

ARP

**LA JOYA DE LOS HACKERS PARA
INTERCEPTAR TU INFORMACIÓN**

[@saulruizplaza](#)

01 ¿QUÉ ES ARP?

ARP (**Address Resolution Protocol**) es el protocolo encargado de mapear direcciones IP a direcciones MAC (48 bits) en redes locales.

Permite que los dispositivos se comuniquen a nivel de **enlace de datos**, facilitando el envío de información a través de la red.

DIRECCIÓN IP	DIRECCIÓN MAC
192.168.1.10	02:1A:3B:4C:5D:6E

02 PROCESO ARP

1. ARP Request

El dispositivo emisor envía un mensaje **broadcast** preguntando “¿**Quién tiene la IP 192.168.1.10?**”

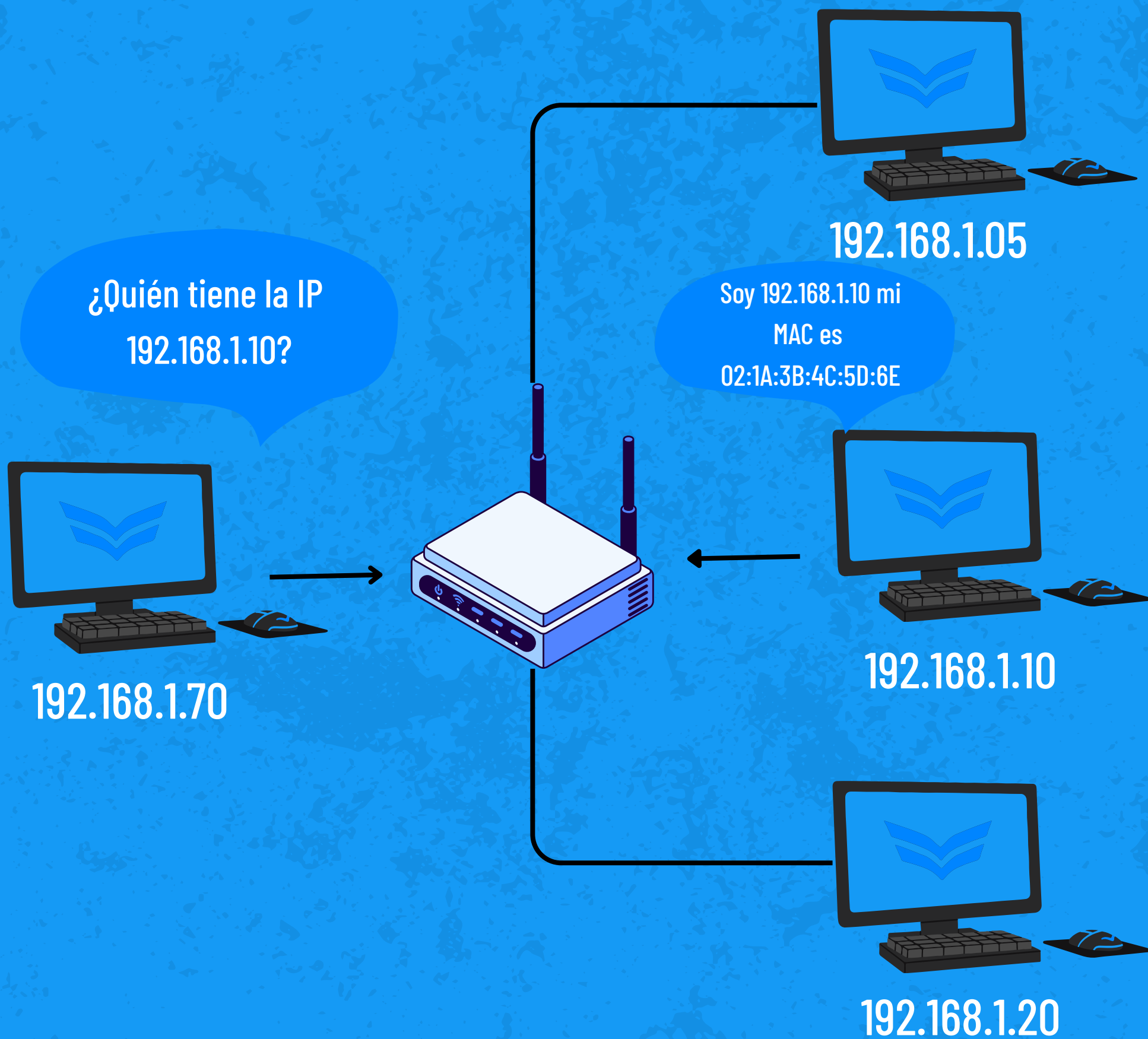
2. ARP Reply

El dispositivo que posee la IP responde de forma **unicast**, **enviando su dirección MAC.**

“Soy 192.168.1.10 y mi MAC es 02:1A:3B:4C:5D:6E.”

3. Actualización de la tabla ARP

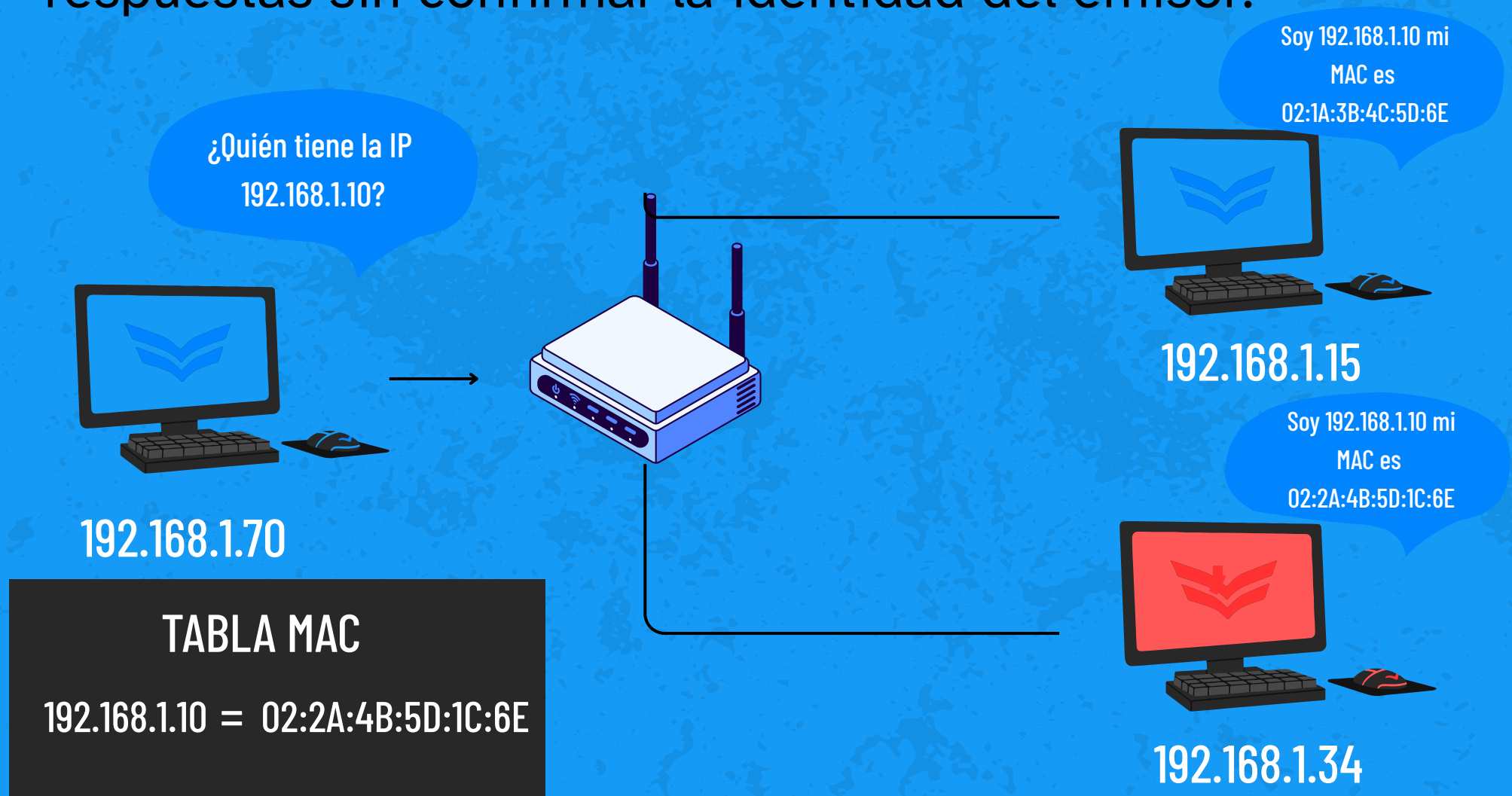
El dispositivo solicitante **almacena la relación IP-MAC** en su caché para futuras comunicaciones



