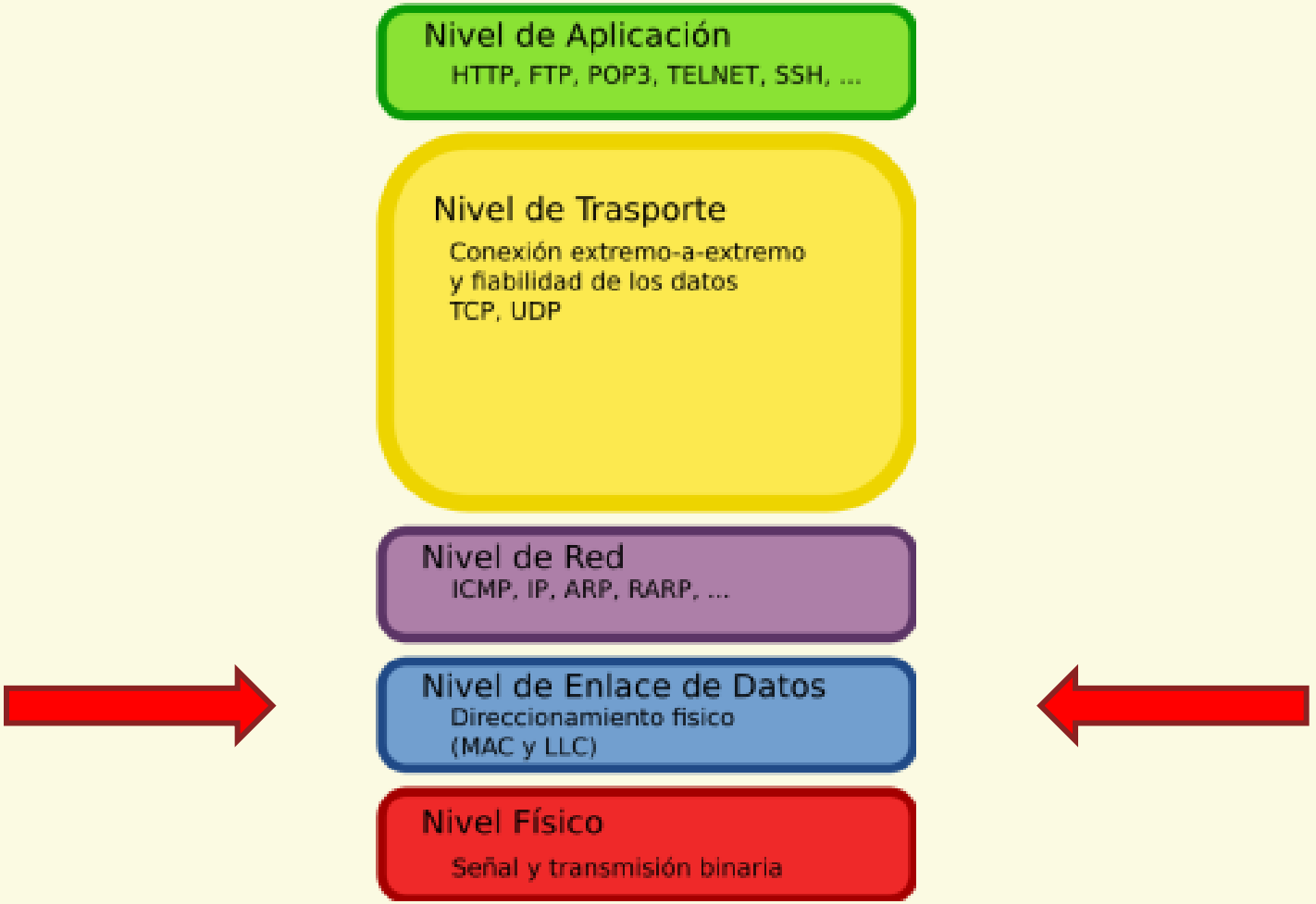
2. NIVEL ENLACE

Planificación y Administración de Redes ASIR1

1. Introducción a la transmisión por medio físico



CONTENIDOS

1. Comunicación en red local a nivel de enlace
2. Direcciones MAC
3. Trama MAC
4. Introducción al análisis del tráfico en la red
5. ARP, RARP
6. Tarjeta de red
7. Dispositivos de conexión
   - Repetidores y concentradores
   - Switch (generalidades, switches gestionables y no gestionables, velocidad puerto, velocidad total)
   - Puente (Bridge)
8. Segmentación de la red. Dominios de colisión
9. Riesgos asociados al nivel de enlace

1. Comunicación en red local a nivel de enlace

Sus principales funciones son:

- **Empaquetar / Desempaquetar los datos del nivel superior en tramas**
- **Control de acceso al medio**
- **Proporcionar al nivel de red una interfaz independiente de la red**

1. Comunicación en red local a nivel de enlace

Sus principales funciones son:

- **Control de errores (acuse de recibo)**
- **Control de flujo (no saturar al receptor)**
- **Recuperación de fallos**
- **Transmisión y direccionamiento de datos entre hosts adyacentes, situados en la misma red/subred**

1. Comunicación en red local a nivel de enlace

Una de las funciones principales de la capa de enlace es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos

Los datos se organizan en unidades llamadas tramas.

Cada trama tiene una cabecera que incluye una dirección e información de control y una cola que se usa para la detección de errores.

