Ya sé analizar pero... ¿dónde capturo?

¡¡Depende!!

- Del medio
  - Red compartida (hubs)
  - Red conmutada (switches)
  - Red wireless
- Objetivo
  - Monitorizar toda la red
  - Monitorizar equipo/s
    - Tráfico desde inicio
    - Tráfico una vez arrancado
- Diversas técnicas y ubicaciones:
  - Wireshark en el equipo
  - Hubbing
  - Machine-in-the-middle
  - Port mirroring/span
  - Network tap

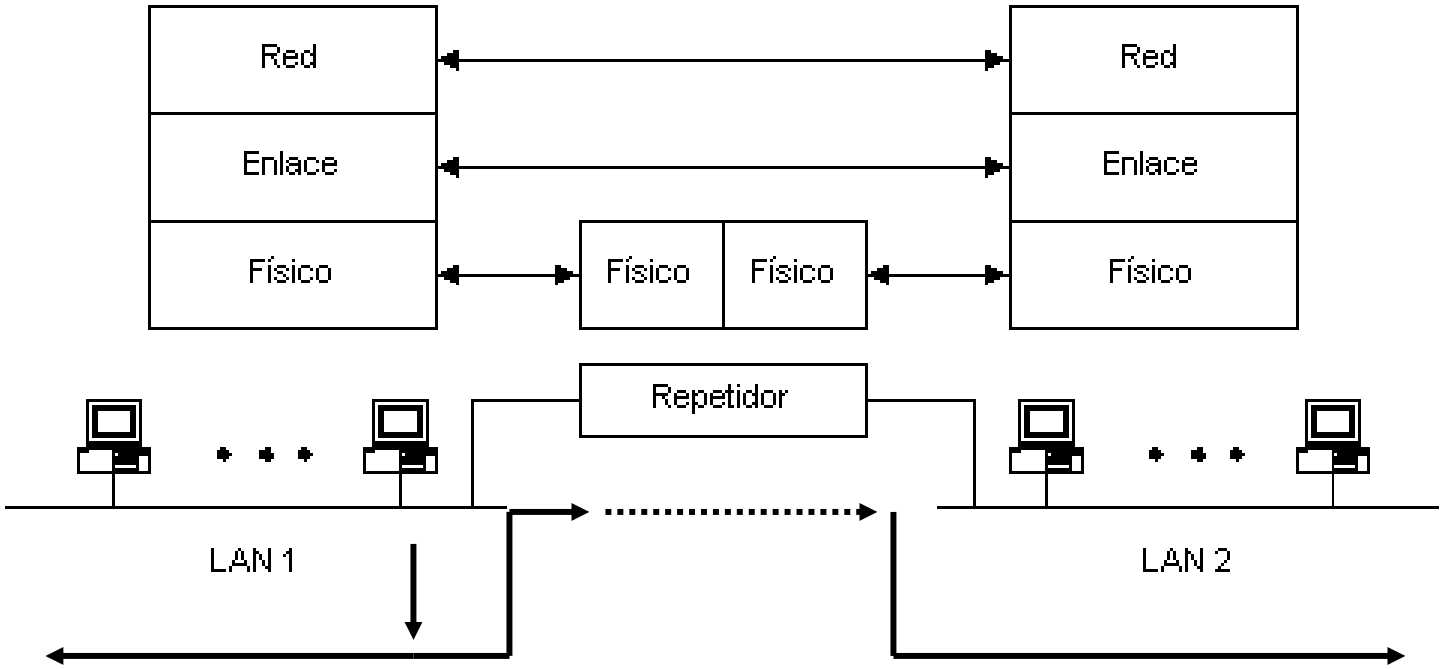
https://youtu.be/Z91RV6xYb8k

Sniffing en redes compartidas: Concentradores/Hubs

- Funcionan a nivel físico.
- Retransmisión de la señal bit a bit.

- señal digital → repetidor
- señal analógica → amplificador

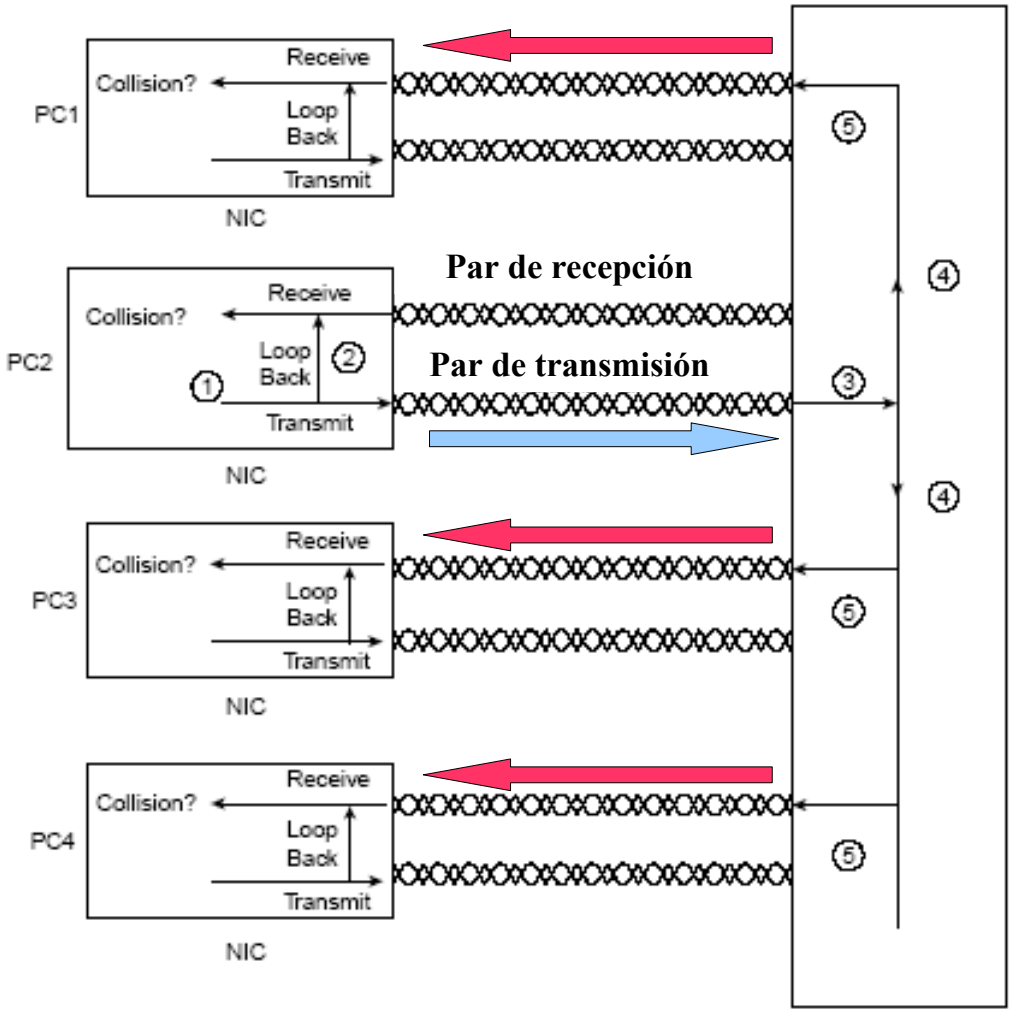
- Permiten que las señales a nivel físico generadas por un host de un segmento (LAN 1) se propaguen al otro segmento (LAN 2).
- Se encargan de regenerar las señales eléctricas, amplificarlas, eliminar ruidos, etc.