03 VULNERABILIDADES DE ARP

- **Falta de Autenticación**

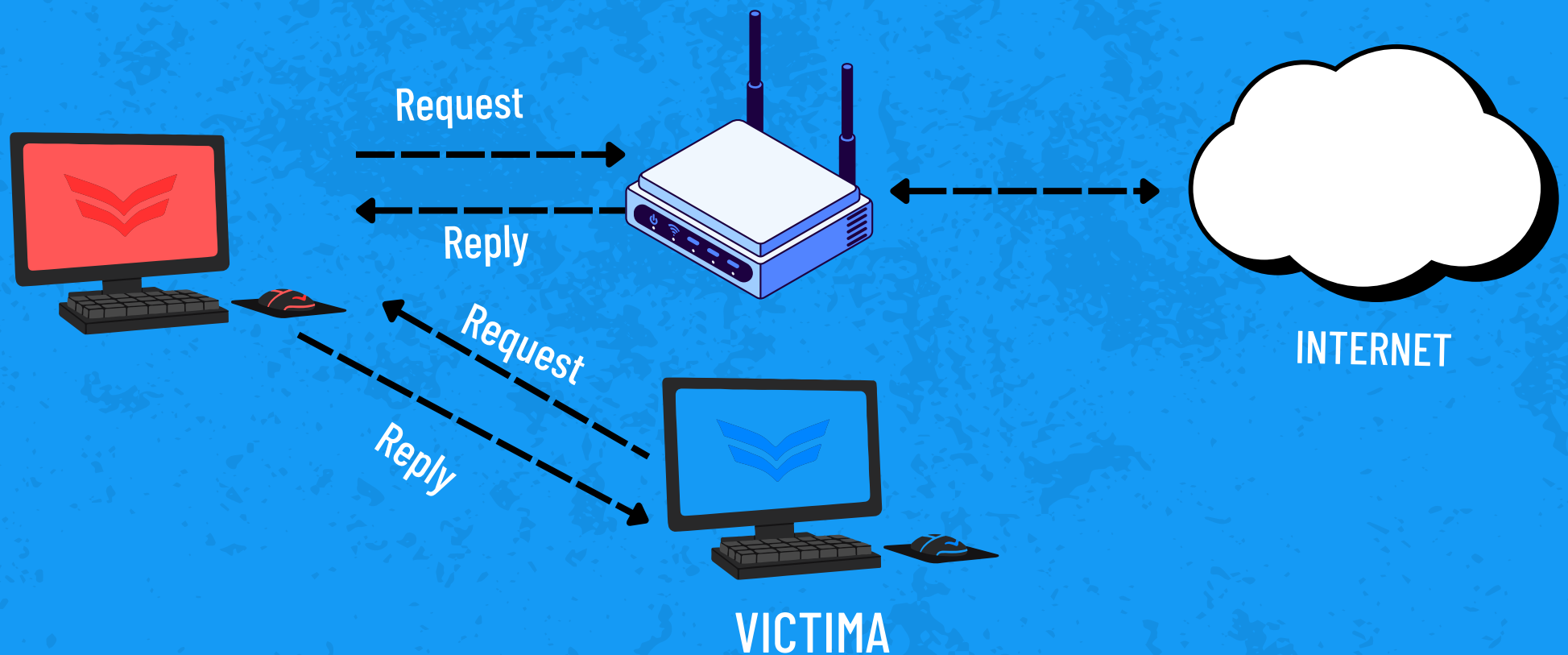
ARP no incorpora mecanismos de verificación ya que prioriza la rapidez de resolución, lo que permite aceptar respuestas sin confirmar la identidad del emisor.