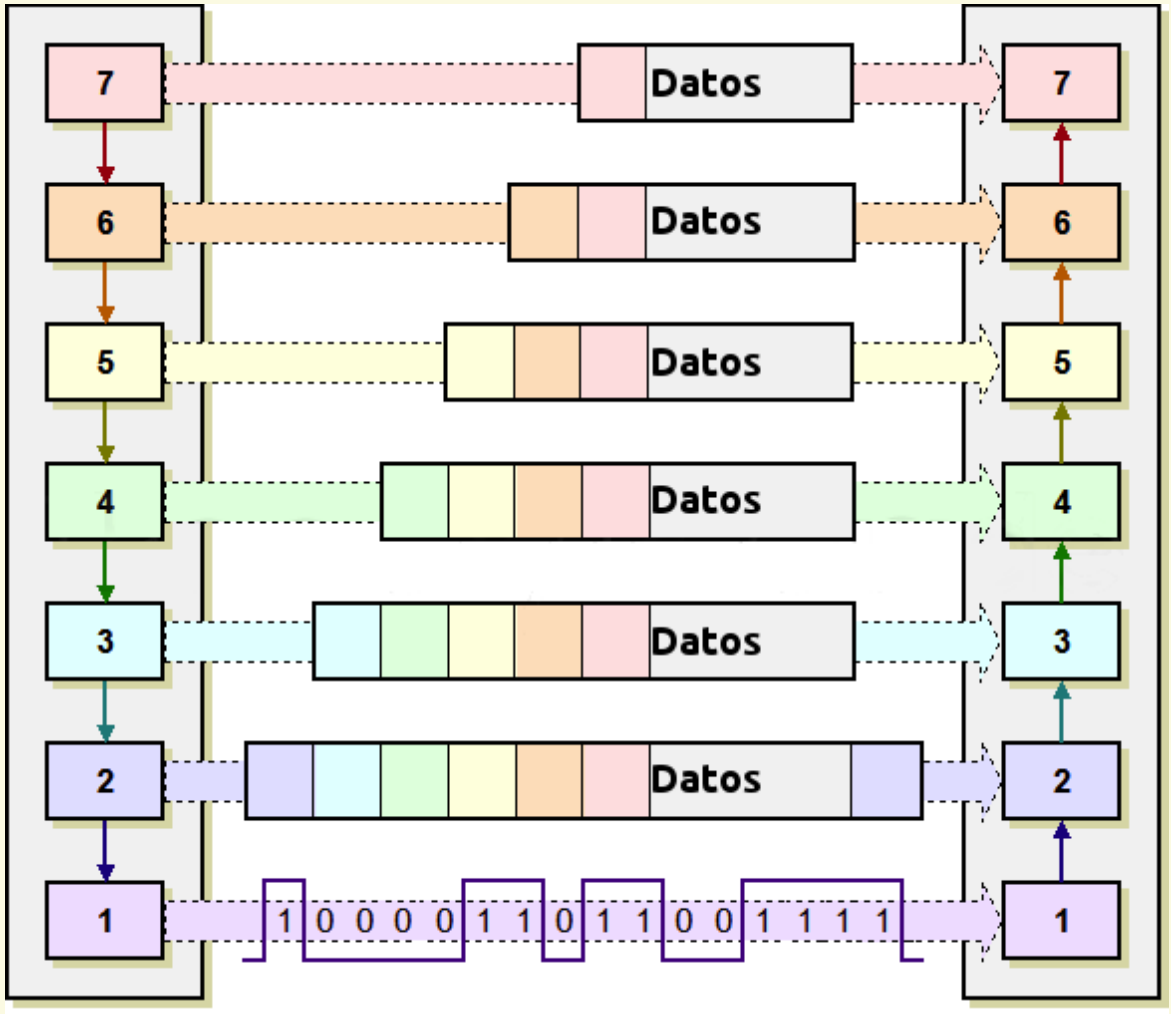
2. Direcciones MAC

- Está formada por 6 bytes (48 bits)
- Es única para cada tarjeta de red. Grabada en la ROM por el fabricante
- No se puede modificar, aunque técnicamente sí es posible
- Se expresan en hexadecimal

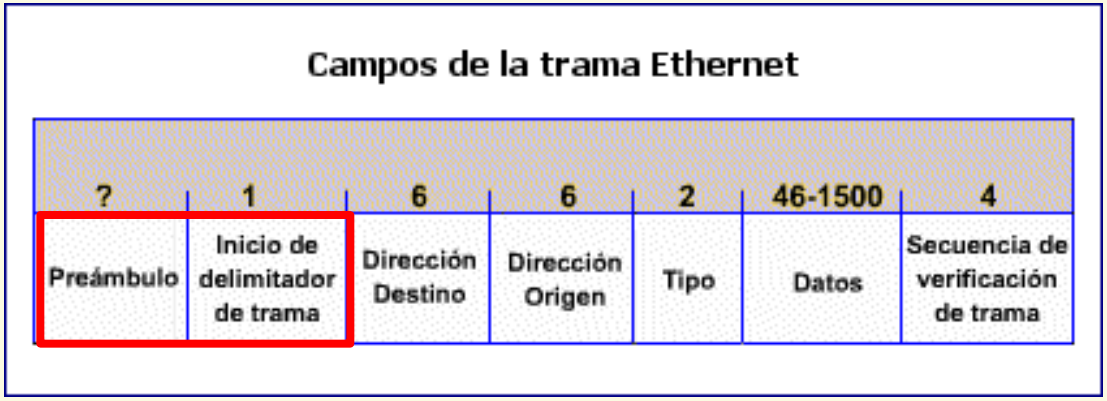
  Ejemplo: 01:A3:EF:34:18:A5

- Los primeros 3 bytes son propios de cada fabricante

3. Trama MAC


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

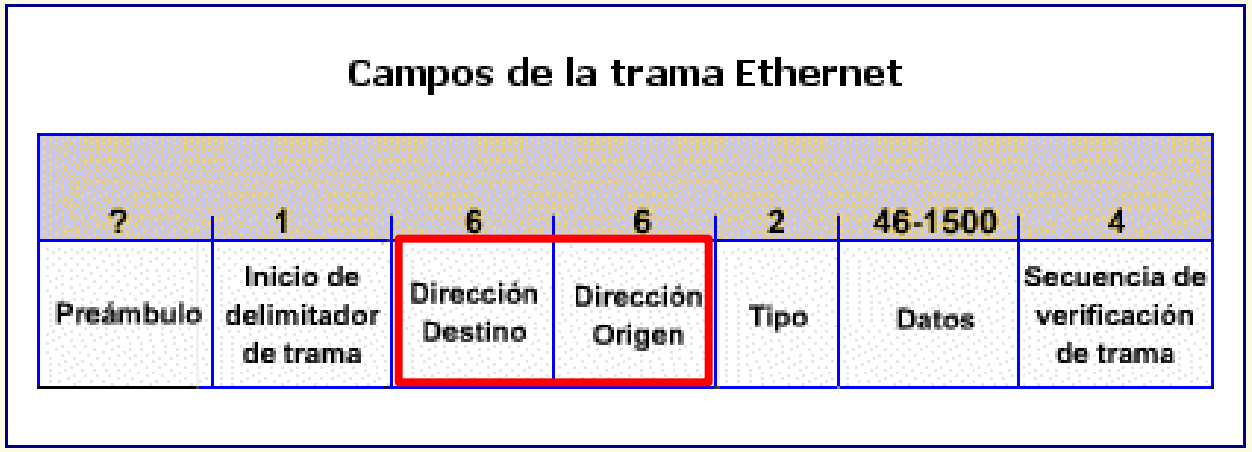
3. Trama MAC



PREÁMBULO: Serie de 0 y 1 alternos para sincronizarse con el receptor.