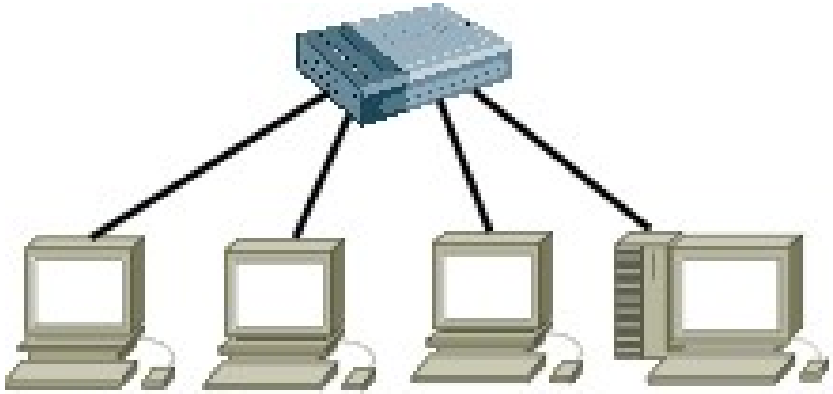


↳ Al operar a nivel físico no entienden de direcciones MAC ni direcciones IP ni de protocolos de niveles superiores.

Sniffing en redes compartidas: Hubs

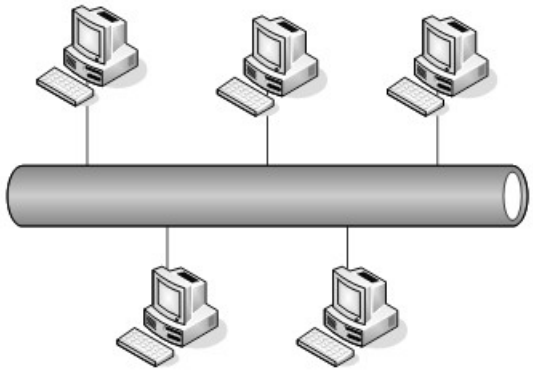
Repetidores multipuerta que aparecieron con el estándar 10BaseT.





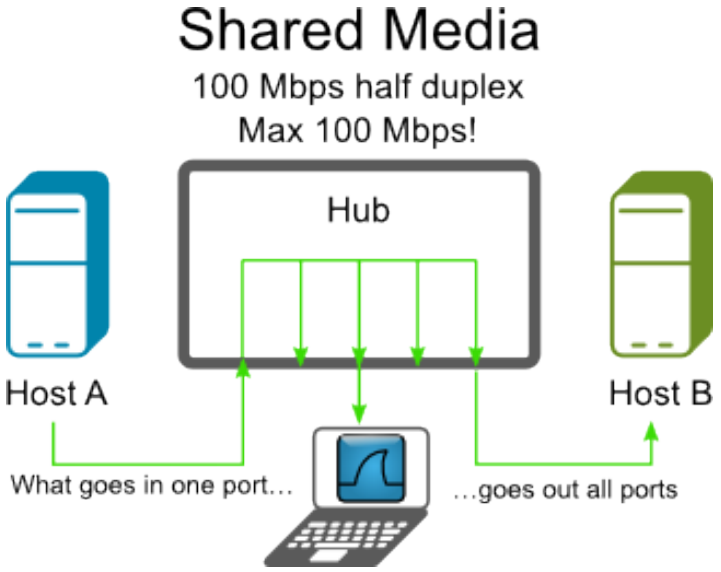
A pesar de la topología en estrella, recrean la estructura de BUS, y se mantiene:

- CSMA/CD.
- Detección de colisiones.
- Half-dúplex.



PC2 envía trama a PC3 → PC1 y PC4 también reciben el paquete

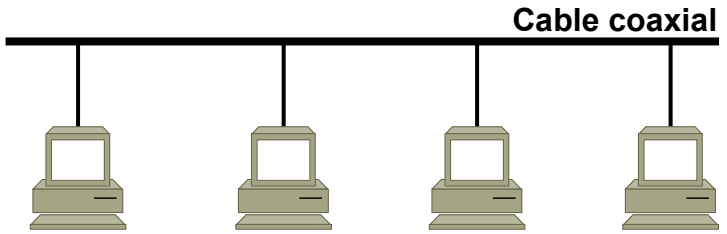
Sniffing en redes compartidas: Hubs



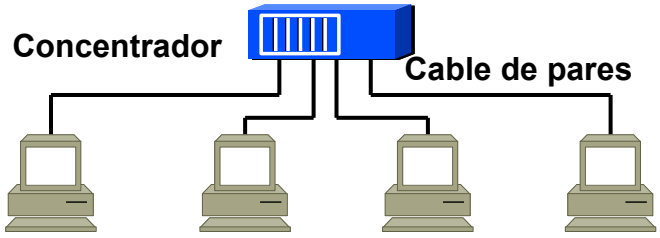
Muy bonito pero …

Evolución histórica de una red local Ethernet

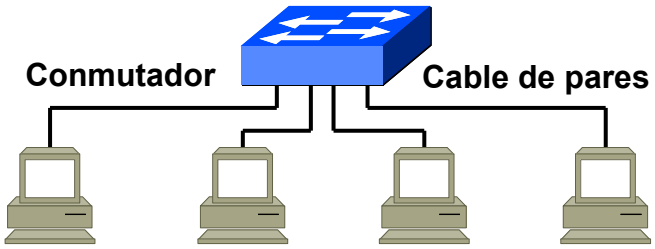
Fase 1 (1988):
Medio compartido (10 Mb/s) con cable coaxial en topología de bus.