03 VULNERABILIDADES DE ARP

- **ARP Spoofing**

Consiste en enviar mensajes ARP falsificados para engañar a los dispositivos y asociar la dirección IP de un dispositivo legítimo a la dirección MAC del atacante.



04 HERRAMIENTAS

- **ARPwatch:** Monitorea la tabla ARP y alerta sobre cambios inusuales.

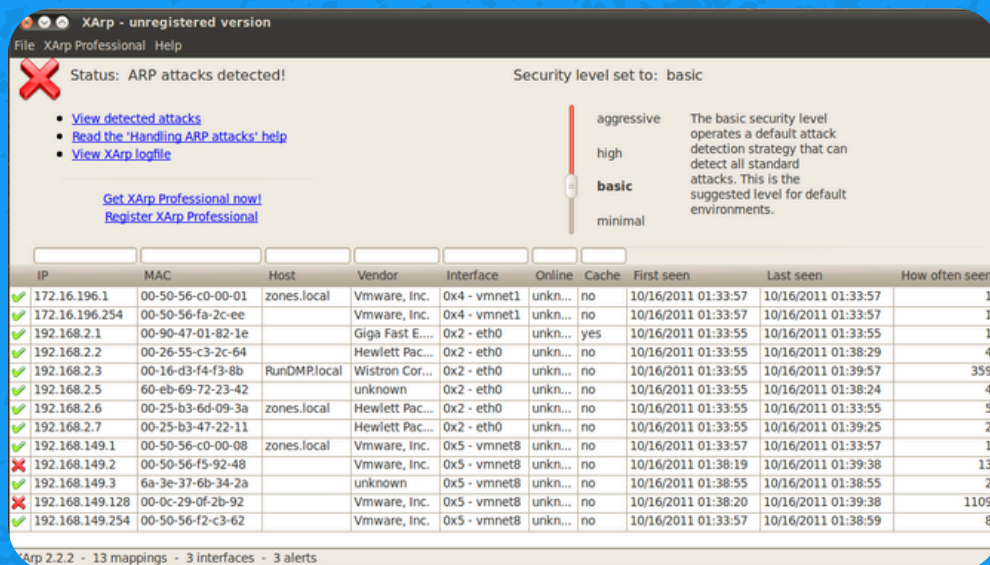
Alerta cuando una IP cambia de dirección MAC

```
hostname: centos
ip address: 172.16.16.25
interface: eth0
ethernet address: 00:56:1d:36:e6:fd
ethernet vendor: GIGA-BYTE TECHNOLOGY CO.,LTD.
old ethernet address: 00:24:1d:76:e4:1d
timestamp: Monday, April 15, 2022 15:43:45
previous timestamp: Monday, April 15, 2022 15:32:29
delta: 9 minutes
```