INICIO DE TRAMA: Comienzo de la trama. El emisor indica con esto que lo que va a continuación ya no es el preámbulo sino una trama nueva.

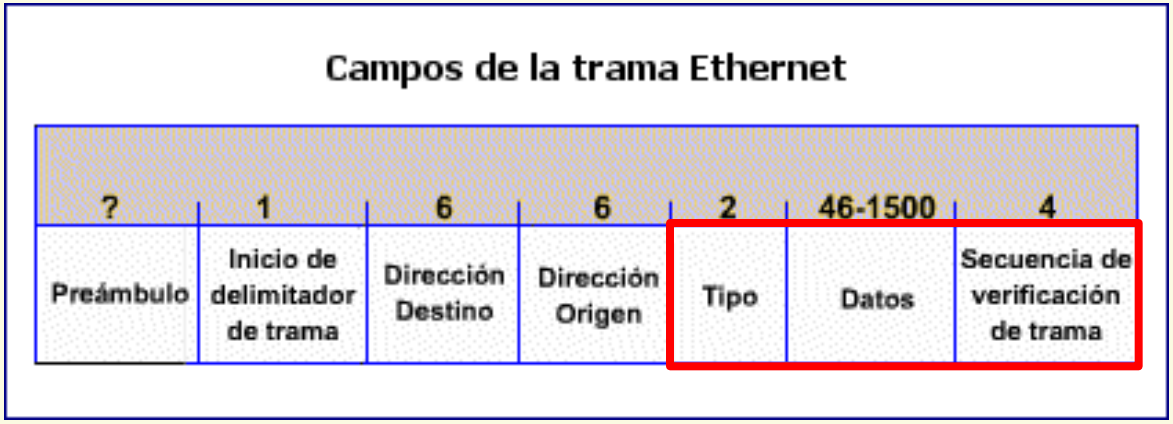
3. Trama MAC



DIRECCIÓN DESTINO: Dirección MAC de la máquina destino

DIRECCIÓN ORIGEN: Dirección MAC de la máquina origen

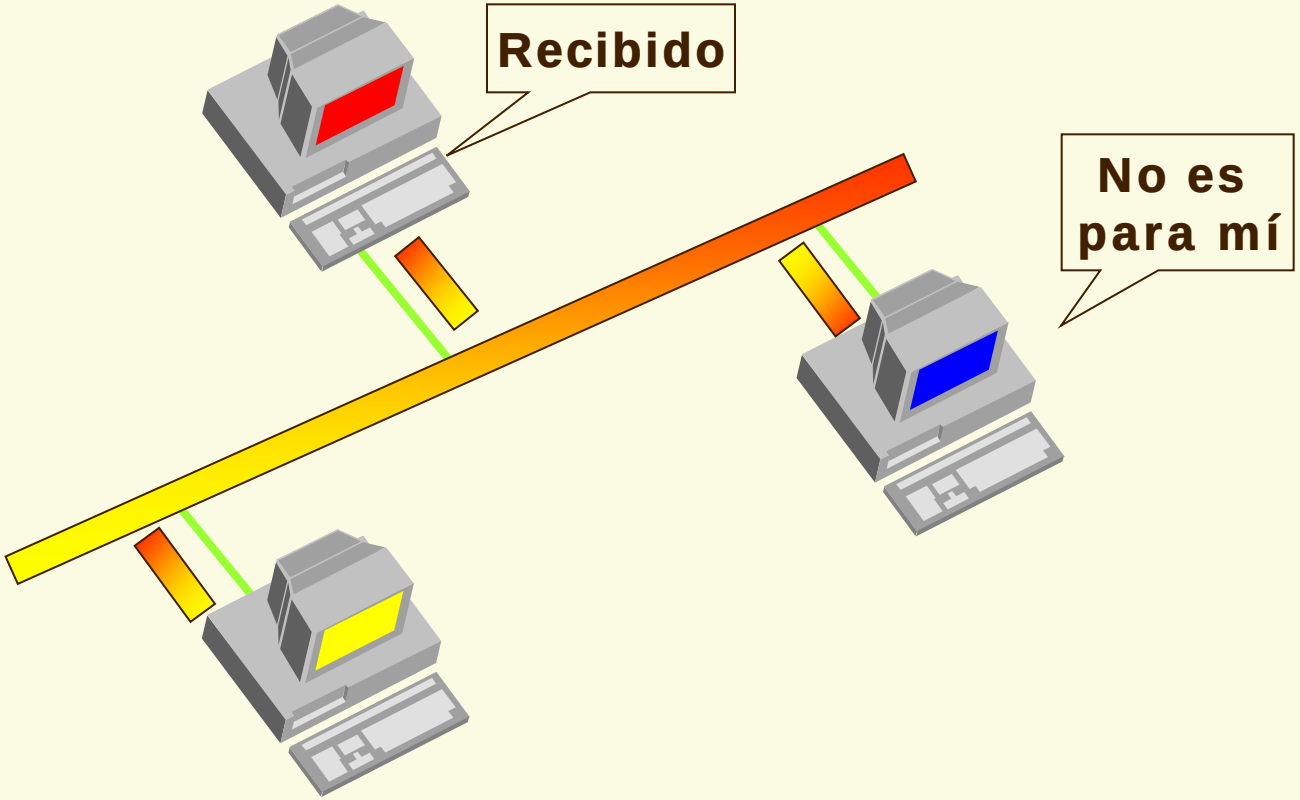
3. Trama MAC



TIPO: Según el estándar 802.3, si el valor es menor o igual que 1500 es la longitud del campo Datos. Sino indica el protocolo de tercer nivel contenido en Datos (p.e. IP)
DATOS: Datos pasados por el nivel superior.
Mínimo de 46 bytes
SECUENCIA DE VERIFICACIÓN DE TRAMA (CRC).
Se calcula con Origen, Destino, Tipo y Datos.