Fase 2 (1992):
Medio compartido (10 Mb/s) con:
- cable de pares (cableado estructurado)
- concentradores (hubs) en topología de estrella



Fase 3 (1996):
Medio dedicado (10 Mb/s) con:
- cable de pares
- conmutadores en topología de estrella



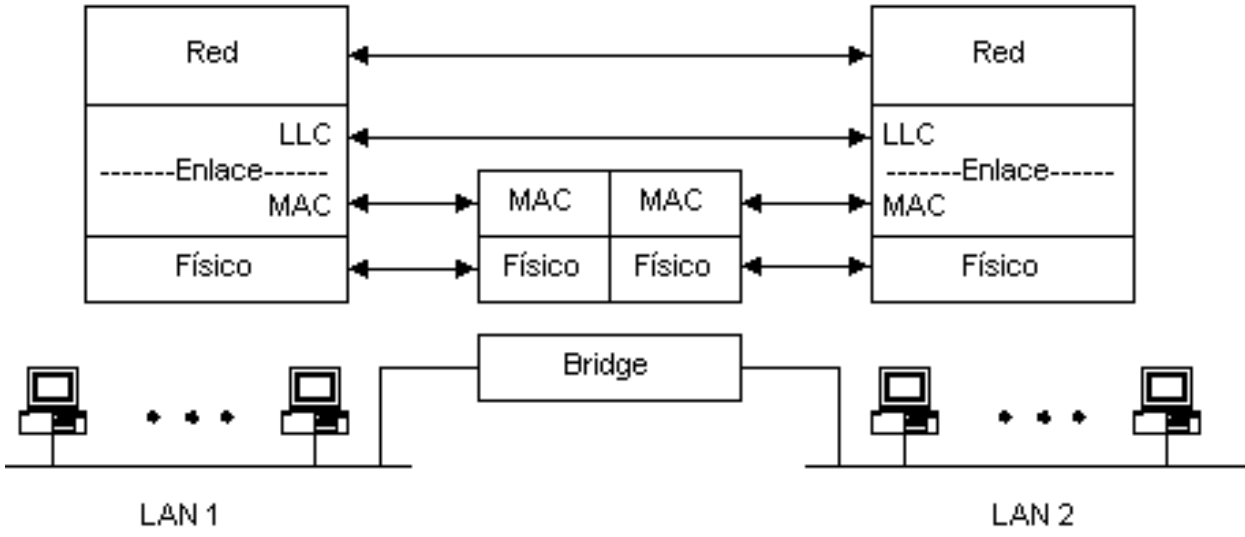
Puentes/Bridges/Conmutadores/Switches

- Funcionan en el nivel de enlace (principalmente en la subcapa MAC).

- El funcionamiento básico de un puente se basa en tres puntos:
  1. Las tramas son almacenadas.
  2. Se chequean para verificar si hay errores.
  3. Se reenvían las tramas que:
     - están libres de errores y ...
     - ... y están destinados a equipos pertenecientes a un segmento de red diferente al que envía la información.

Reenvío → MAC destino

Aprendizaje → MAC origen.



Puentes transparentes, switches

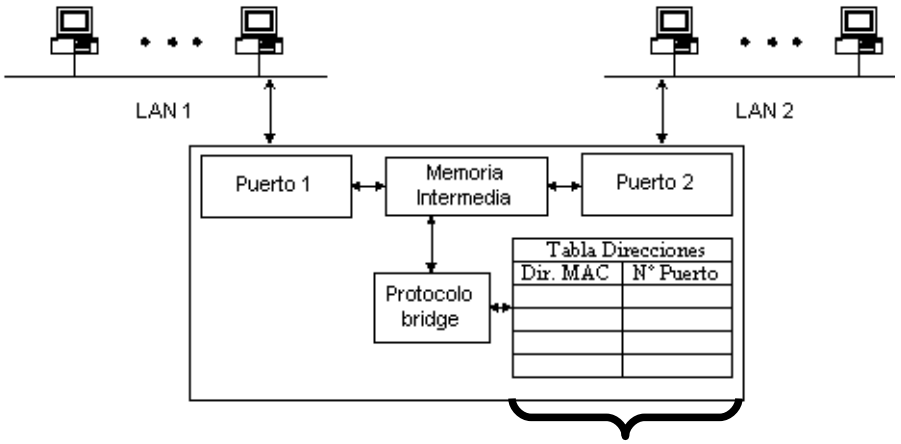


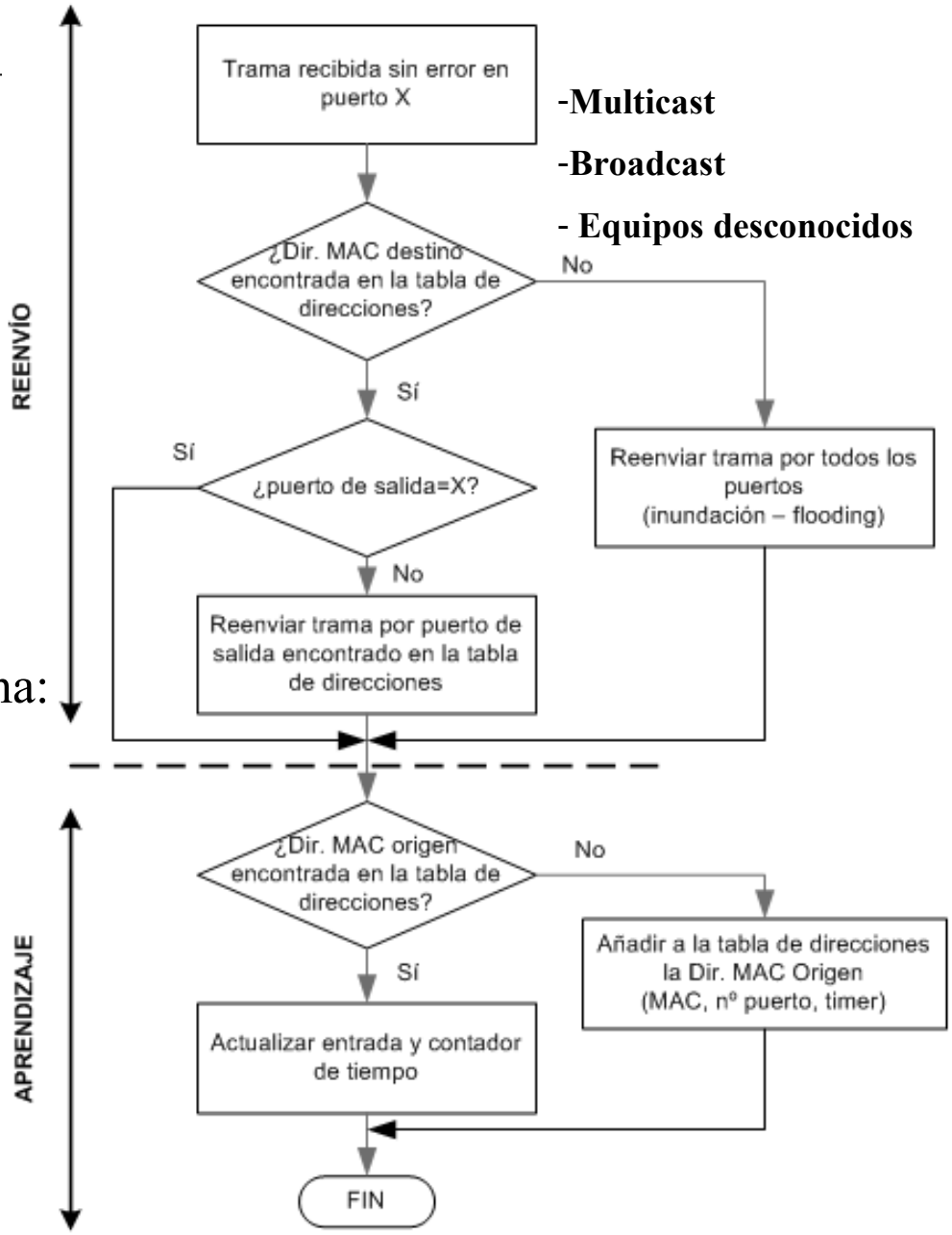
Tabla de direcciones → reenvío selectivo de las tramas

El puente analiza las Dir. MAC de la trama:

- **MAC Destino → decisión de reenvío**
- **MAC Origen → aprendizaje**

Puente transparente: los hosts conectados no son conscientes de la presencia del puente.

