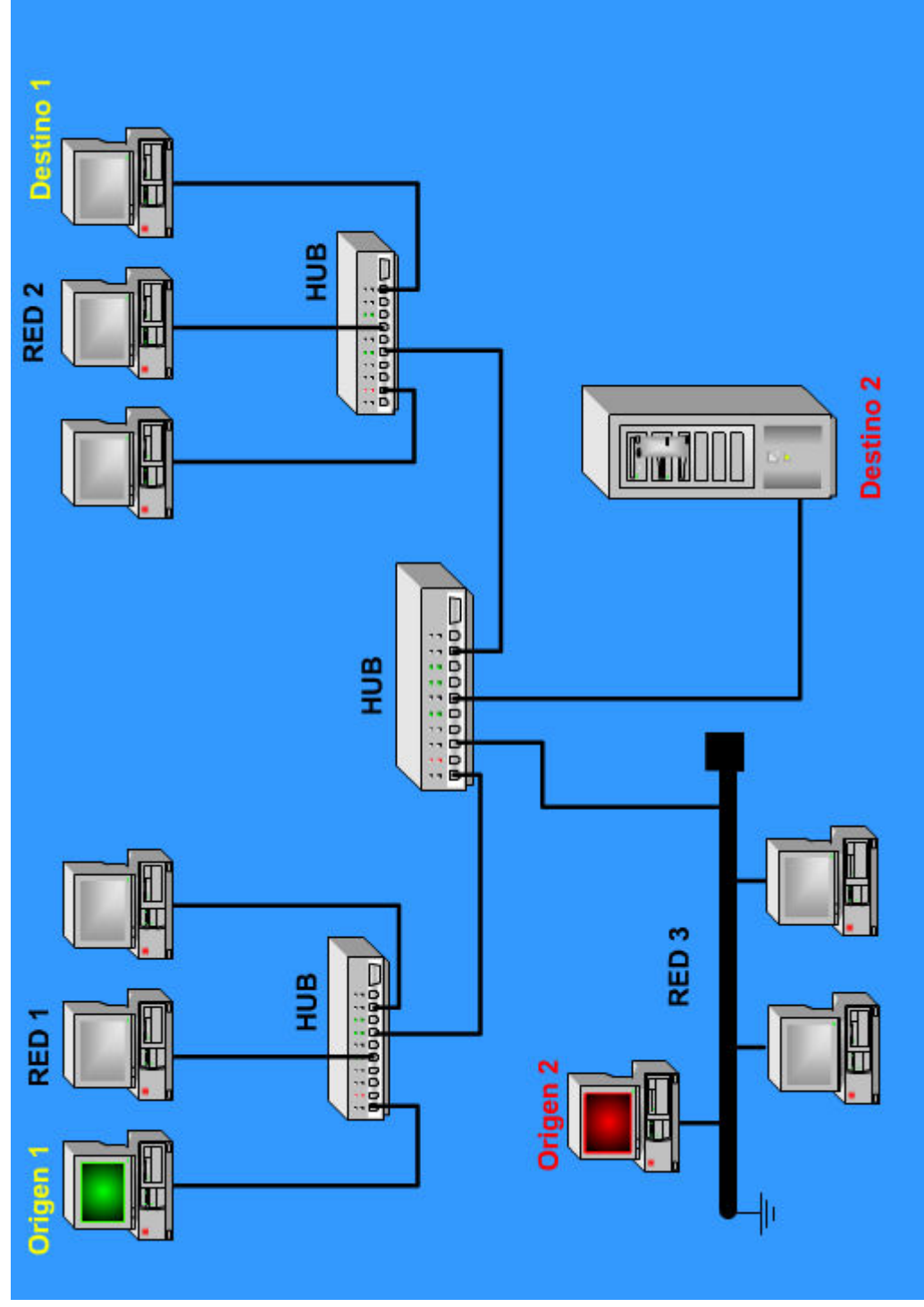
Funcionamiento Hubs/Repetidores



Hubs Conectando LANs



Hubs y Dominios de Colisión

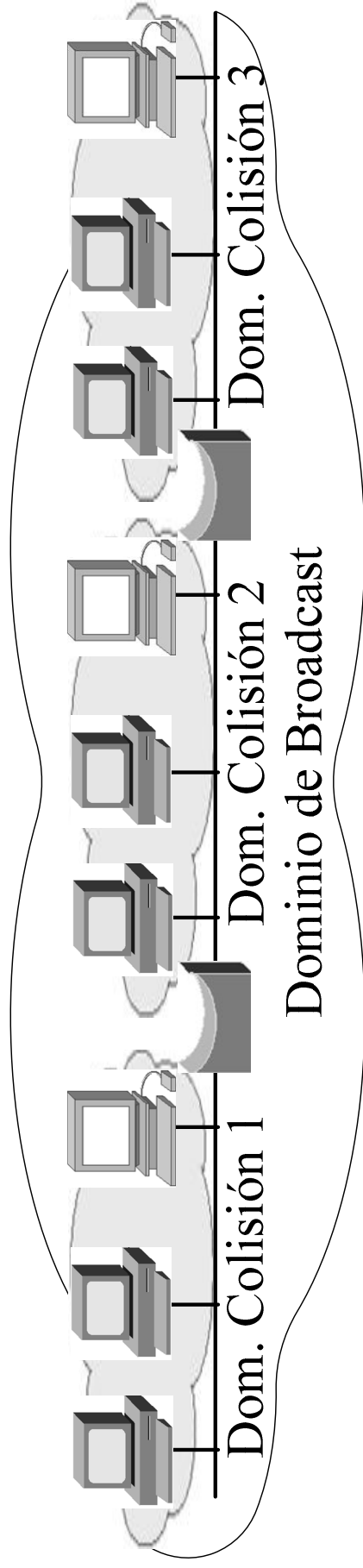


Puentes o Bridges

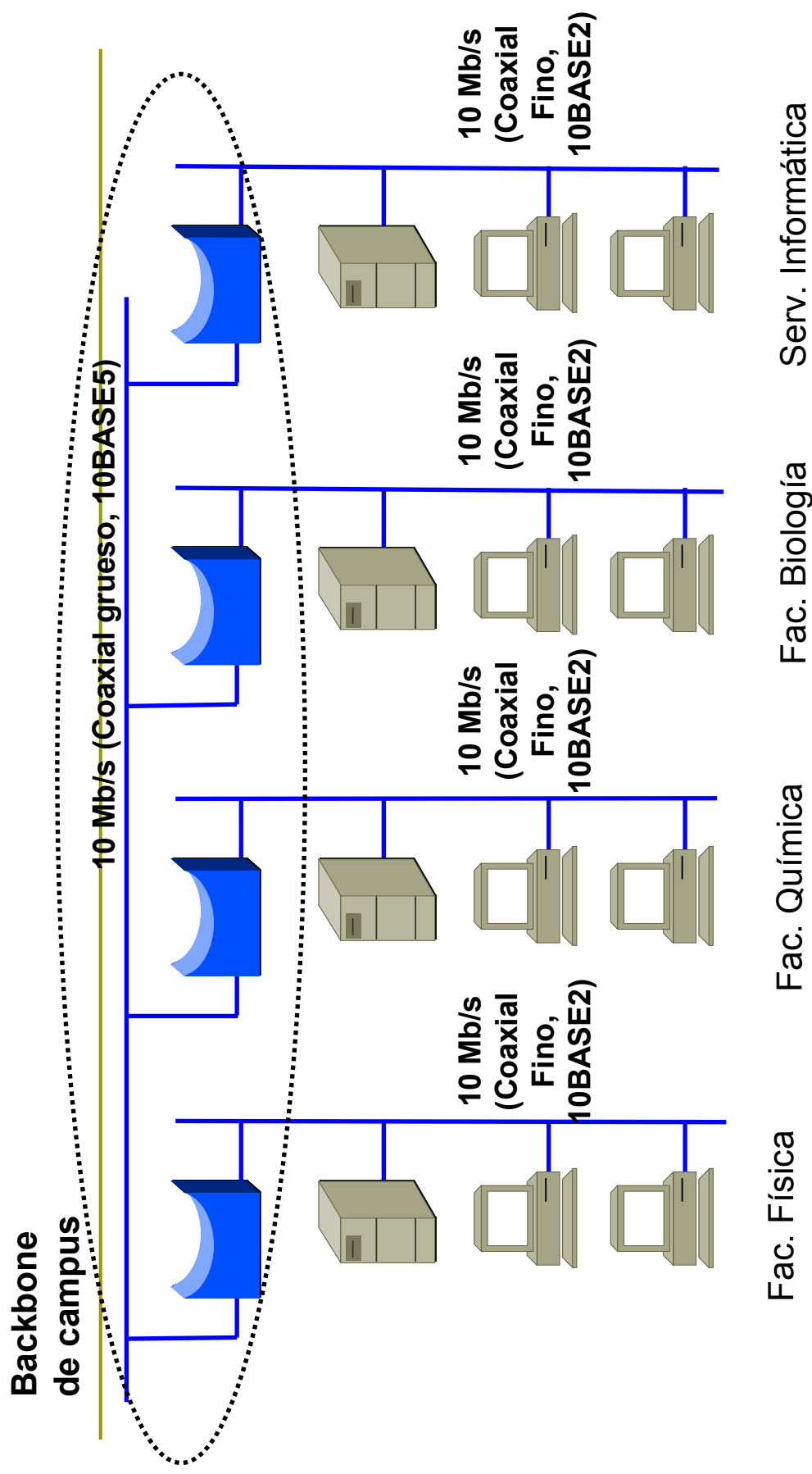
- Separan redes a nivel MAC
- Objetivos:
 - Rendimiento (separan tráfico local)
 - Seguridad (separan medio broadcast)
 - Fiabilidad (un problema no afecta a toda la red)
 - Interoperabilidad (Ethernet-Token Ring)
 - Distancia (en Fast Ethernet 412 m)
 - Número de estaciones (1024 en Ethernet)