4. Introducción al análisis del tráfico en la red

A nivel de enlace se controla también el acceso al medio ya que este es compartido:

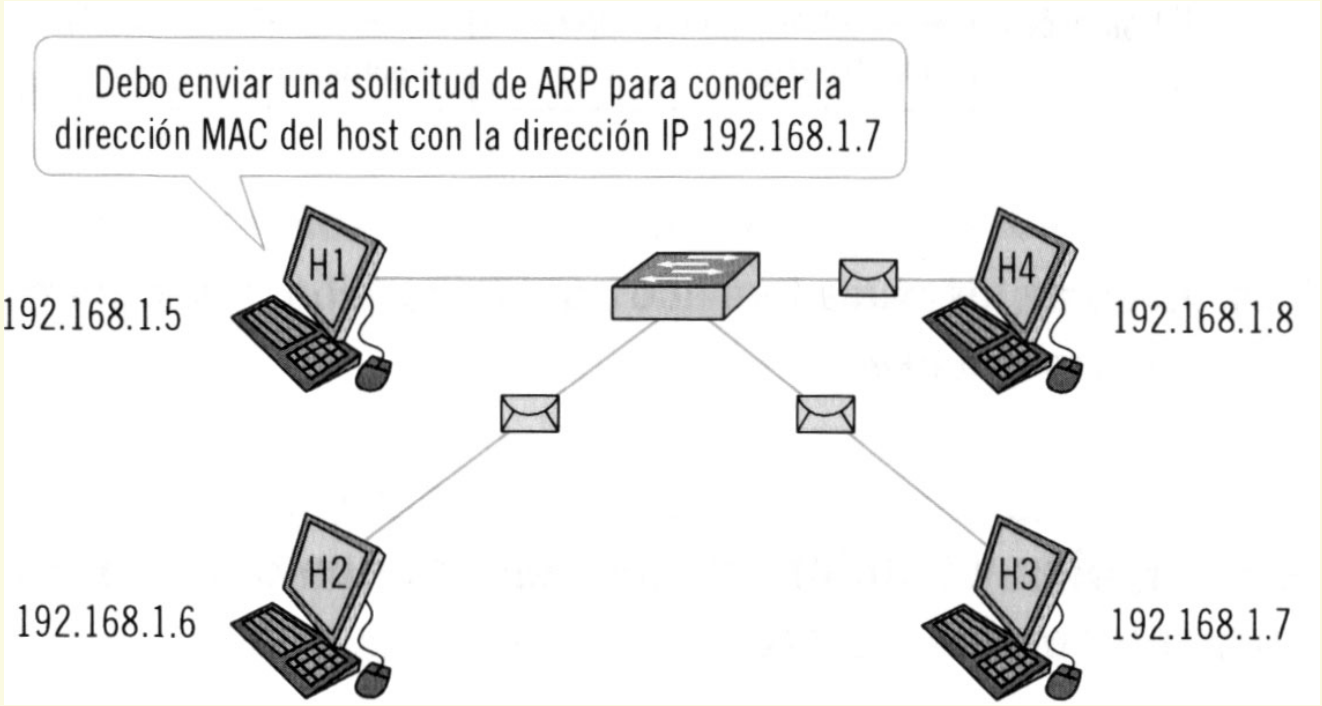


5. ARP, RARP

- **A**ddress **R**esolution **P**rotocol - Protocolo de resolución de direcciones.
- Es un protocolo de nivel de red responsable de encontrar la dirección hardware (MAC) que corresponde a una determinada dirección IP
- Las MAC se obtienen enviando mensajes de broadcast a todos los dispositivos de la red.
- La trama contiene un paquete de solicitud ARP con la dirección IP del host de destino.
- El nodo que recibe la trama y que identifica la dirección IP como suya responde enviando un paquete de respuesta de ARP al emisor como una trama unicast.
- Esta respuesta se utiliza para crear una entrada nueva en la tabla ARP

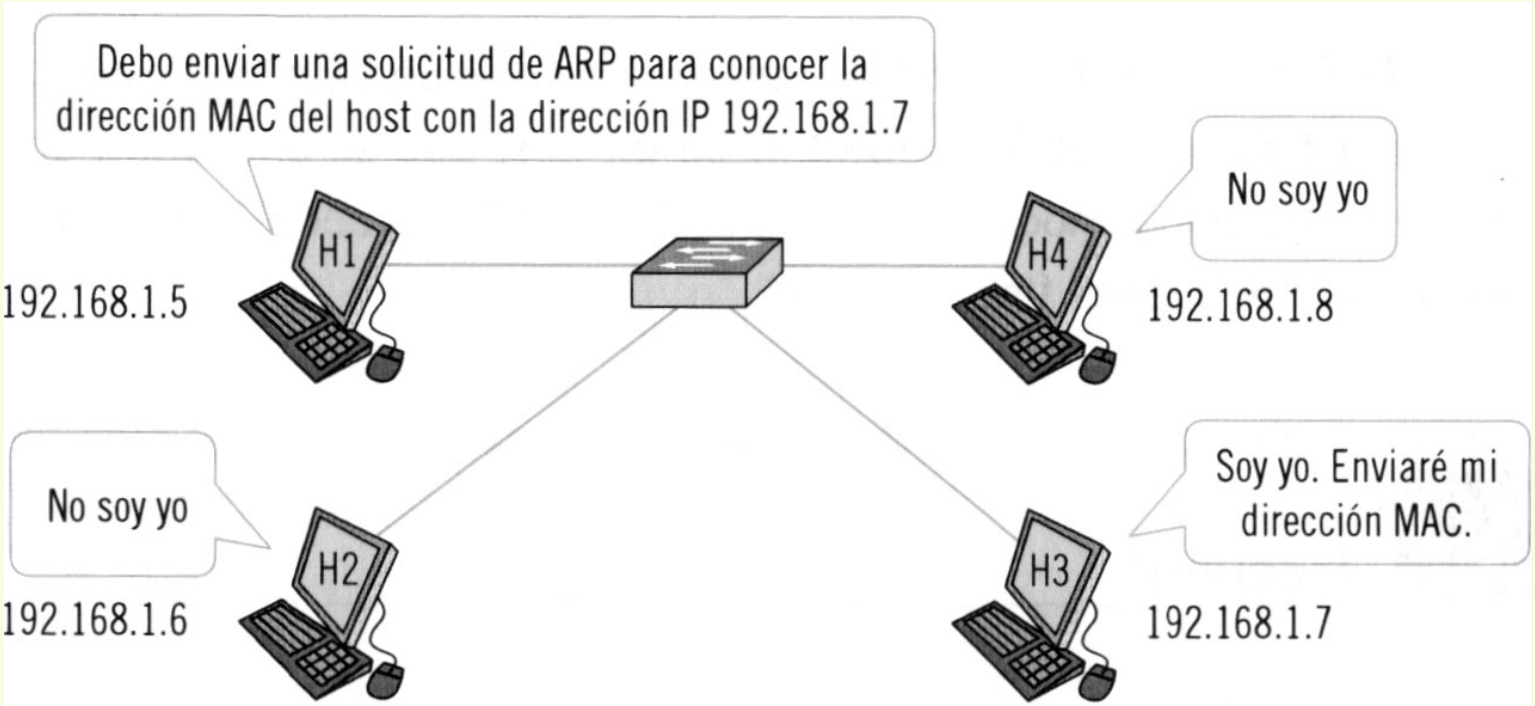
5. ARP, RARP

1. El host emisor crea una trama dirigida a una dirección MAC de broadcast y la envía. Esta trama contiene un mensaje con la dirección IP del host de destino que se desea encontrar