Normalmente actúan como dispositivos 'plug and play' al no necesitar ninguna configuración para funcionar.



Puentes transparentes, switches

- **Ordenador tímido (no emite tramas):**
  - Al no poder ser localizado, el puente enviará por todos los puertos las tramas destinadas a ese equipo.
  - No es probable que un ordenador que recibe tráfico no responda, por lo que antes o después se aprenderá su ubicación.
- **Tramas Multicast/Broadcast:**
  - Siempre son **retransmitidas por todas las interfaces** (puede haber destinarios en cualquier parte).
  - Nunca se almacenan en las tablas de direcciones de los puentes.
- **Tabla de Direcciones dinámica:**
  - Para **adaptarse a los cambios de la red** (cambios en la ubicación de los equipos), las entradas de la tabla de direcciones se eliminan al cabo de unos minutos si la dirección correspondiente no envía ninguna trama.

Tabla de direcciones
Tabla de direcciones MAC
Forwarding Database

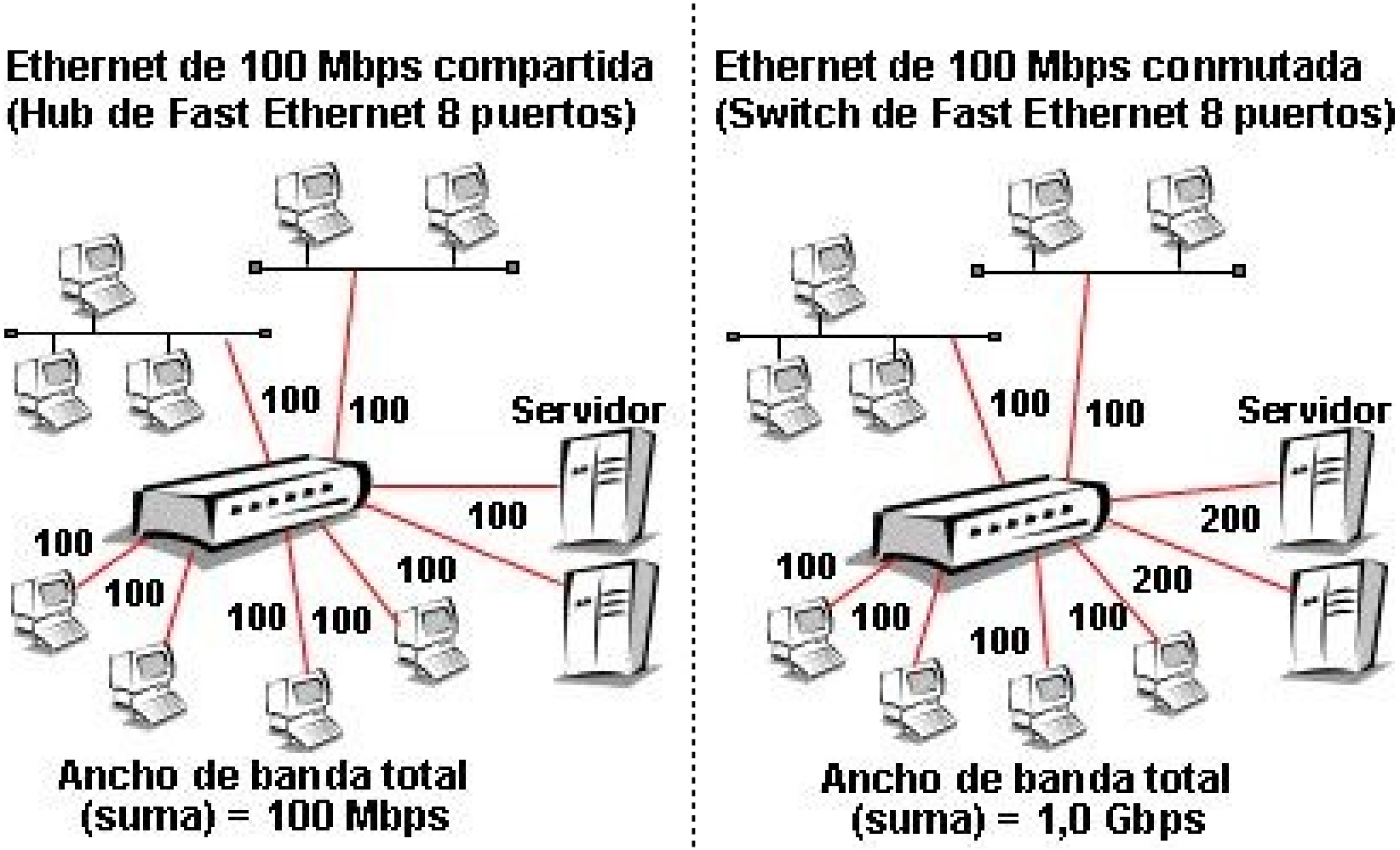
```
switch#show mac-address-table dynamic
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   1    0007.8580.71b8    DYNAMIC     Fa0/5
   1    0007.8580.7208    DYNAMIC     Fa0/8
   1    0007.8580.7312    DYNAMIC     Fa0/13
```