Dominios de Colisión y Bridges

- ❑ Se separa el dominio de colisiones al usar bridges.
- ❑ *Dominio de broadcast:* toda la zona o distancia lógica en la que un frame dirigido a FF:FF:FF:FF es recibido por los nodos conectados a una LAN.

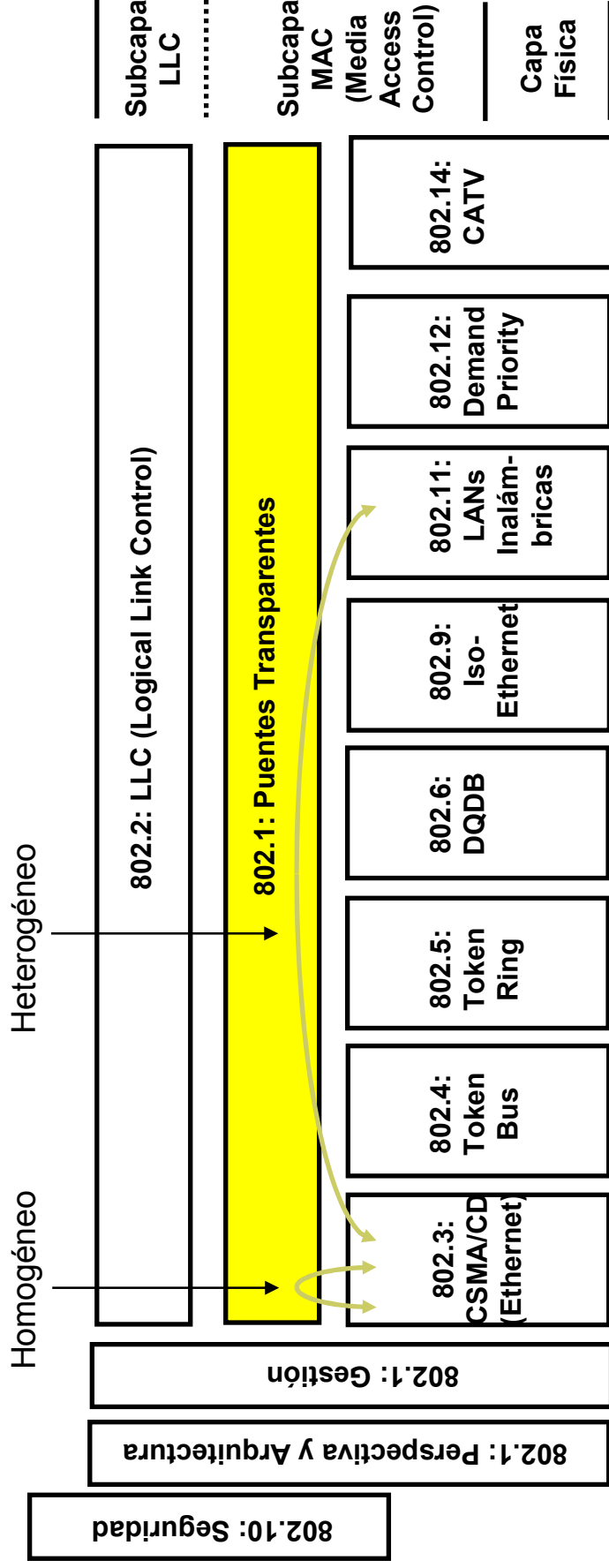


Red con puentes



Red típica de un campus universitario en los años 1985-1990

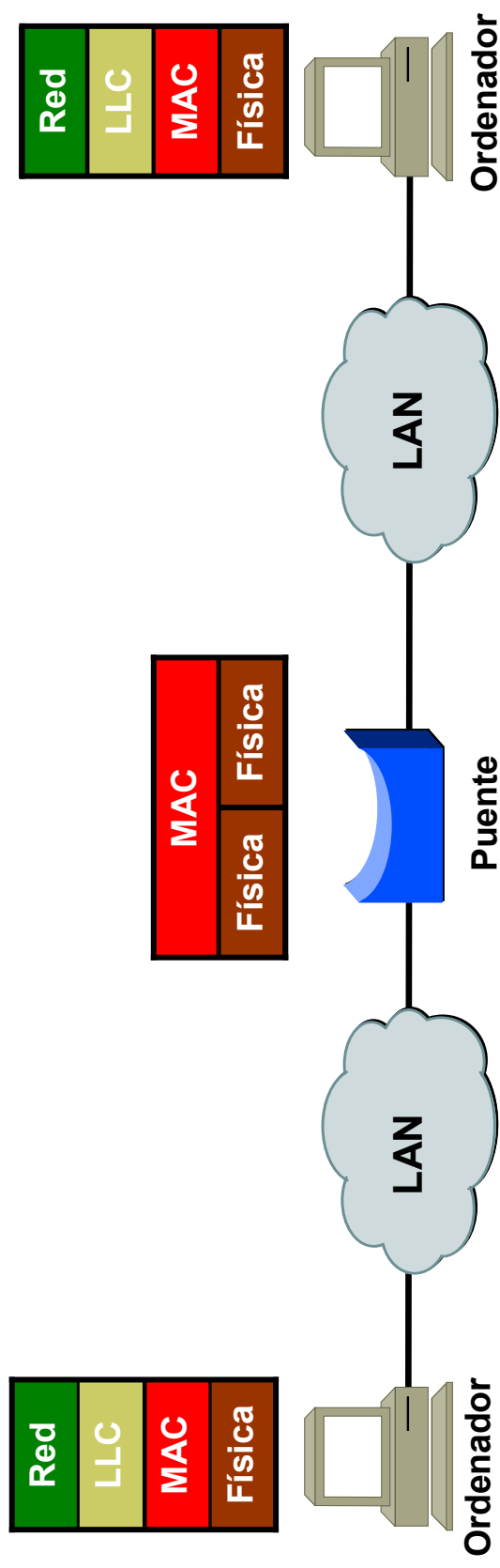
Los puentes transparentes en la arquitectura IEEE 802



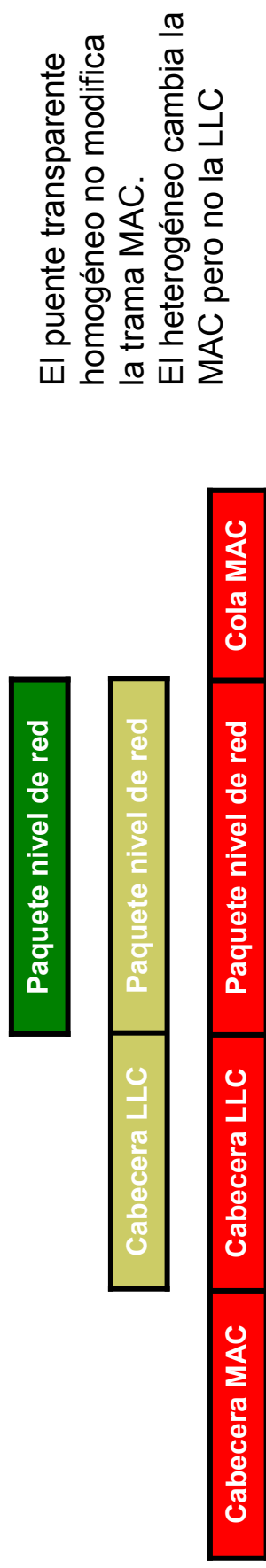
Tipos de Bridges

- Por su funcionamiento:
 - Transparentes (802.1): el puente sin conversión de formato
 - Ruteo desde el origen (802.5): Token Ring
- Por su alcance:
 - Locales: interconectan LANs directamente
 - Remotos: para unir LANs a través de conexiones WAN.