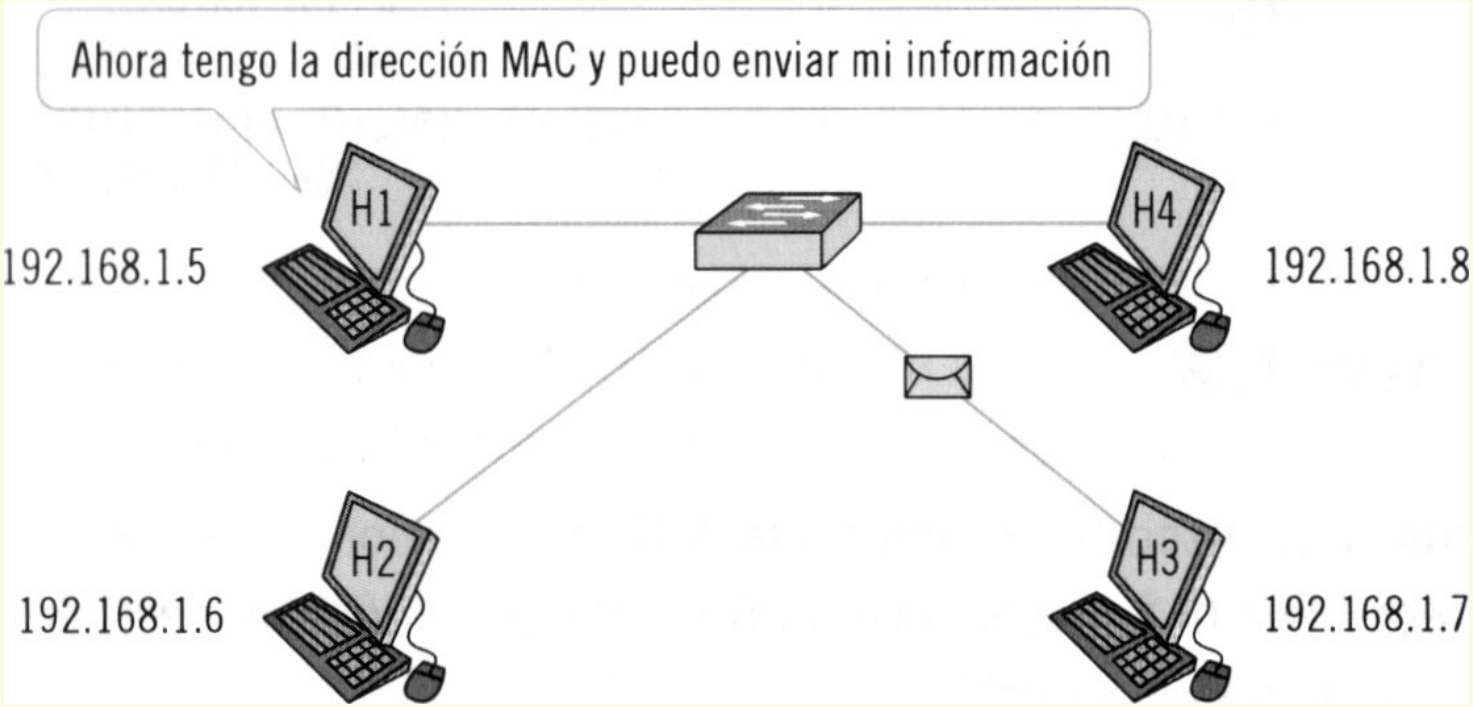
5. ARP, RARP

2. Cada host de la red recibe la trama de broadcast. Compara su dirección IP con la de la trama. En el caso de que coincida envía su dirección MAC al host emisor original



5. ARP, RARP

3. El host emisor recibe el mensaje y actualiza su tabla ARP con la IP y la MAC recibida. Ahora ya puede enviar tramas directas al destino



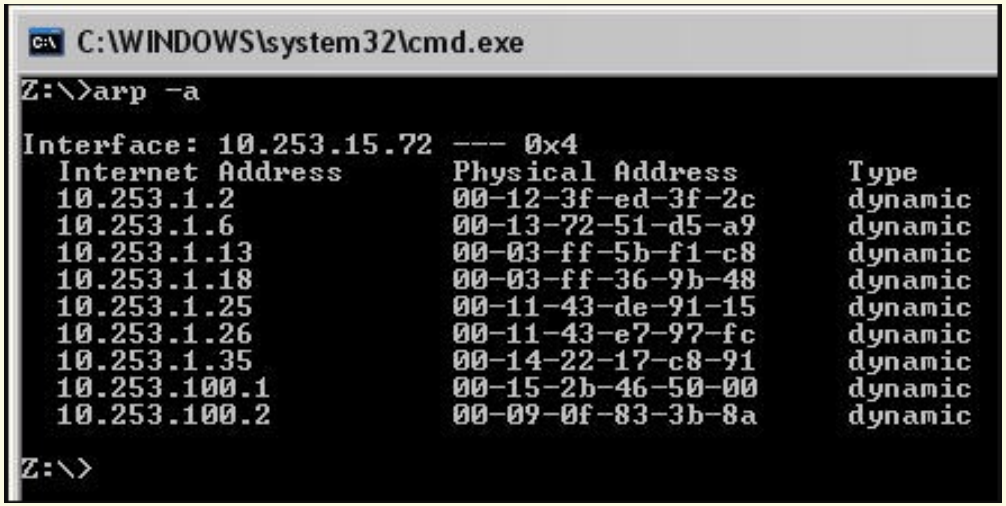
5. ARP, RARP

Tabla ARP	
Dirección IP	**Dirección física**
212.5.26.1	26-5A-C5-42-FD-11
212.5.26.2	2C-2A-48-A6-36-00
212.5.26.3	5D-F1-80-02-A7-93

La información se va guardando en las tablas ARP que se puede consultar:
-Linux → arp –n
-Windows → arp –a

Las entradas de estas tablas se borran cada cierto tiempo.