El administrador de la red puede crear entradas estáticas que no caducan

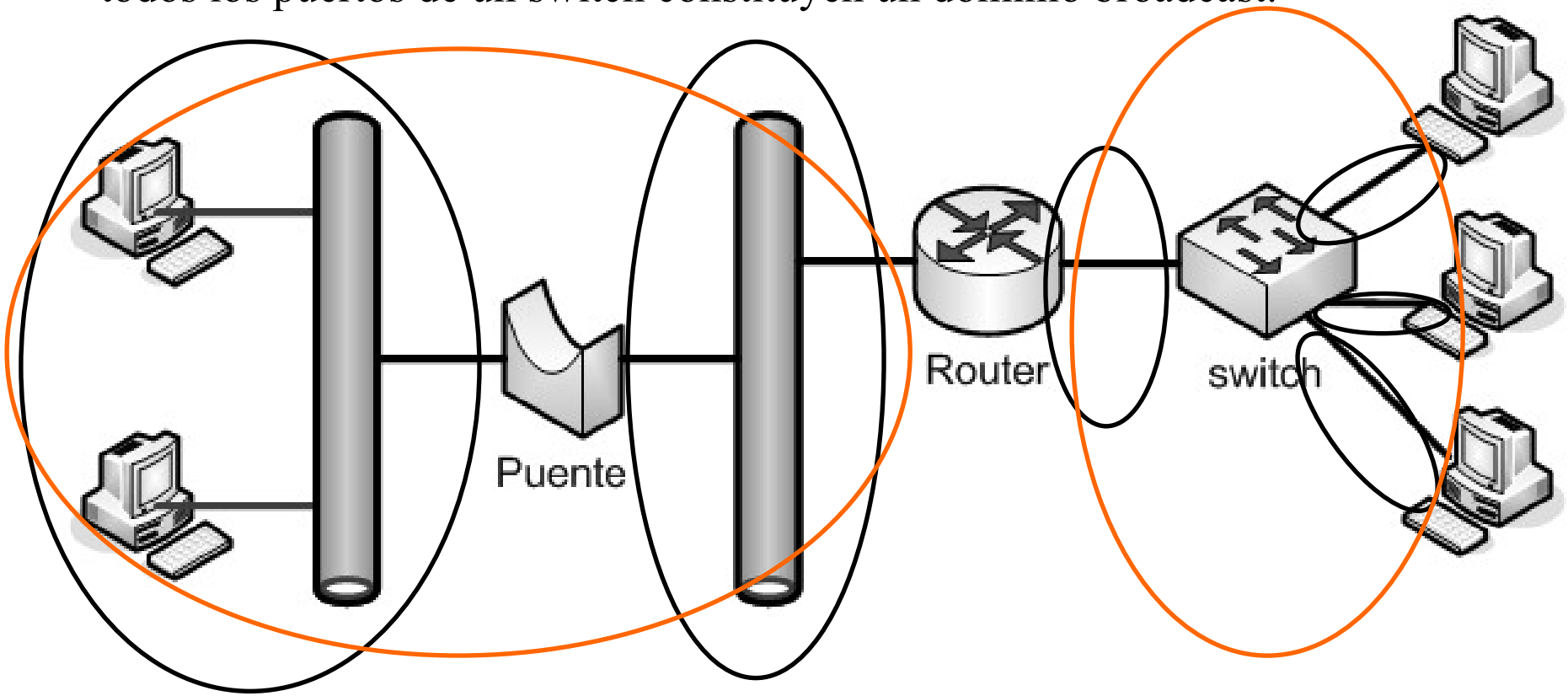
LAN Conmutadas: Switches

- Cada puerto es un Dominio de Colisiones independiente.
- El switch proporciona un ancho de banda dedicado por puerto.



Dominios de Colisión/Broadcast

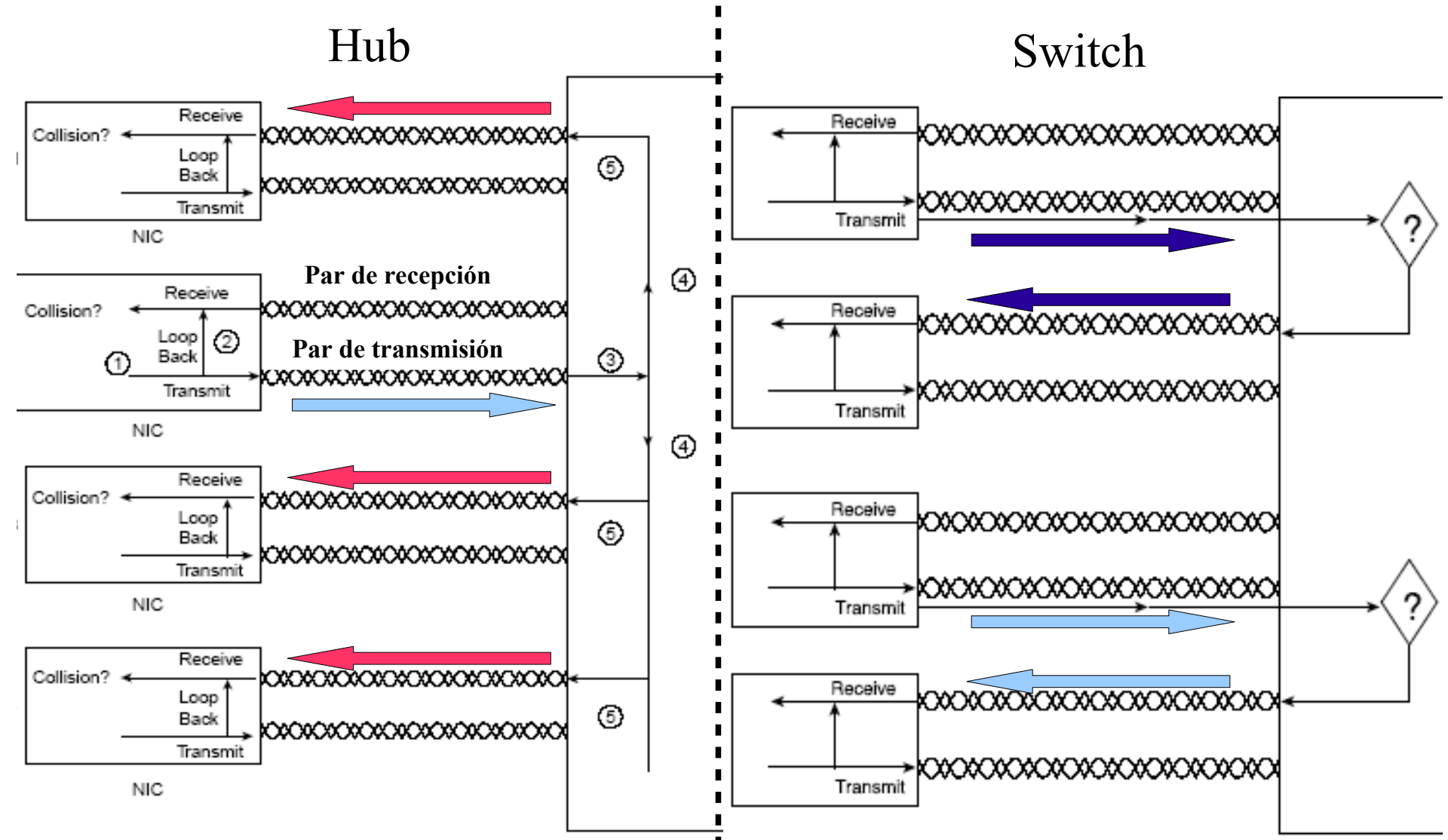
- cada puerto de un switch es un dominio de colisión independiente
- todos los puertos de un switch constituyen un dominio broadcast.