Funcionamiento de un puente transparente

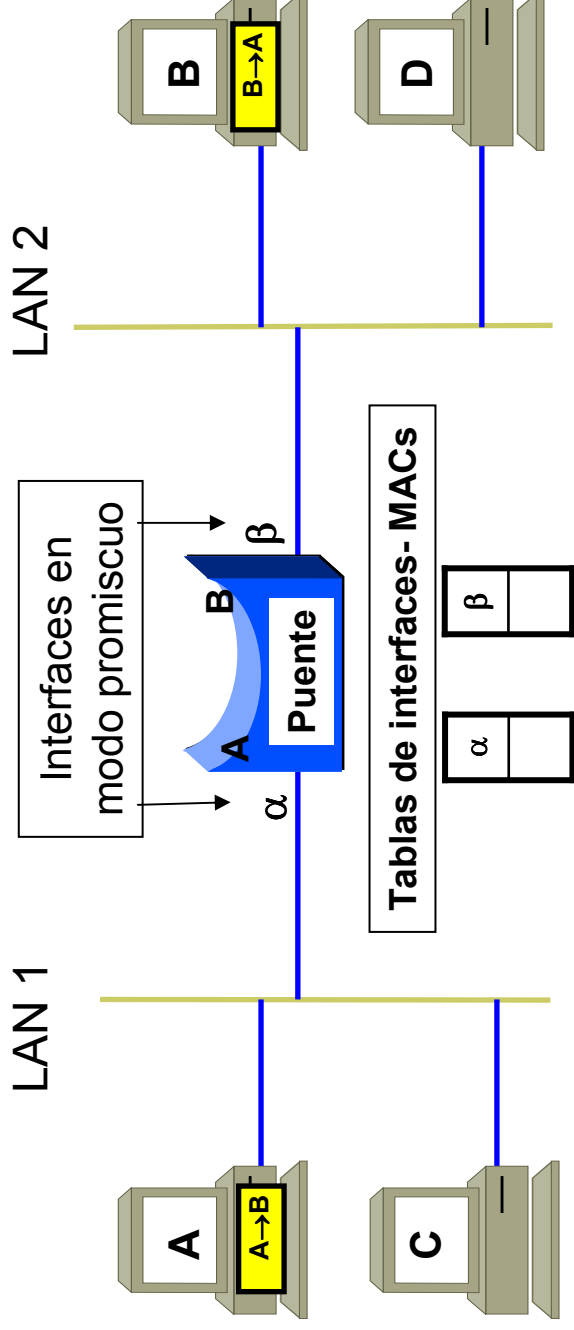


Arquitectura



Encapsulado

Funcionamiento de un puente transparente



1. A genera una trama con destino B que el puente recibe por α
 2. El puente busca a B en la tabla de direcciones de α ; si le encuentra descarta la trama, si no la reenvía por β
 3. El puente incluye A en su lista de direcciones de la interfaz α
 4. Cuando B envía una trama de respuesta el puente le incluirá en la lista de la interfaz β
- Las tablas solo se actualizan con direcciones de origen. Si una estación nunca emite una trama (o no pone la dir. de origen) su dirección no estará en las tablas.

Formato de una trama MAC 802.x (x=3,4,5,...)

6 6 4

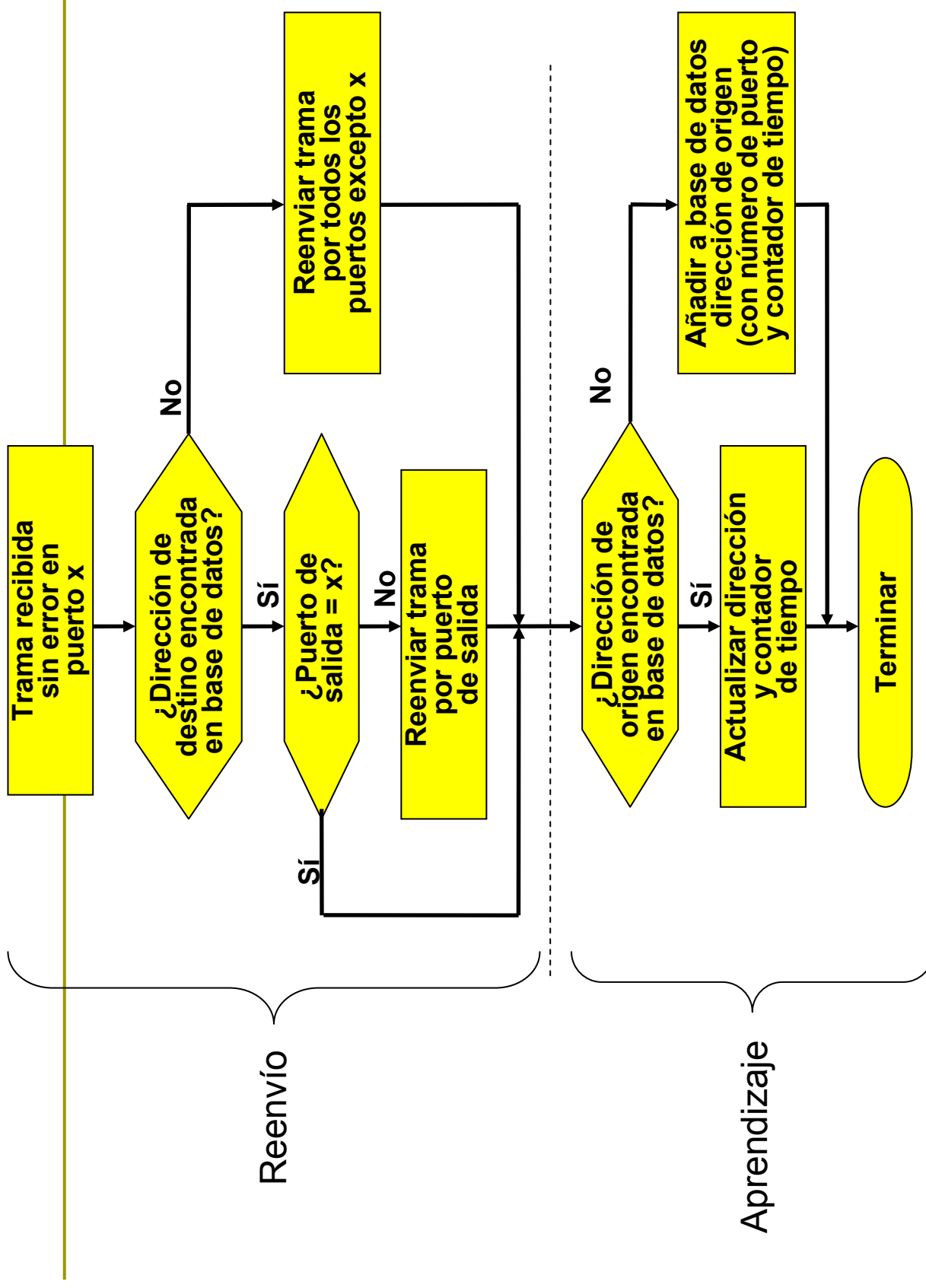
| Preámbulo de trama | Direcc. MAC de destino | Direcc. MAC de origen | Datos | CRC | Final de Trama |
|--------------------|------------------------|-----------------------|-------|-----|----------------|
|--------------------|------------------------|-----------------------|-------|-----|----------------|

La principal utilidad de la dirección MAC de origen es permitir el funcionamiento de los puentes transparentes