5. ARP, RARP

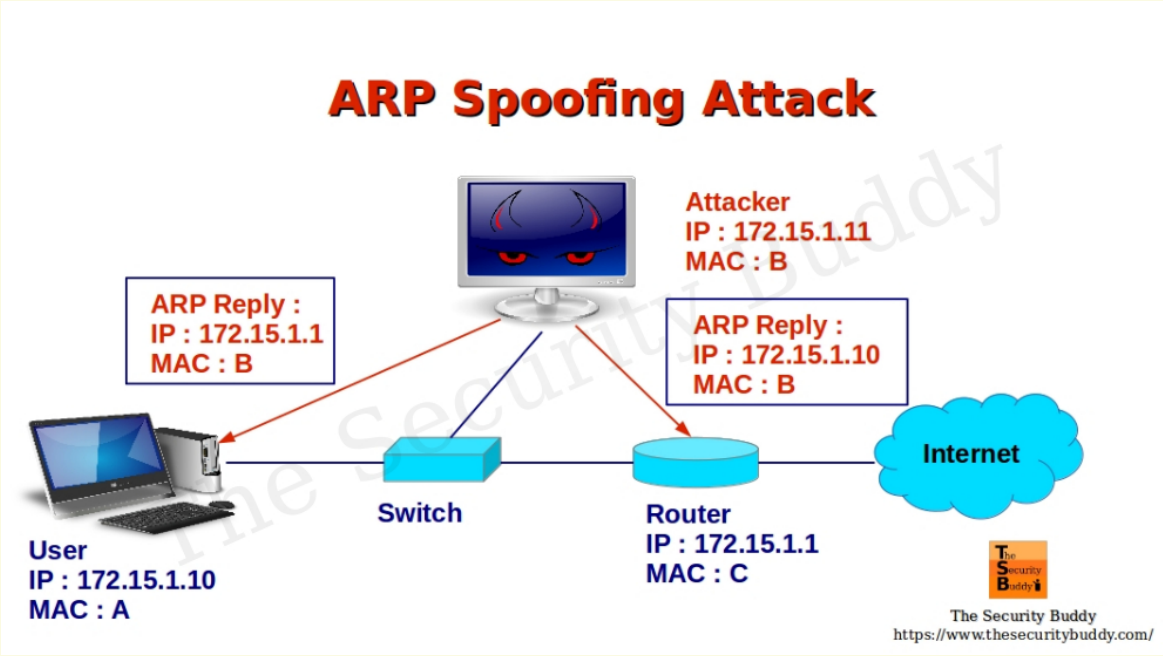



```
root@kali3:~# arp -a -n
? (192.168.50.15) auf 52:54:00:74:60:4a [ether] auf eth0
? (192.168.50.14) auf 52:54:00:74:60:4a [ether] auf eth0
? (192.168.50.1) auf f6:8e:e2:25:0d:b8 [ether] auf eth0
root@kali3:~#
```

5. ARP, RARP

Problema 1: Sobrecarga del medio si varios equipos se conectan a la red a la vez y envían broadcasts de ARP iniciales. El impacto se minimizará cuando aprendan las direcciones.

Problema 2: Seguridad. ARP Spoofing



5. ARP, RARP

RARP (Reverse Address Resolution Protocol)
Protocolo de resolución de direcciones inverso.

Es un protocolo de nivel de red responsable de encontrar la dirección IP dada una dirección hardware (MAC)

Apenas se utiliza actualmente por ser muy limitado y por estar superado por otros protocolos más potentes.

Ejemplo de uso: máquinas sin discos duro que deben comunicarse con un servidor para conocer su dirección IP.

6. Tarjeta de red

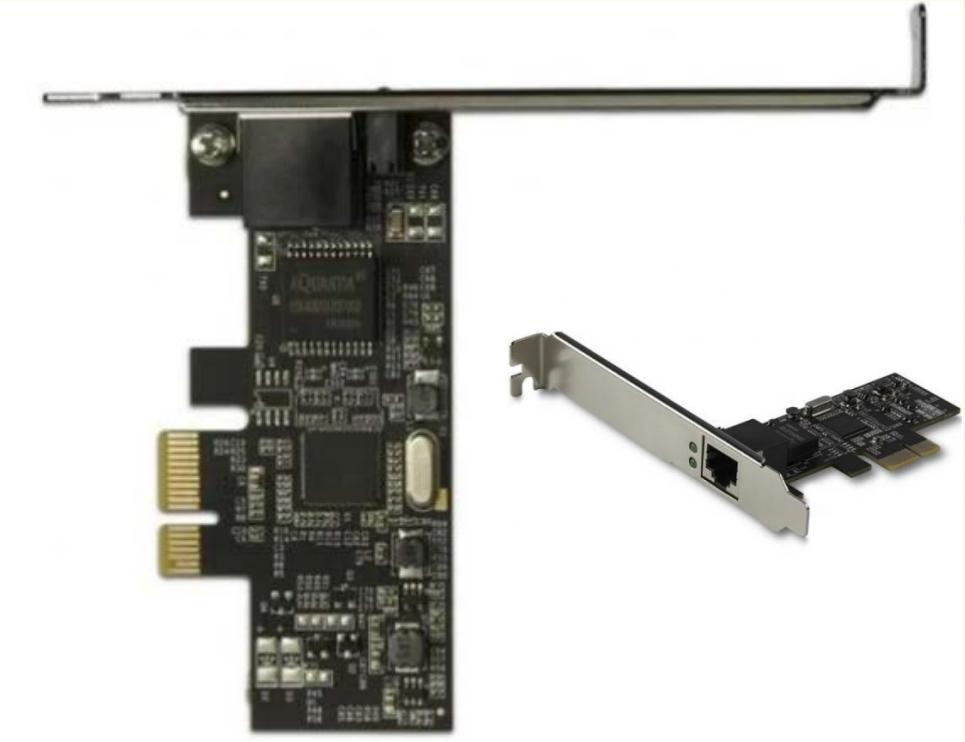
- También denominada NIC (Network Interface Card)
- Realiza la función de intermediaria entre el ordenador y la red de comunicación.
- En ella se encuentran grabados los protocolos de nivel físico, enlace y red.
- Conectado a la placa base a través de ranuras de expansión (PCIe)

6. Tarjeta de red

Pasos que sigue la tarjeta de red para transmitir la información:

- Determinar velocidad de transmisión, la longitud del bloque de información, ... de la configuración establecida en el sistema
- Convertir el flujo de bits en paralelo a secuencia en serie
- Codificar la secuencia de bits en serie formando una señal eléctrica adecuada

6. Tarjeta de red



7. Dispositivos de conexión

6.1 Repetidor (repeater) y concentrador (hub)

- Trabajan solo a nivel físico
- Su función es recibir una señal y devolverla reconstruida, pero sin ningún análisis ni proceso de datos
- Se diferencian principalmente en el número de puertos, mayor en el caso de los hubs
- No necesitan configuración

7. Dispositivos de conexión

6.2 Switch

- Funciona como un hub pero distinguiendo qué direcciones MAC se alcanzan por cada puerto.
- Une segmentos de red con los mismos protocolos a nivel físico y de enlace.
- Guarda esta información en una tabla.
- Puertos: RJ45, fibra

7. Dispositivos de conexión

6.2 Switch

- En un switch hay dos partes diferenciadas:
  - Backplane: el hardware que comunica los puertos
  - Frontplane: los puertos

- Switches gestionables: se pueden administrar a través de la red. Se accede a ellos mediante una IP (telnet, SSH, web)
  VLANs, bloqueo de puertos, ...