Dominio de Colisión: conjunto de NICs para los que una trama enviada por una de ellas puede resultar en una colisión.

Dominio Broadcast: conjunto de NICs para las que una trama broadcast enviada por una de ellas es escuchada por todas las otras.

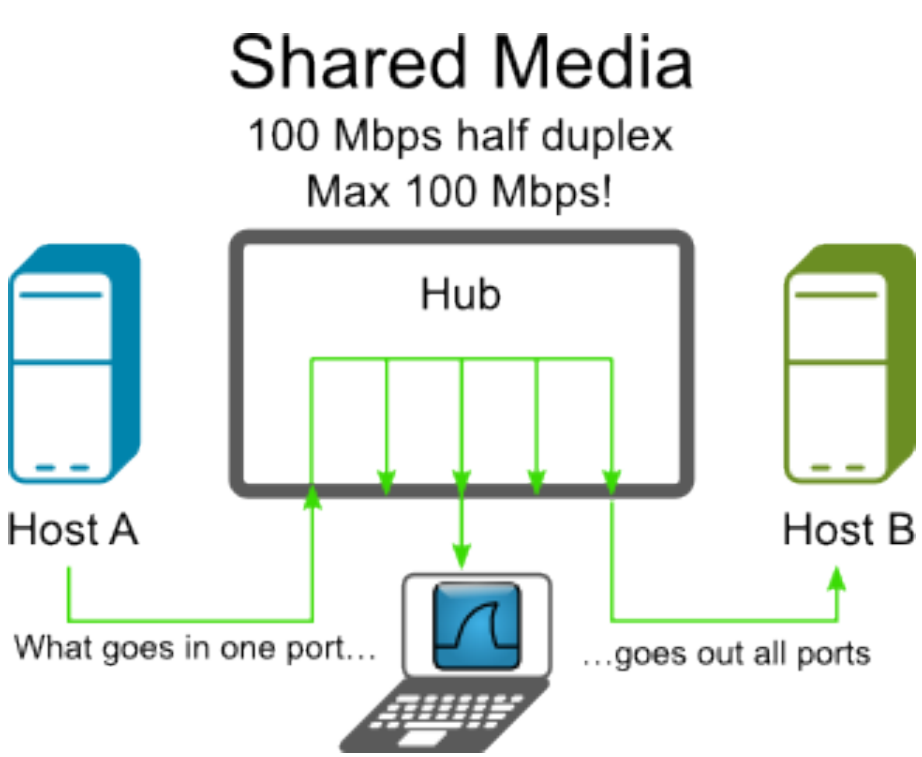
Conmutación en redes Ethernet: Full-Dúplex



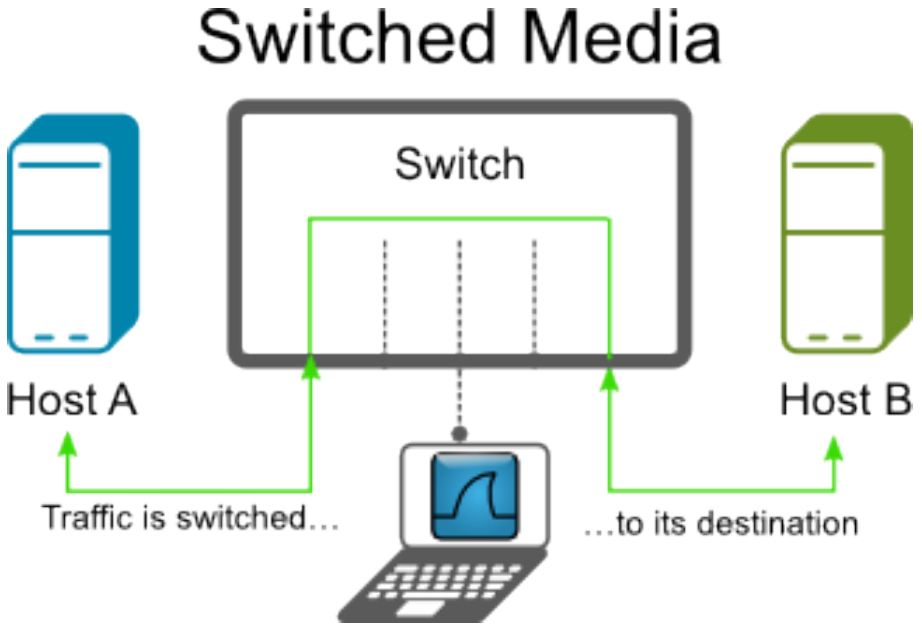
- medio compartido
- half-dúplex

- medio dedicado (no compartido)
- full-dúplex

Compartido frente conmutado



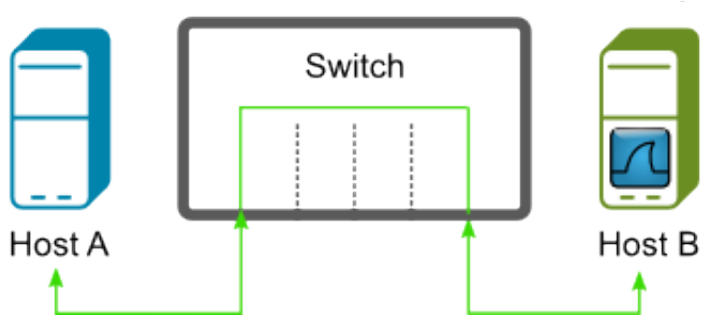
- todo el tráfico



- tráfico broadcast
- tráfico multicast
- tráfico desde/hacia mi equipo
- tráfico a equipos desconocidos

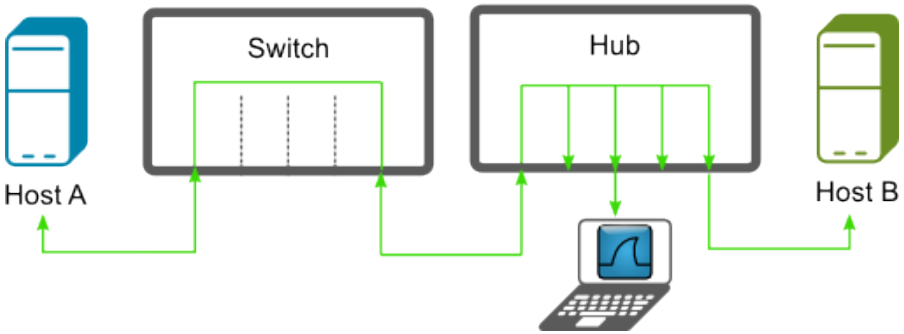
¿y ahora que hago?