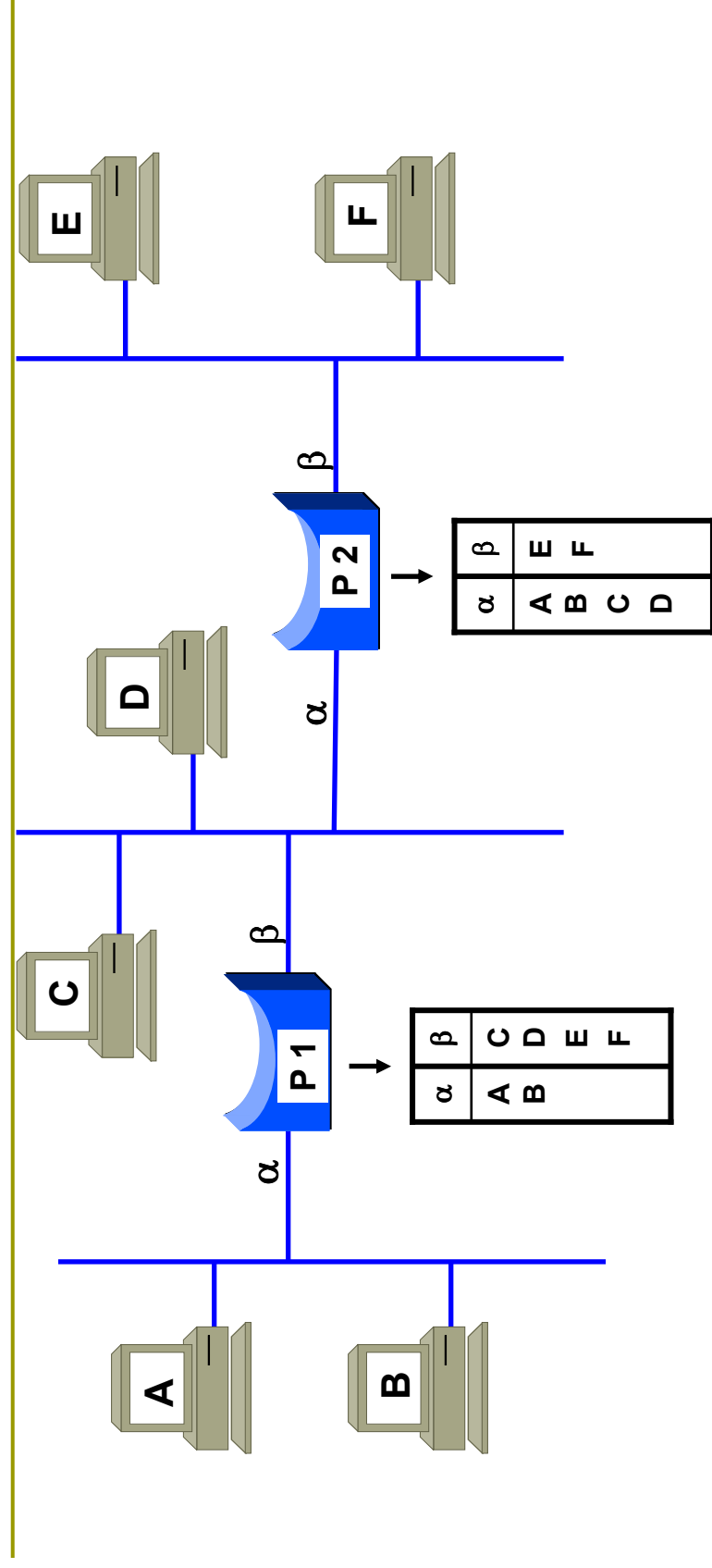
Puentes transparentes (IEEE 802.1D)

- ❑ Se pueden utilizar en todo tipo de LANs
- ❑ Funcionan en modo 'promiscuo' (lo oyen todo)
- ❑ El puente averigua que estaciones (direcciones MAC) tiene a cada lado, y solo reenvía las tramas que:
 - Van dirigidas a una estación al otro lado, ●
 - Tienen un destino desconocido para el puente, ●
 - Tienen una dirección de grupo (broadcast o multicast). Estas no figuran nunca como direcciones de origen y por tanto no están nunca en la tabla MAC
- ❑ La trama reenviada es idéntica a la original (la dirección MAC de origen no se cambia por la de la interfaz de salida).
- ❑ Aunque cada interfaz del puente tiene una dirección MAC distinta, estas direcciones no aparecen nunca en las tramas reenviadas por él.

Funcionamiento de los puentes transparentes



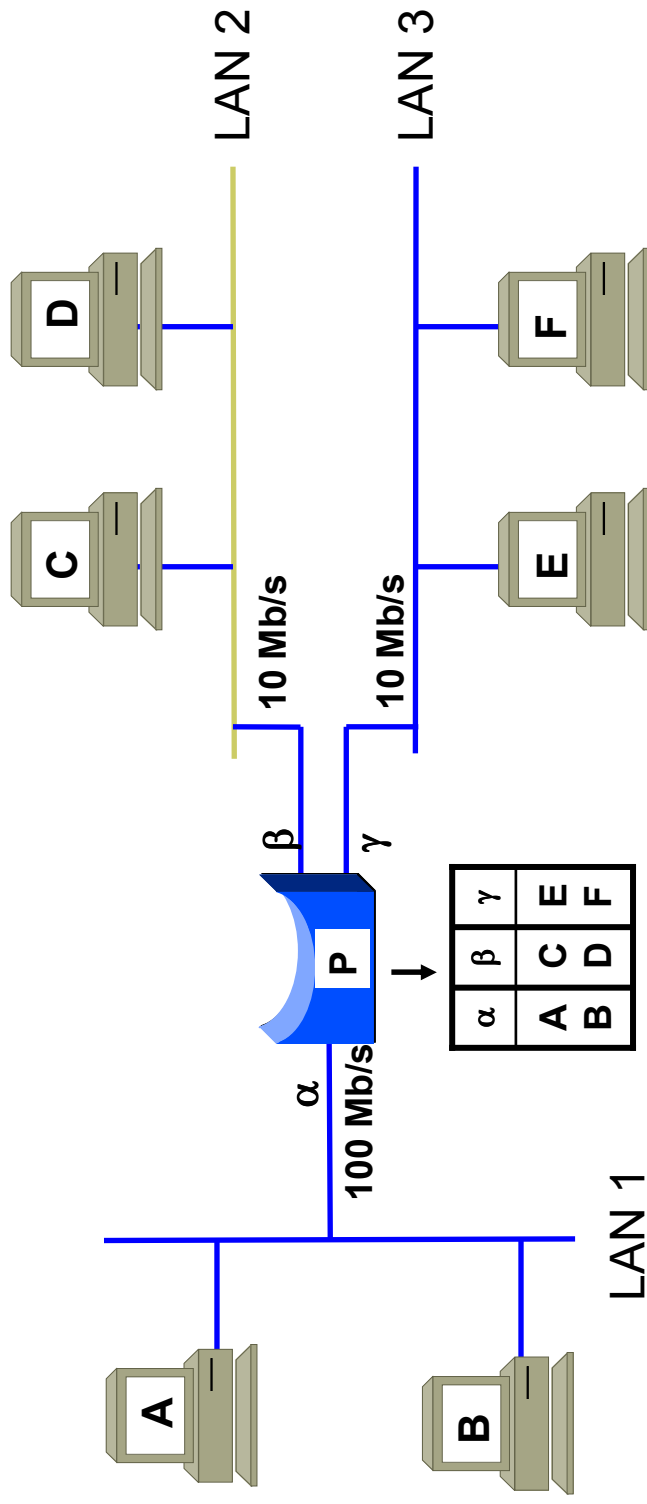
Red con dos puentes



Desde el punto de vista de P1 las estaciones C, D, E y F están todas en la misma LAN, ya que cuando P2 reenvía por α las tramas de E y F la copia es idéntica al original (la dirección MAC de origen no se cambia)

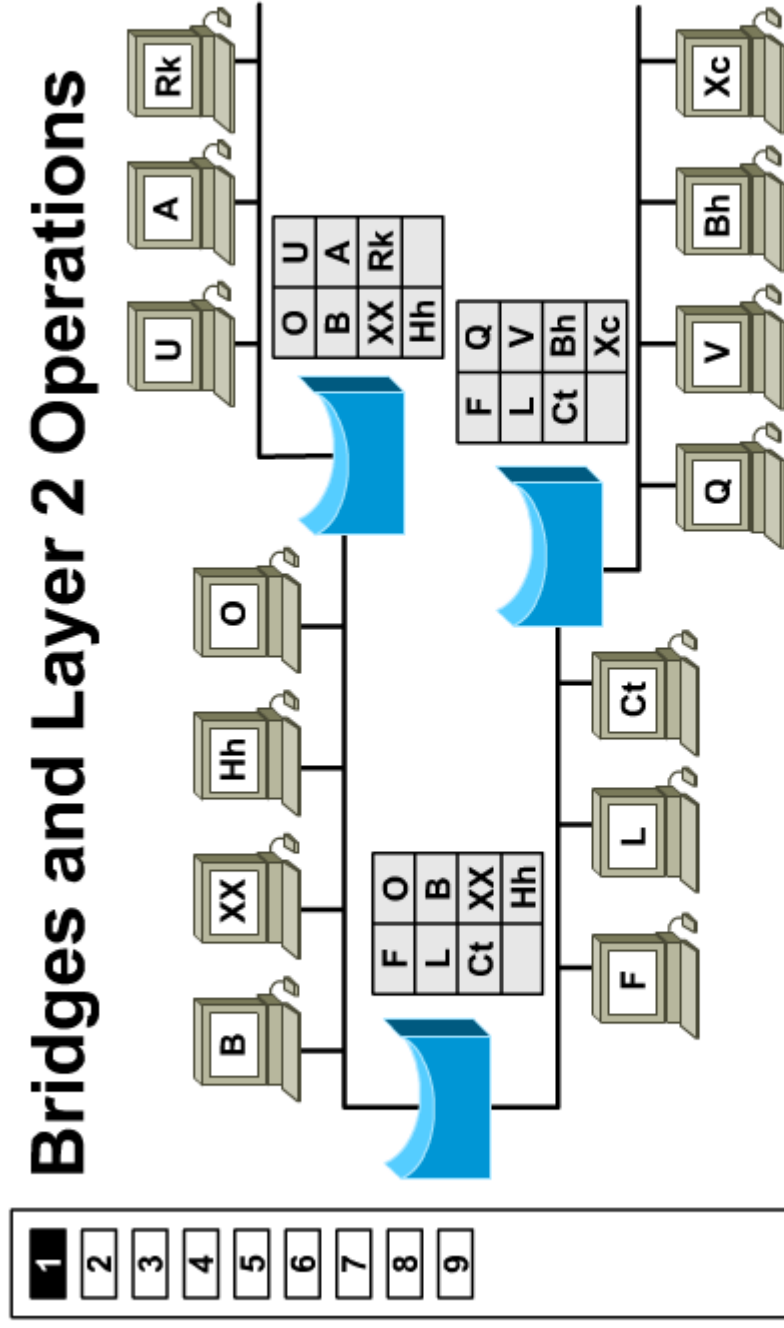
Puente con tres interfaces (de diferente velocidad)

La velocidad puede no ser la misma en todas las interfaces. El puente procesa tramas enteras y puede adaptar velocidades diferentes.