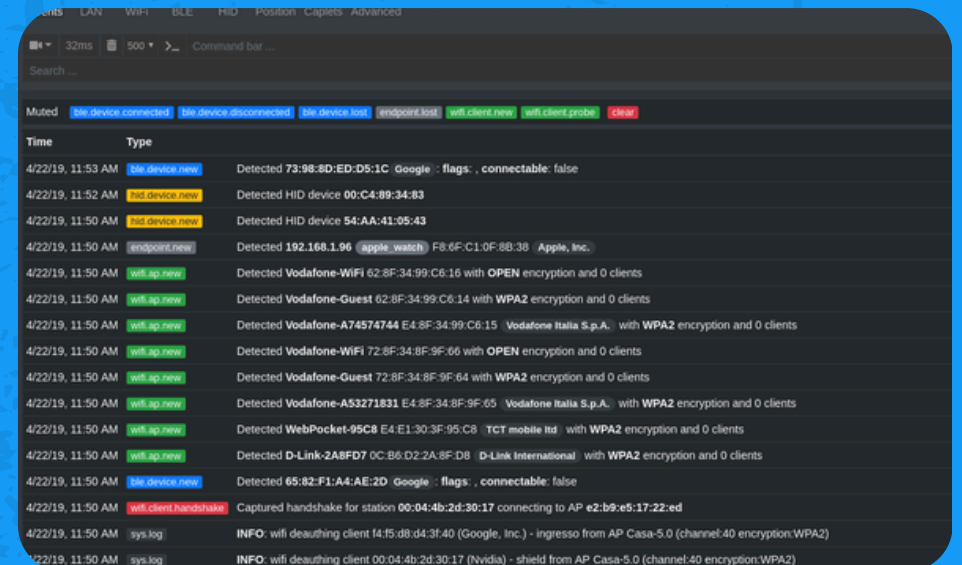
Captura extraída de Tecmint.com

04 HERRAMIENTAS

- **ARPwatch:** Detectan y analizan patrones de tráfico para identificar posibles ataques ARP.