Solución#1: sniffing en el propio equipo



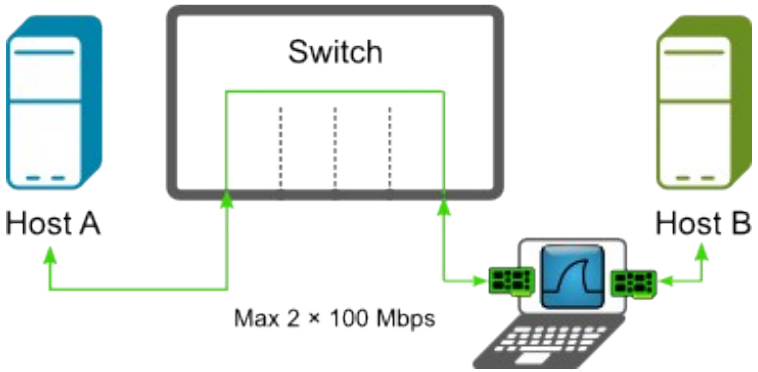
- Ventaja: fácil de implementar
- Desventaja: se pierde el resto del tráfico

Solución#2: hubbing



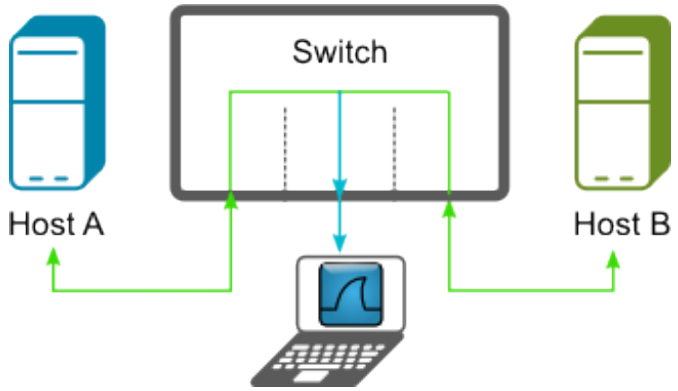
- Ventaja: fácil de implementar
- Desventaja:
  - Difícil encontrar hub
  - Desactiva el modo full-duplex

Solución#3: Machine-in-the-middle (modo bridge)

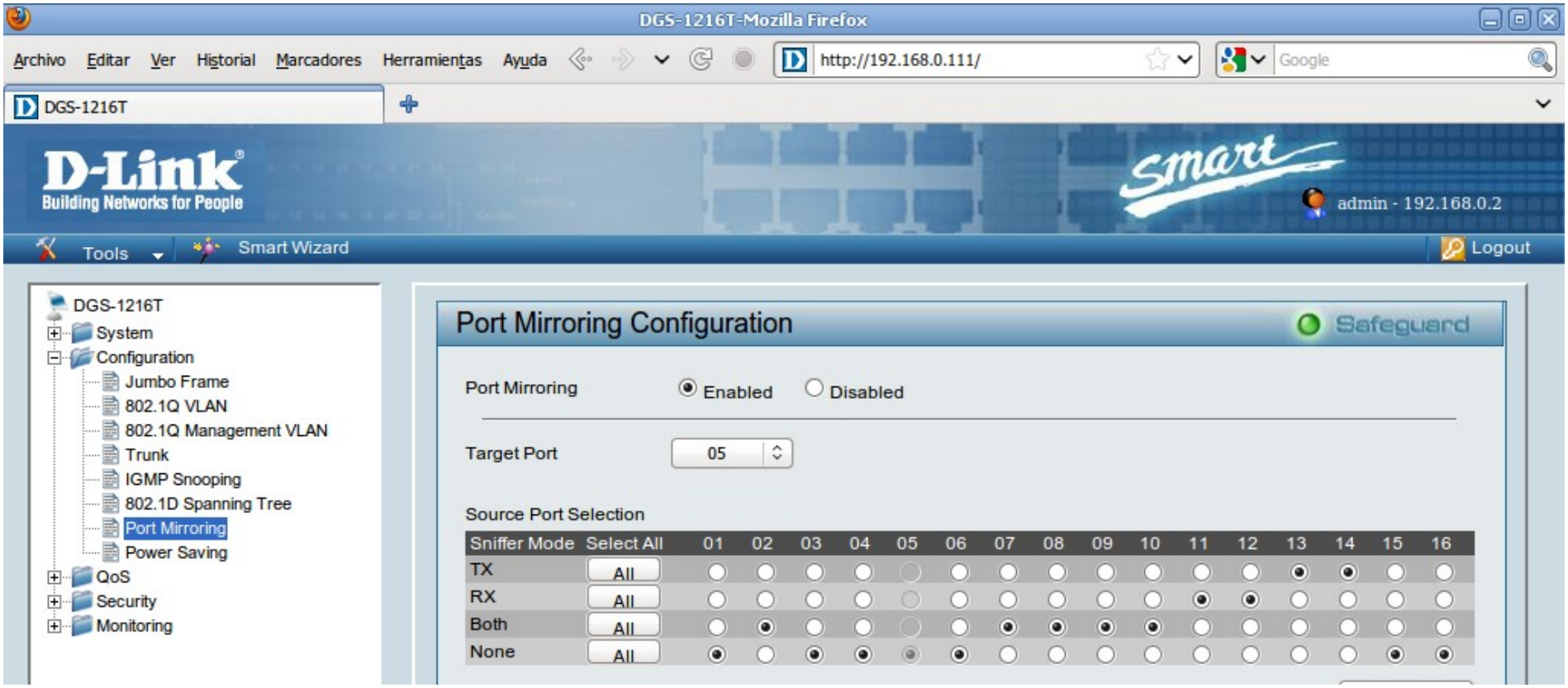


- Ventaja: fácil de implementar
- Desventaja:
  - Se introduce un ligero retardo
  - Las NICs pueden responder a algún paquete broadcast

Solución#4: Port mirroring

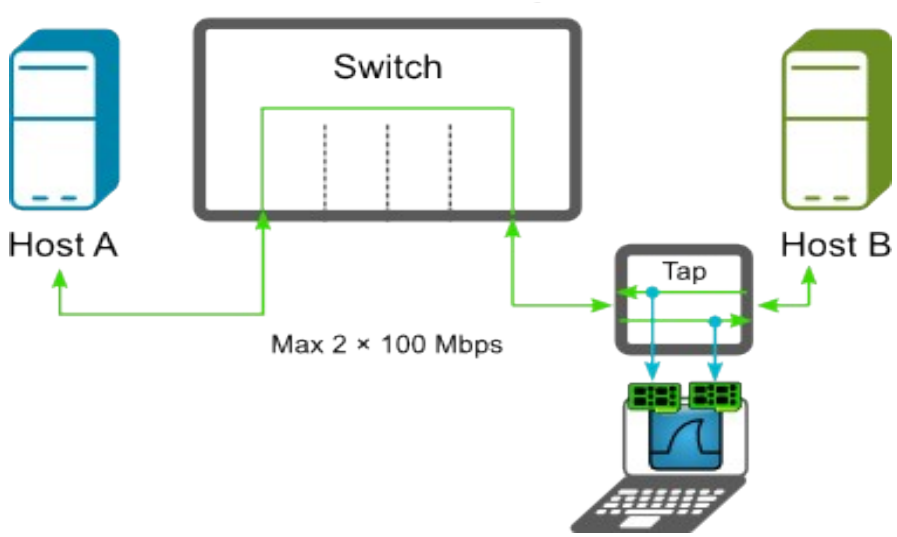


- Ventaja: fácil de implementar si el switch lo permite
- Desventaja:
  - switches gestionables → €
  - se pueden perder paquetes en situaciones de tráfico elevado