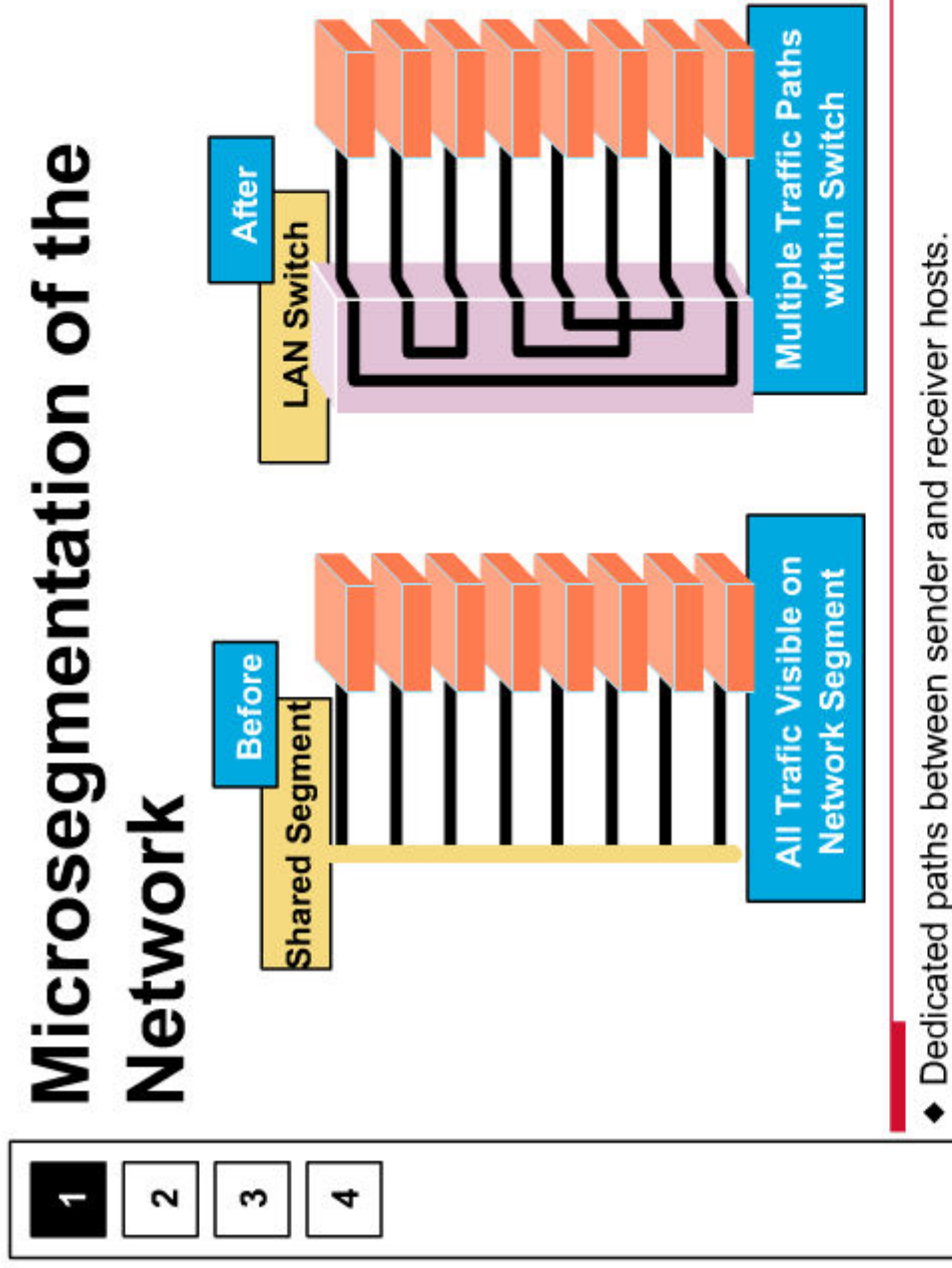


Una vez el puente ha conseguido las direcciones de todos los ordenadores las tramas solo viajan por las LANs que es preciso. Una trama de A hacia C solo sale por β , no por γ

