José Eduardo Gutiérrez Conejo - 2019073558

Redes

Lectura 4: Address Resolution Protocol

1. *¿En qué consiste ARP?*

ARP (Address Resolution Protocol) es un protocolo que se usa para encontrar la dirección MAC de un dispositivo dentro de una red local (LAN) cuando solo se conoce su dirección IP. Es esencial para la comunicación en redes Ethernet.

2. *¿Cómo funciona ARP?*

Cuando un dispositivo quiere comunicarse con otro en la red local, envía un mensaje ARP broadcast preguntando "¿Quién tiene esta IP?". El dispositivo con esa IP responde con su dirección MAC, permitiendo la comunicación.

3. *¿Cuáles considera son las ventajas y desventajas de Static y Dynamic Mapping?*

El Static Mapping ofrece mayor seguridad, ya que solo los dispositivos autorizados pueden comunicarse, pero requiere administración manual, lo que puede ser complicado en redes grandes. Por otro lado, el Dynamic Mapping es más flexible y fácil de gestionar, ya que ARP aprende automáticamente las direcciones MAC, aunque es más vulnerable a ataques como ARP Spoofing.

4. *¿Cuáles son las aplicaciones de un Proxy ARP?*

El Proxy ARP permite la comunicación entre dispositivos en subredes distintas sin necesidad de una puerta de enlace (gateway), facilitando la conexión en redes que no soportan enrutamiento. Además, mejora la compatibilidad con equipos antiguos, permitiendo que sigan funcionando en infraestructuras modernas.

5. *¿Cómo funciona el ARP spoofing? Puede usar otros recursos para dar respuesta a esta pregunta.*

El ARP Spoofing es un ataque en el que un atacante engaña a los dispositivos de una red local (LAN) para que crean que él es otro dispositivo, generalmente el router o un servidor importante. Esto le permite interceptar, modificar o redirigir el tráfico de la red sin que los usuarios lo noten.

Referencia: Veracode. (s.f.). *ARP Spoofing*. Veracode. Recuperado el 27 de marzo de 2025, de https://www.veracode.com/security/arp-spoofing