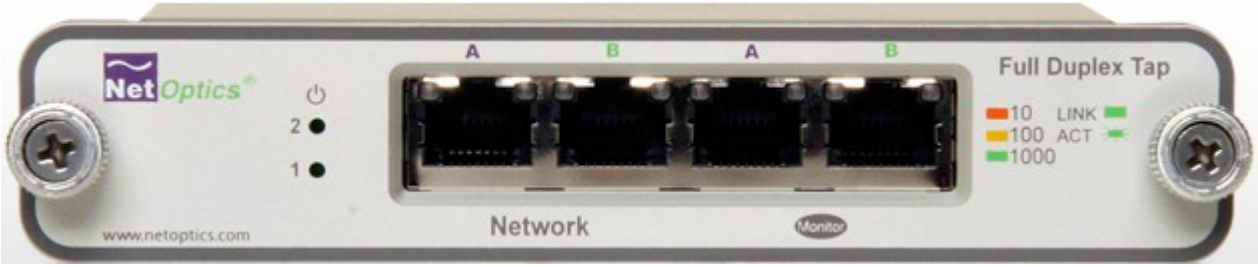
CISCO → SPAN (Switched Port ANalysis)

Solución#5: Network TAP (Test Access Port)



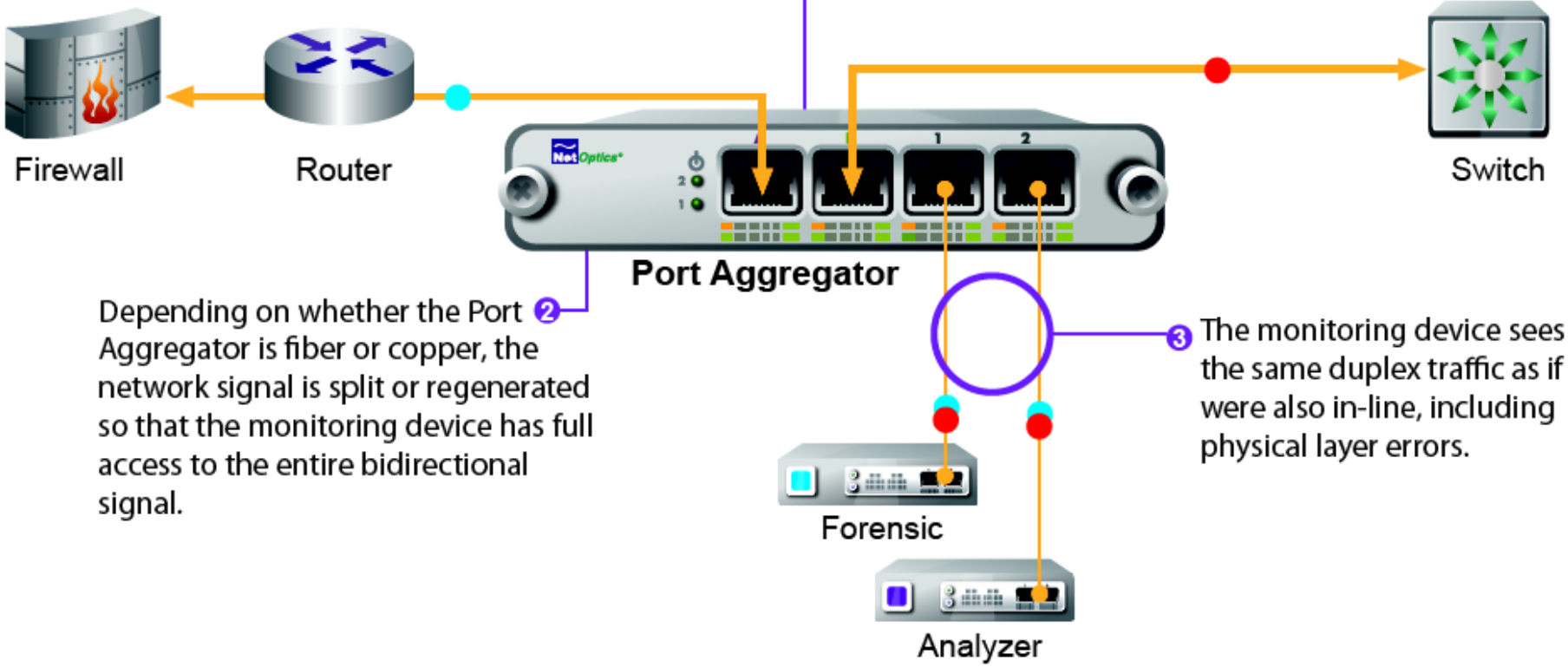
- Dispositivo pasivo que se coloca en línea para escuchar tráfico entre 2 equipos.
- No introducen retardos ni alteran el contenido del tráfico:
  - Tráfico con errores a nivel 1 y 2.
  - Etiquetado VLAN.
  - No descartan paquetes, les es indiferentes el tipo de tráfico (p.e. Ipv4 o IPv6).
- Tipos:
  - Non-aggregating:
    - Comunicaciones en dos puertos.
    - Necesidad de dos interfaces de red/instancias de wireshark. → Merge
  - Aggregating:
    - Combinan el tráfico bidireccional en un único puerto.
    - Una interfaz de red llega para monitorizar el tráfico.

Net optics 10/100/1000BaseT Non-aggregating tap



Net optics 10/100/1000BaseT Aggregating tap

The passive Port Aggregator Tap provides multiple permanent, in-line access ports to monitor all full-duplex traffic without data interference.



Genial, wireshark permite detectar anomalías en mi red pero ...

¡¡ Primero hay que saber que es lo normal !!

Baselining

Haz análisis en situaciones normales → Toma referencias

Broadcast/Multicast

- Equipos
- Aplicaciones
- Ratio paquetes/segundo

Protocolos/Aplicaciones

- Protocolos
- Aplicaciones
- Puertos TCP/UDP
- Protocolos de routing
- Tráfico ICMP

Momentos de Inactividad

- Equipo sin usuario
- Red sin usuarios

Resolución DNS

Wireless

Arranque de equipo

Login / logout

Aplicaciones clave

Comunicación VoIP