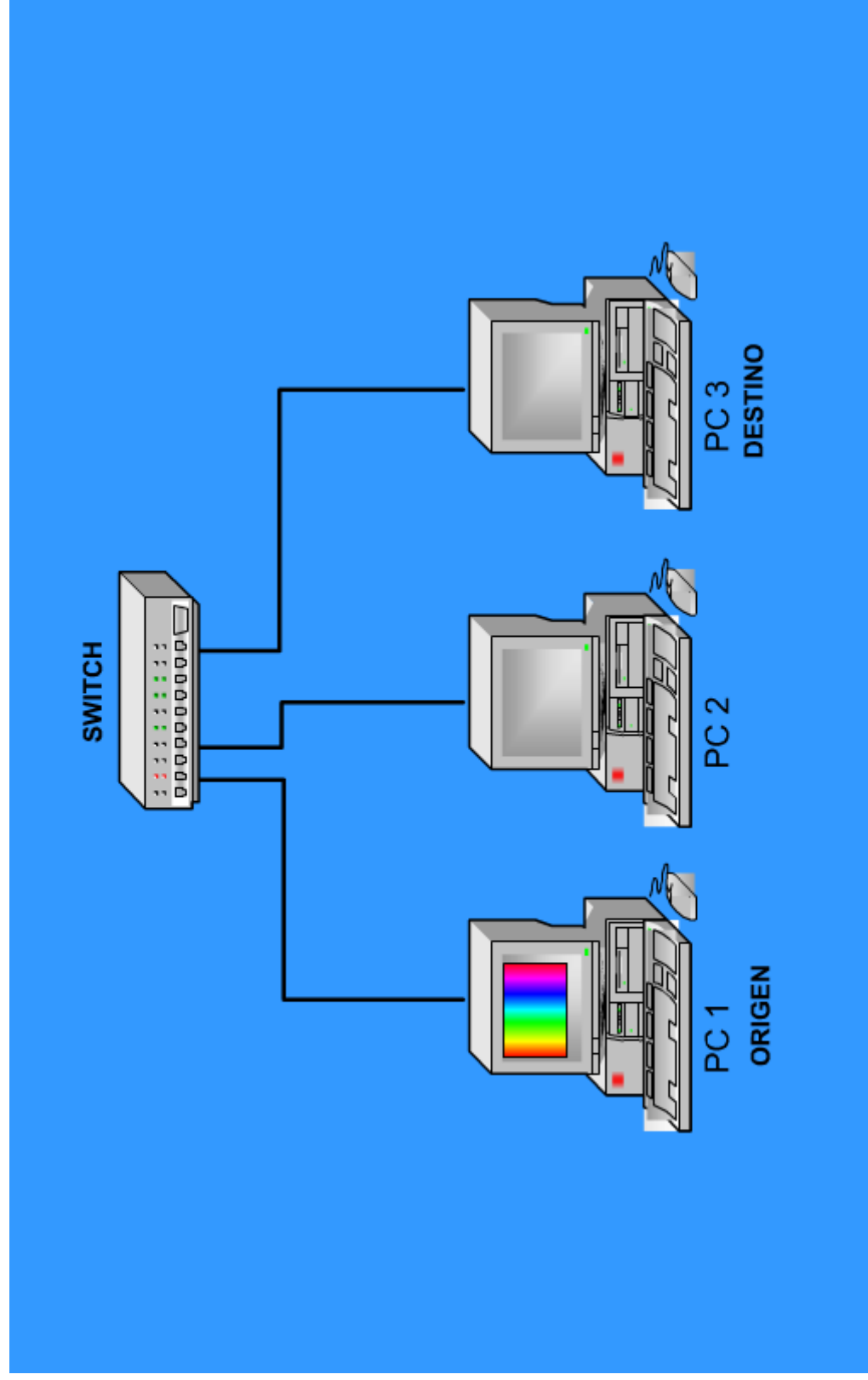
Ej. Funcionamiento Puente transparente



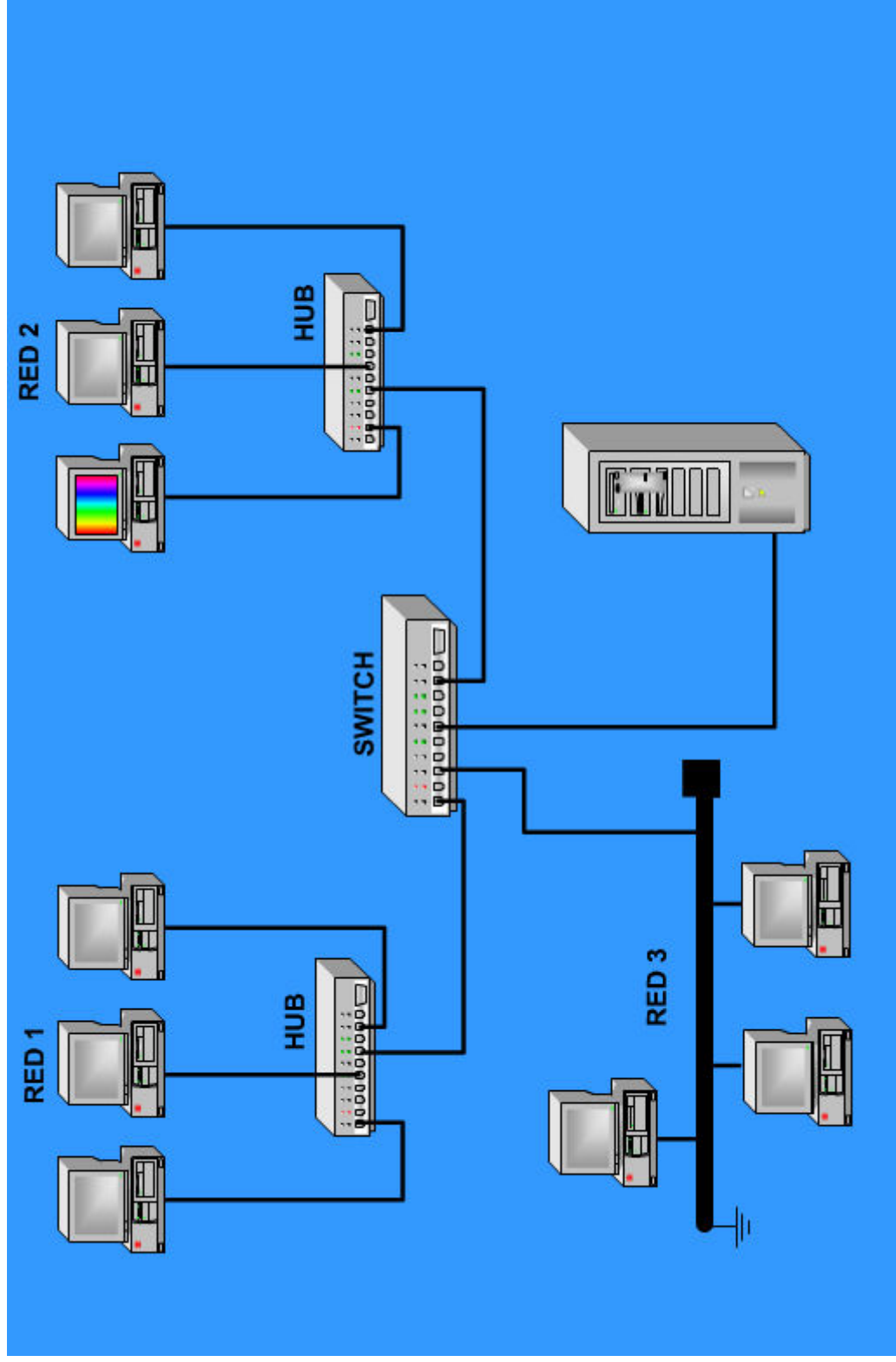
Segmentación con bridge transparente



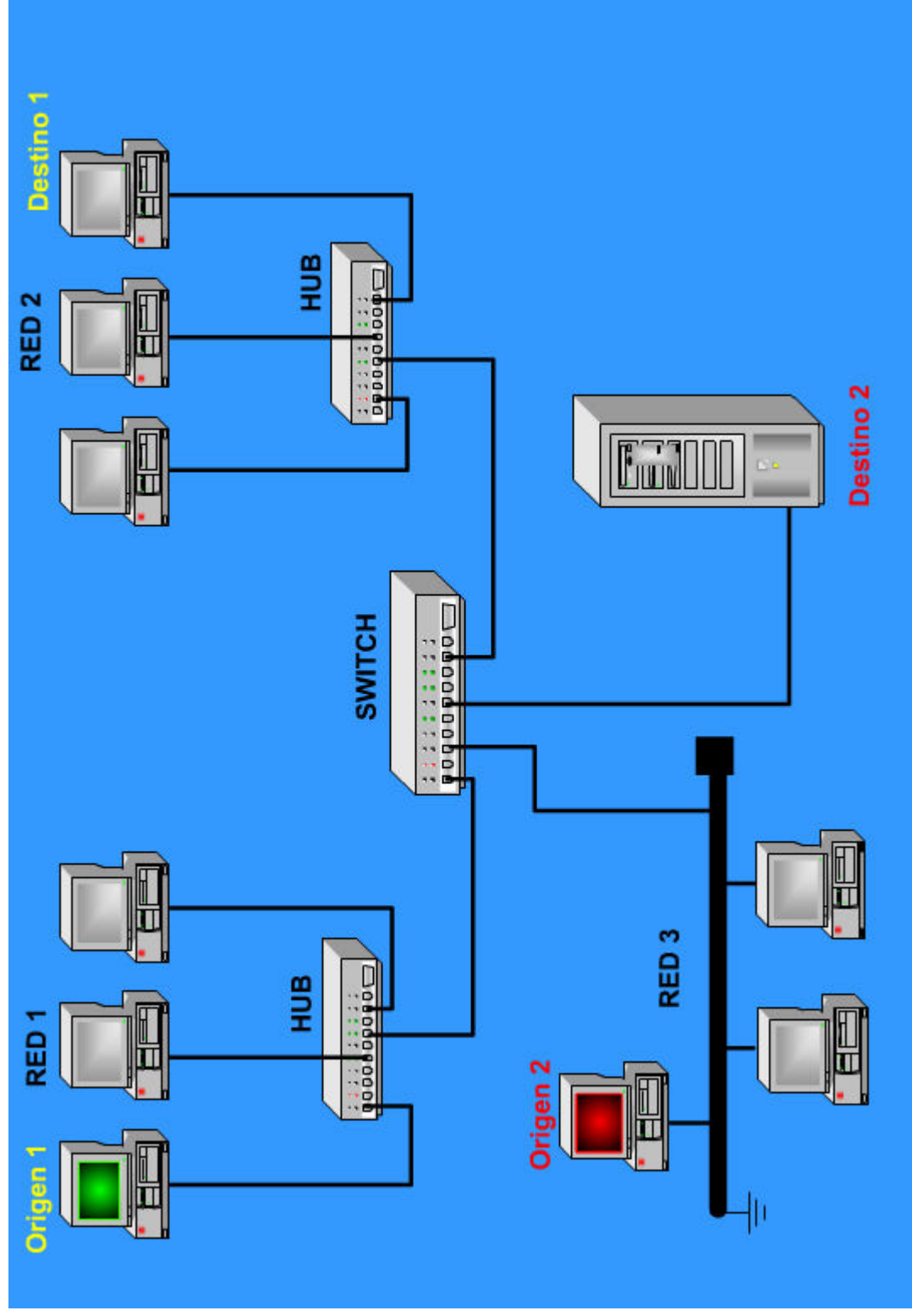
Funcionamiento bridge transparente



Bridges Conectando LANs



Bridges y Dominios de Colisión



Repasemos Aprendizaje de direcciones

Bridge con dos interfaces: eth0 y eth1:

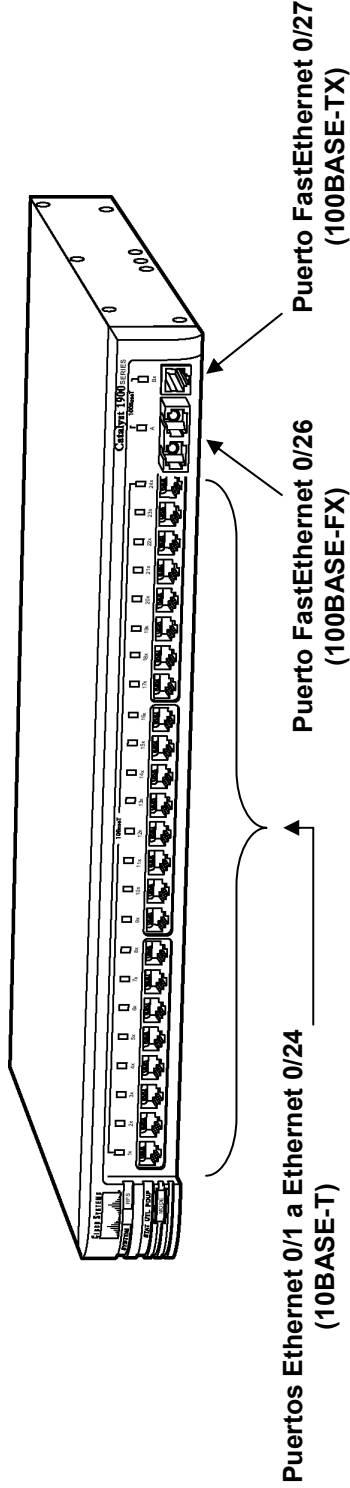
1. Bridge recibe por eth0 frame con dirección de origen A y dirección de destino B
2. Bridge incluye A en su tabla de direcciones (SAT) y la asocia a la interfaz eth0
3. Bridge busca B en la SAT; si la encuentra asociada a eth0 descarta frame, si no reenvía usando por la otra interfaz.