- Velocidad de los puertos

- Half Duplex vs Full Duplex

7. Dispositivos de conexión

6.2 Switch

- Modos de reenvío o conmutación de información:
  - Cut-through: reenvía tan pronto como recibe la dirección MAC de destino. No detecta errores en CRC.
  - Store and forward: recibe toda la trama antes de reenviarla. Detecta errores pero necesita más tiempo de proceso.
  - Adaptative switching: diseñado para funcionar en cut-through, si la tasa de error es alta pasa a store and forward.

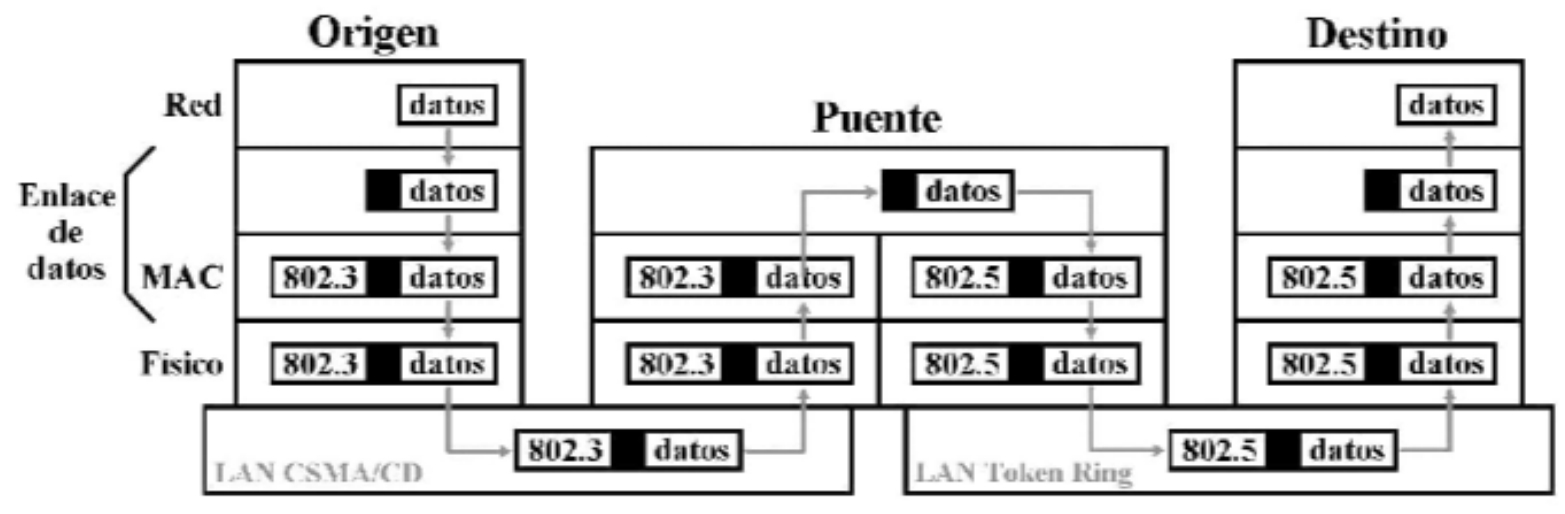
7. Dispositivos de conexión

6.3 Puente (Bridge)

- Funciona a nivel de enlace
- Permite la conexión de distintos segmentos de red
- Estos segmentos de red pueden ser de distinta topología (ej: Ethernet y Token Ring) y distinto protocolo

7. Dispositivos de conexión

6.3 Puente (Bridge)



Ej: puente de 802.3 a 802.5. Su objetivo es adaptar los formatos de tramas de ambas redes

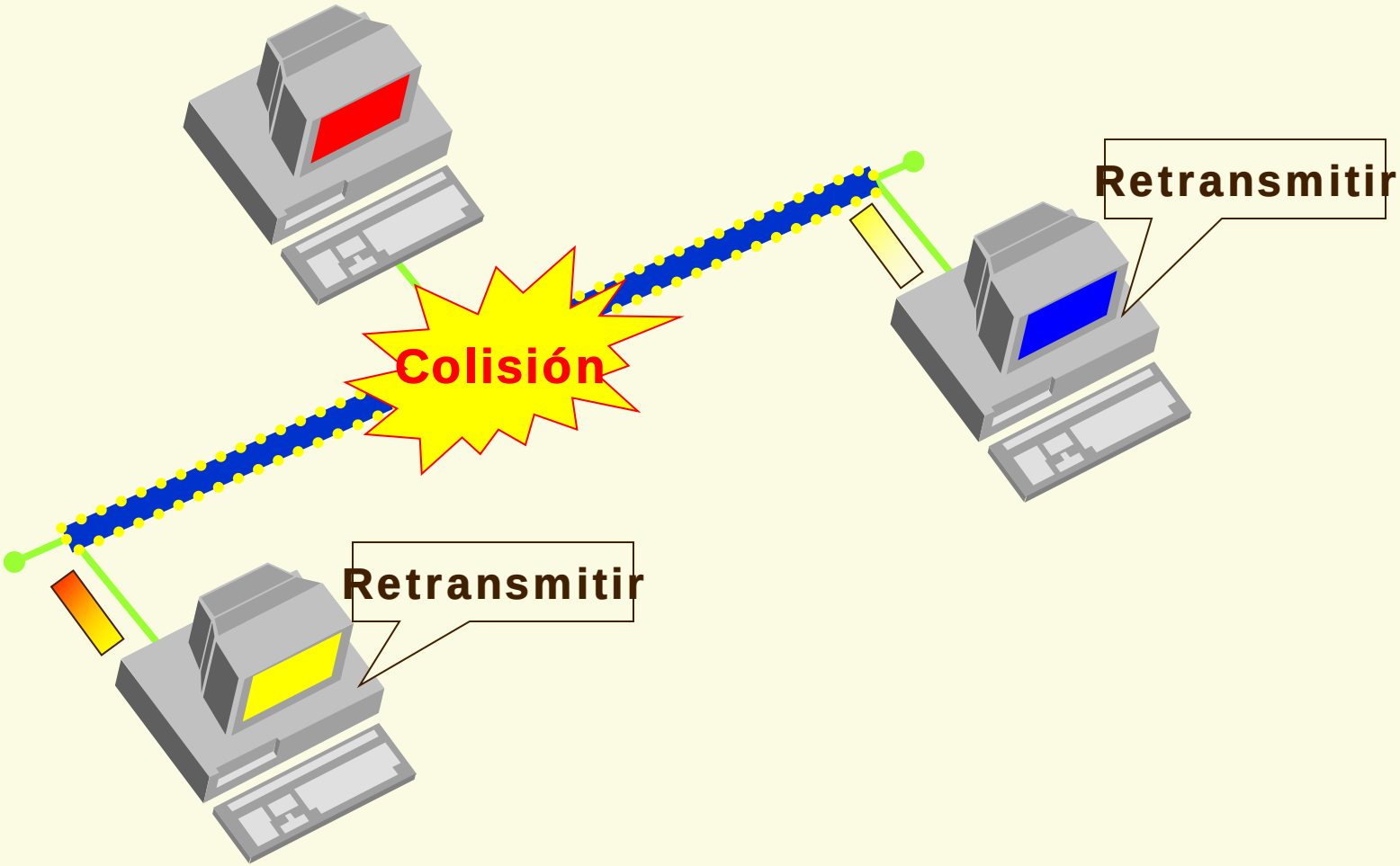
8. Segmentación de la red. Dominios de colisión