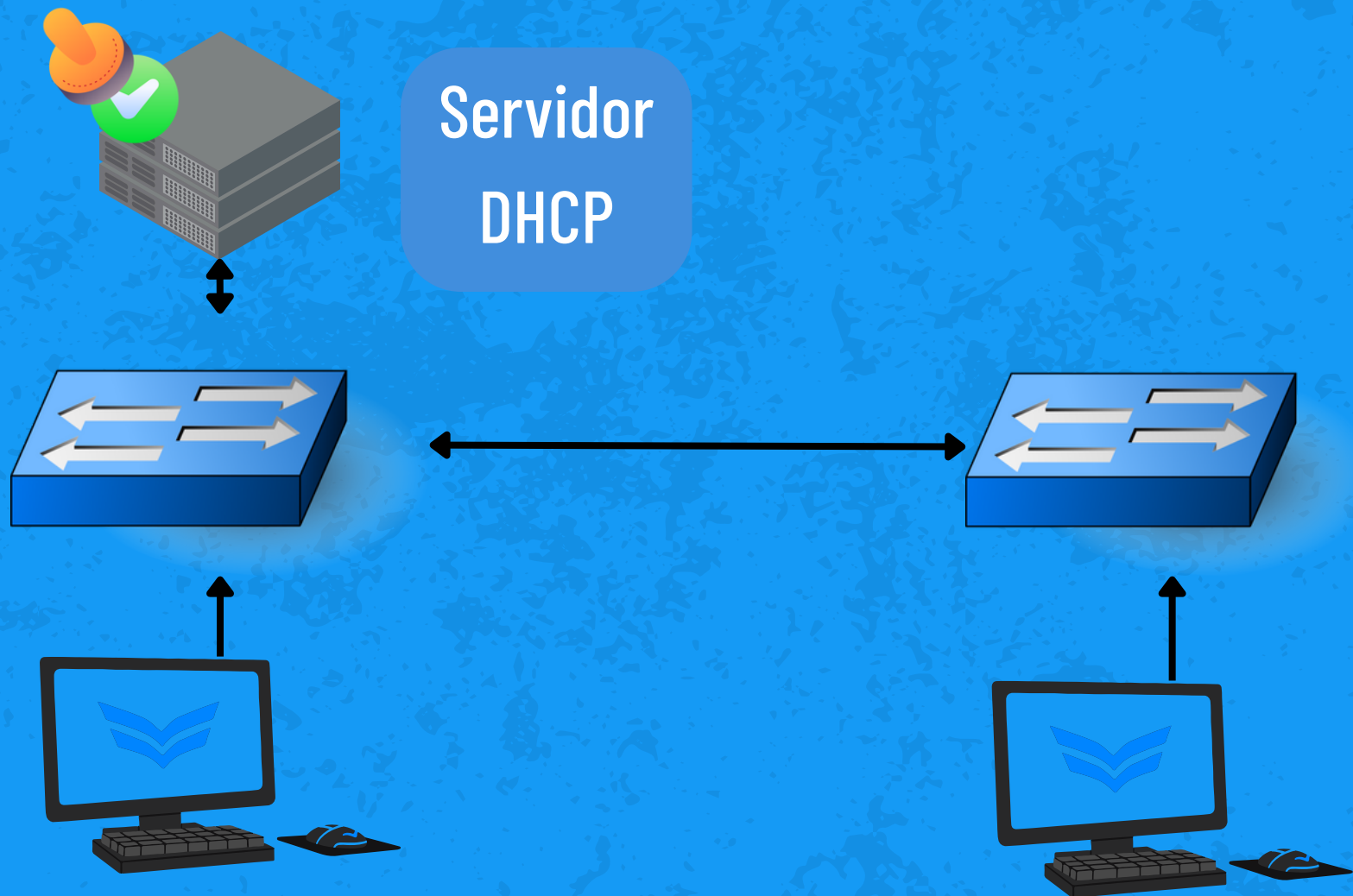
XArp



Bettercap

04 HERRAMIENTAS

- **Dynamic ARP Inspection (DAI):** Funcionalidad que valida las respuestas ARP y bloquea aquellas que no provengan de fuentes autorizadas (Servidor DHCP).