Consecuencias del Aprendizaje

1. Bridge sólo aprende direcciones de origen para actualizar las tablas.
2. Si nodo no Tx frames su dirección no estará en las tablas.
3. Se utiliza contadores de tiempo (aging) para borrar direcciones de SAT
4. Los bridges especifican el número máximo de direcciones que pueden almacenar (1 a 8K direcciones)

Tabla MAC de un conmutador LAN (Catalyst 1900)

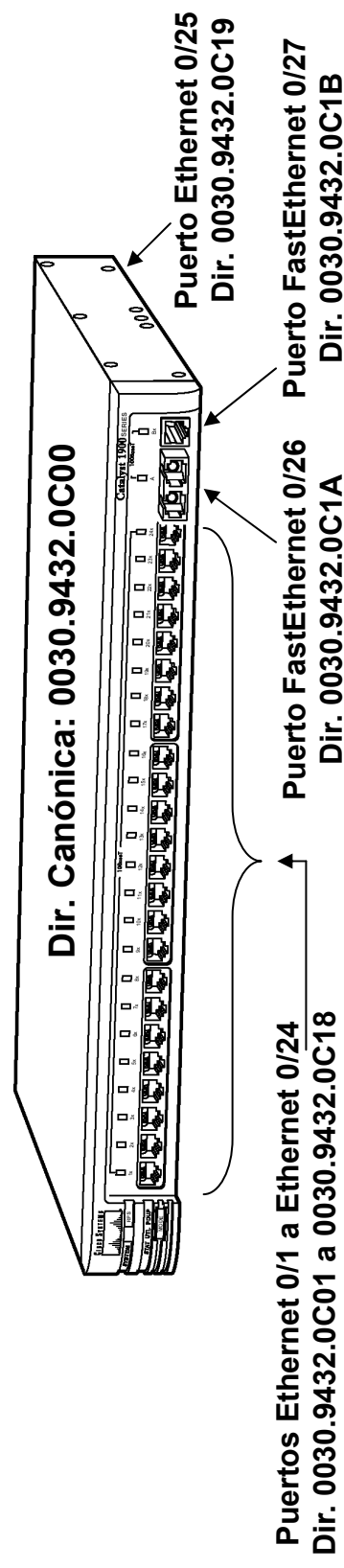
| # show mac-address-table | |
|--------------------------|-------------------|
| 0004.75EF.4BEB | Ethernet 0/1 |
| 0004.75EF.4B1C | Ethernet 0/2 |
| 0004.75EF.2DA6 | Ethernet 0/3 |
| 0004.75EF.4AD9 | Ethernet 0/4 |
| 0004.75EF.49D6 | Ethernet 0/5 |
| 0004.75EF.49D2 | Ethernet 0/7 |
| 0004.75EF.4B0C | Ethernet 0/8 |
| 0004.75EF.49D3 | Ethernet 0/9 |
| 0004.75EF.472B | Ethernet 0/10 |
| 0004.75EF.4952 | Ethernet 0/11 |
| 0004.75EF.4BF8 | Ethernet 0/12 |
| 0004.75EF.4B19 | Ethernet 0/13 |
| 0004.75EF.41DB | Ethernet 0/16 |
| 0004.75EF.49CF | Ethernet 0/17 |
| 0004.75EF.494F | Ethernet 0/18 |
| 0004.75EF.4AD8 | Ethernet 0/19 |
| 0004.75EF.4B30 | Ethernet 0/20 |
| 0004.75EF.3D67 | Ethernet 0/21 |
| 0004.75EF.4753 | Ethernet 0/22 |
| 0004.75EF.49D8 | Ethernet 0/23 |
| 0001.E654.0FF9 | Ethernet 0/24 |
| 0040.3394.95CD | FastEthernet 0/27 |
| 00C0.DF0F.C9E0 | FastEthernet 0/27 |
| 000C.6E1D.126E | FastEthernet 0/27 |
| 0060.0811.9114 | FastEthernet 0/27 |
| 0000.B458.D92B | FastEthernet 0/27 |
| 00D0.BABF.B200 | FastEthernet 0/27 |
| 0000.48B5.246F | FastEthernet 0/27 |
| 0004.0018.C74B | FastEthernet 0/27 |
| 0040.F479.6773 | FastEthernet 0/27 |
| 0004.769F.7ABC | FastEthernet 0/27 |
| 0001.020B.F581 | FastEthernet 0/27 |
| 0001.E68E.7273 | FastEthernet 0/27 |
| 000B.5FF8.8900 | FastEthernet 0/27 |
| 00D0.BABF.B218 | FastEthernet 0/27 |
| 0000.E87B.9E9B | FastEthernet 0/27 |



Un conmutador LAN es un puente con muchas interfaces

Puentes y direcciones MAC

- ❑ Cada interfaz del puente tiene una dirección MAC diferente. A menudo hay una dirección adicional que no se corresponde con ninguna interfaz y que se usa para identificar el puente mismo. Es la que llamamos **dirección 'canónica'**.
- ❑ Las direcciones propias del puente no aparecen nunca en las tramas que reenvía, pero él las usa como direcciones de origen cuando tiene que enviar tramas propias.
- ❑ En unos casos utiliza la dirección canónica y en otros la de la interfaz por la que envía la trama.



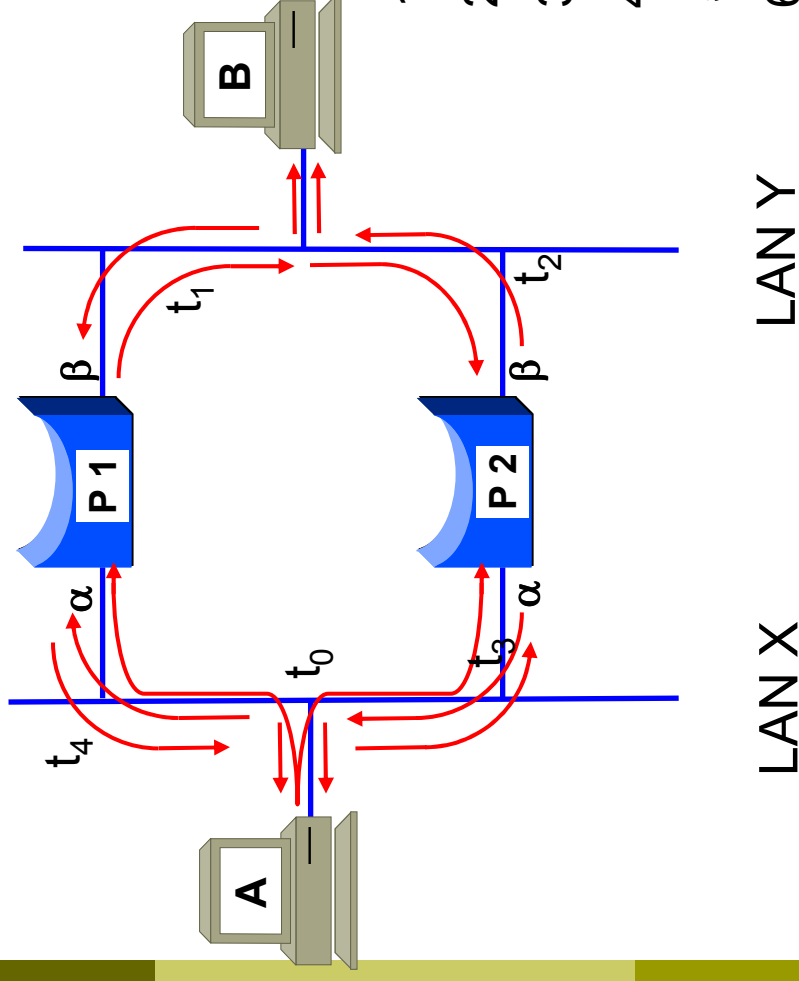
Aprendizaje de direcciones

- ❑ Al cabo de un rato las tablas incluyen las direcciones de la mayoría de las estaciones activas de todas las LANs conectadas directa o indirectamente.
- ❑ Las entradas de la tabla MAC tienen un tiempo de expiración (típico 5 min.) para permitir la movilidad.
- ❑ Las tablas se mantienen en memoria RAM, y tienen un tamaño limitado (típico 1000-8000 direcciones máx.)
- ❑ Las tablas son exhaustivas. No existe un mecanismo de sumarización o agrupación de direcciones por rangos ya que normalmente no guardan ninguna relación.