Al aumentar el número de estaciones en una red aumenta también el tráfico de red.

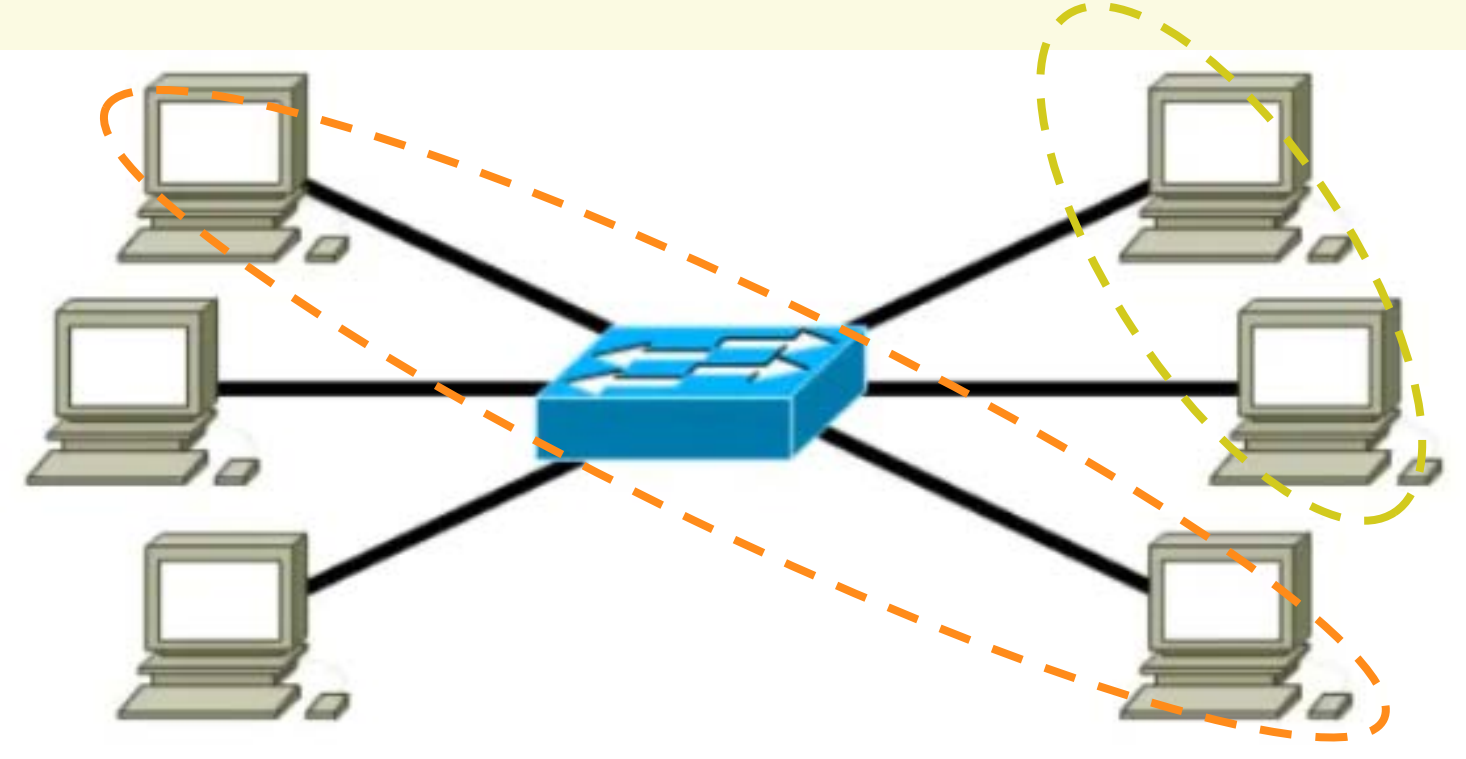
Cada estación debe esperar más tiempo si quiere transmitir o se producirá un mayor número de colisiones.

En estas condiciones es mejor segmentar la red mediante conmutadores para evitar que dichas colisiones disminuyan mucho el rendimiento

8. Segmentación de la red. Dominios de colisión



8. Segmentación de la red. Dominios de colisión



8. Segmentación de la red. Dominios de colisión

Razones para segmentar la red y crear distintos dominios de colisión:

- Aislar el tráfico entre segmentos → Seguridad
- Lograr mayor ancho de banda, lo que se consigue con dominios de colisión más pequeños.

  Menos colisiones → Menos retransmisiones → Mayor ancho de banda

9. Riesgos asociados al nivel de enlace

El nivel 2 es muy inseguro. En su momento nadie pensó que se pudieran espiar las comunicaciones o suplantar a alguien.

- Sniffing o captura de tráfico
- Inundación ARP o en general, ataques ARP
- Posibilidad de suplantación (man in the middle)
- Usar switch para aislar dominios y que no haya demasiadas colisiones
- Clonación MAC
- Riesgo DHCP: configuración de red falsa