05 BUENAS PRÁCTICAS

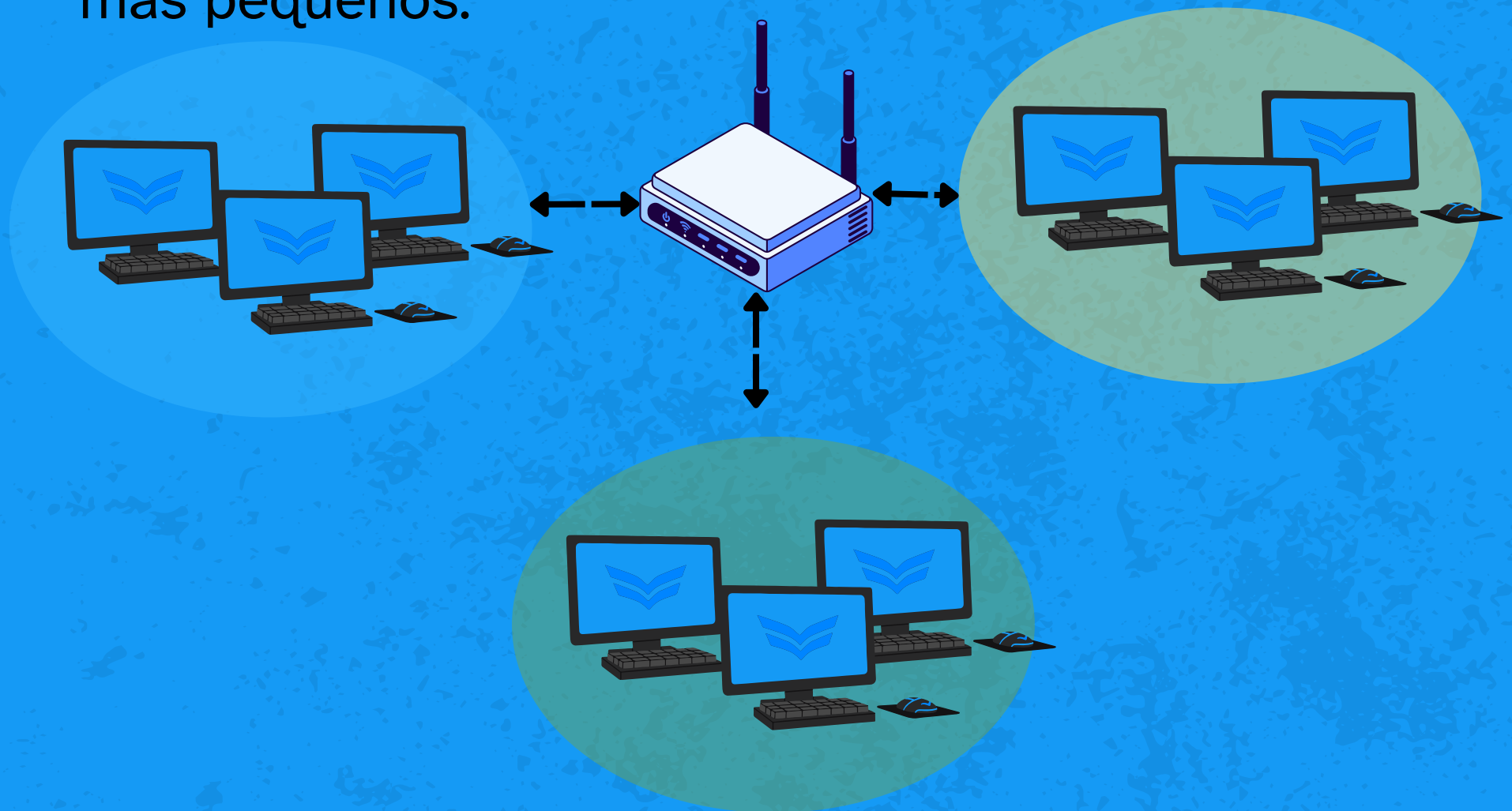
- **Entradas ARP Estáticas:** Configura manualmente entradas ARP en dispositivos críticos para evitar modificaciones no autorizadas.



Tip: Realiza un filtrado MAC para controlar el acceso

05 BUENAS PRÁCTICAS

- **Segmentación de Redes y VLANs:** Limita el alcance de un posible ataque al dividir la red en segmentos más pequeños.



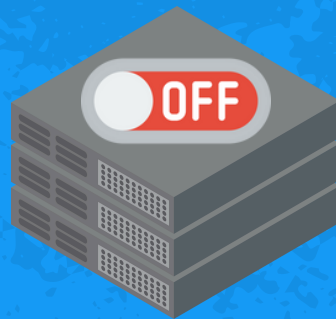
Tip: Utiliza VPNs para cifrar el tráfico

06 IMPACTO ATAQUE ARP

- **Robo de Datos Sensibles:** Con ARP Spoofing puede usarse para interceptar contraseñas, información bancaria o cualquier tipo de dato sensible.



- **Interrupción de Servicios:** Manipular el tráfico puede interrumpir servicios críticos como comunicaciones entre servidores o aplicaciones internas.



07 EJEMPLO ATAQUE ARP

En una cafetería, un atacante puede utilizar ARP Spoofing para asociar su dirección MAC con la IP del punto de acceso Wi-Fi legítimo.

Esto hace que los dispositivos de los usuarios envíen su tráfico al atacante, quien puede interceptar, modificar o redirigir la comunicación. El atacante **redirige el tráfico a una página falsa de inicio de sesión** para robar credenciales (carga útil)



MUCHAS GRACIAS



@saulruizplaza