Bucles entre Puentes

- ❑ A veces al conectar LANs con varios puentes se producen bucles, es decir hay más de un camino posible entre dos redes.
- ❑ Estos bucles pueden hacerse por error o porque se quiere disponer de varios caminos para tener mayor fiabilidad y tolerancia a fallos.
- ❑ Con el funcionamiento normal de los puentes transparentes cuando se produce un bucle la red se bloquea. Para evitarlo se ha creado el protocolo denominado Spanning Tree.

Bucle entre dos LANs: el problema



1. A envía trama t_0 a LAN X
2. P1 retransmite t_0 en LAN Y como t_1
3. P2 retransmite t_0 en LAN Y como t_2
4. P2 retransmite t_1 en LAN X como t_3
5. P1 retransmite t_2 en LAN X como t_4
6. ... y así sucesivamente.

Transmitiendo una sola trama la red se satura eternamente

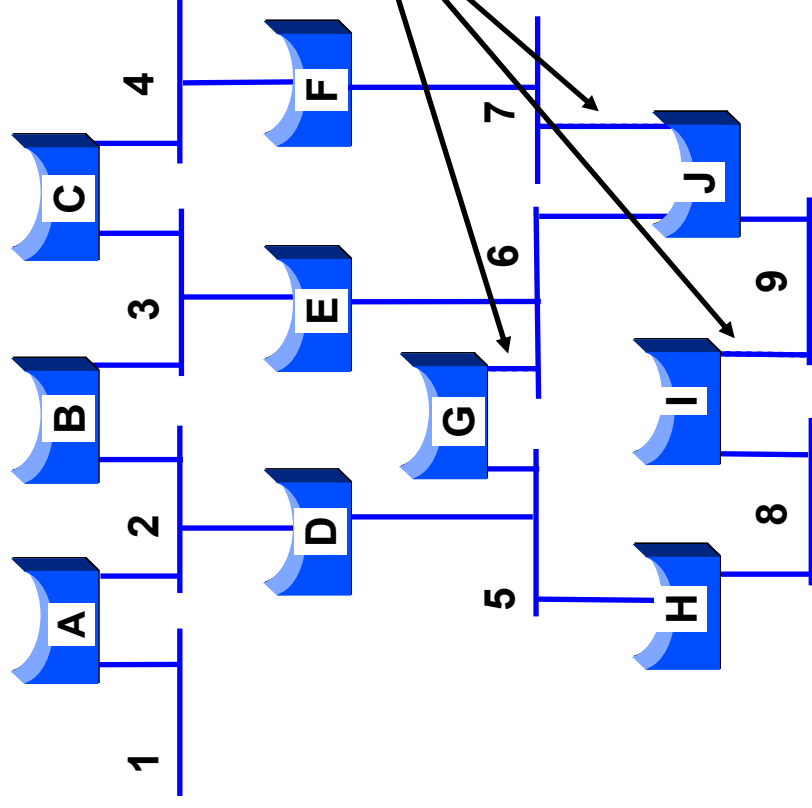
Red con bucles

En esta red hay tres bucles:

B-D-G-E

G-H-I-J

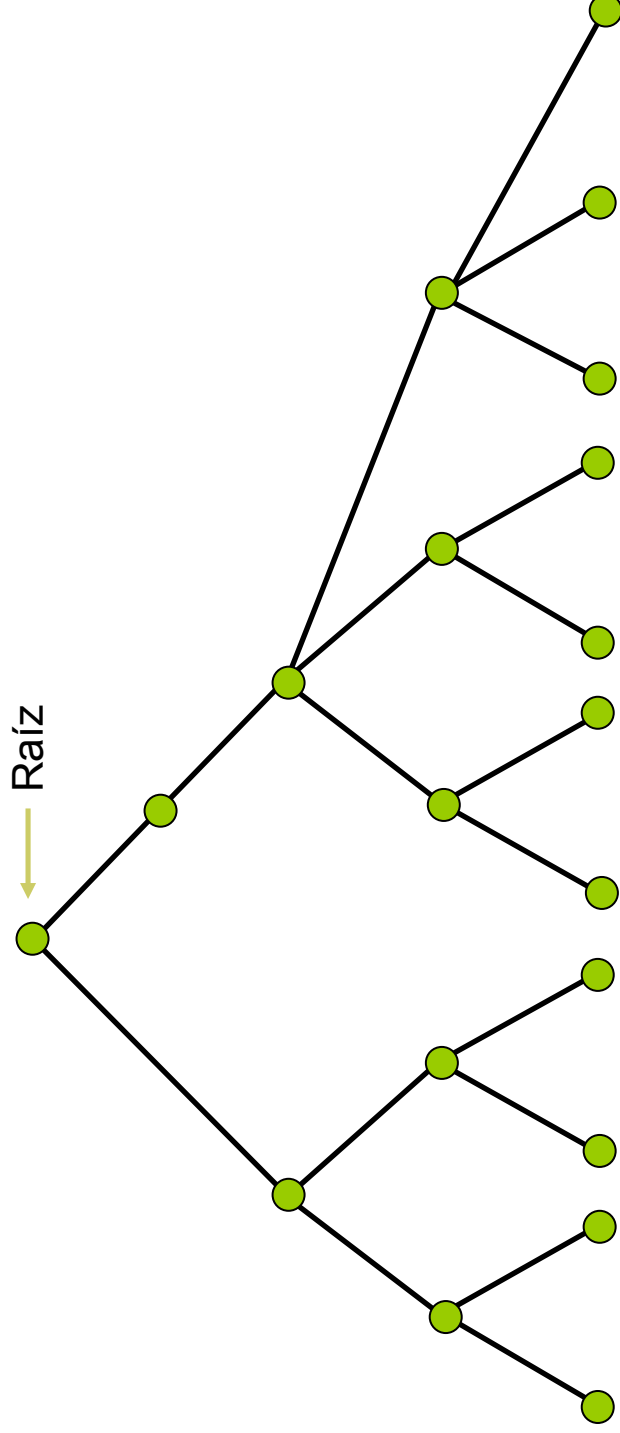
C-E-J-F



Desconectando tres cables (por ejemplo estos) se suprimen los bucles

Spanning Tree

Un Spanning Tree, o árbol de expansión, es un grafo en el que solo hay un camino posible entre dos nodos (un árbol sin bucles).



Si podemos pintar una red de puentes transparentes como un spanning tree, entonces el problema del bucle no puede darse. El objetivo del protocolo Spanning Tree es evitar que la red tenga bucles

Protocolo spanning tree

- ❑ Los puentes intercambian información sobre sus conexiones. La información se envía regularmente siguiendo un protocolo denominado Bridge Protocol. Los mensajes se denominan **BPDUs** (Bridge Protocol Data Units).
- ❑ Las BPDUs emplean un Ethertype propio y se envían a una dirección multicast reservada, la 01-80-C2-00-00-00. Así se asegura que se identifican fácilmente y que llegan a toda la red.
- ❑ Cada puente se identifica por su dirección MAC 'canónica'.
- ❑ Cada puerto recibe un identificador y tiene asociado un costo que por defecto es inversamente proporcional a su velocidad (ej.: 10 Mb/s costo 100, 100 Mb/s costo 10).
- ❑ Cada puente calcula el grafo de la red y observa si existe algún bucle; en ese caso se van desactivando interfaces hasta cortar todos los bucles y construir un árbol sin bucles o 'spanning tree'.

Protocolo spanning tree

- ❑ El protocolo Spanning Tree permite crear topologías redundantes, para mejorar la tolerancia a fallos.
- ❑ Spanning Tree es parte de la especificación de puentes transparentes (802.1D), pero los equipos de gama baja no lo implementan
- ❑ El tiempo de reacción ante fallos es lento (minutos) y no es fácil reducirlo en redes grandes. Por tanto no es adecuado como mecanismo de protección para redes de alta disponibilidad
- ❑ En 2001 se estandarizó el Rapid Spanning Tree (802.1w). Con el RST la red converge en pocos segundos. No todos los equipos soportan RST.