UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

Departamento de Computación

Redes de Computadoras

Tema:

Práctica detección de direcciones MAC en una red local mediante el protocolo ARP

Autores:

Gabriel López

Medranda Mateo

Marcelo Pareja

NRC: 2192

Ecuador 2024-11-28

1.1 Objetivo General

Analizar el funcionamiento de las direcciones MAC y el protocolo ARP en una red local mediante la captura y análisis de tráfico con Wireshark.

1.2 Objetivos Específicos

- Identificar la estructura y composición de las direcciones MAC
- Analizar el proceso de resolución de direcciones mediante el protocolo ARP
- Examinar la comunicación entre dispositivos a nivel de capa 2 usando Wireshark
- Comprender la relación entre direcciones IP y direcciones MAC en una red local

1.3 Antecedentes

Trama Ethernet

La trama Ethernet es una unidad de transmisión que contiene:

- Preámbulo (8 bytes)
- Dirección MAC destino (6 bytes)
- Dirección MAC origen (6 bytes)
- Tipo (2 bytes) - 0x800 para IP, 0x806 para ARP
- Datos (46-1500 bytes)
- FCS - Frame Check Sequence (4 bytes)

Protocolo ARP

El protocolo ARP (Address Resolution Protocol) permite:

- Mapear direcciones IP a direcciones MAC
- Mantener tablas de correspondencia IP-MAC en caché
- Realizar consultas broadcast para encontrar MACs desconocidas

2. Desarrollo

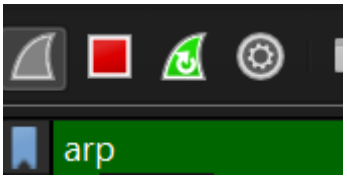
Primero, uno de los integrantes creó una red local que tenía como host a su máquina, y los demás integrantes conectaron sus equipos. Una vez conectados, se realizaron los siguientes pasos:

1.-Limpiar la tabla ARP local: Como administrador, se ejecutó en cmd el comando “arp -d *”, con el fin de olvidar todas las direcciones previas, en caso de haberse conectado previamente a la misma red.

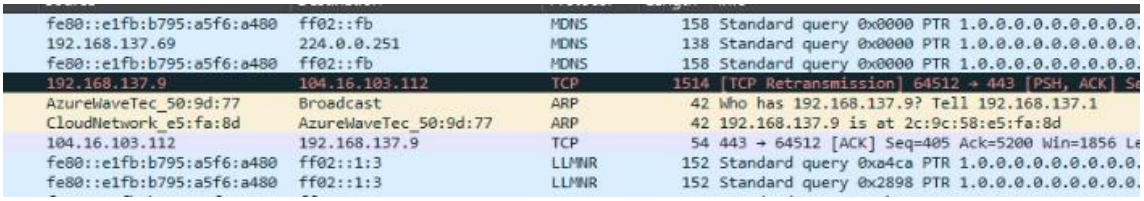
```
C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

Interfaz: 192.168.100.5 --- 0x4
  Dirección de Internet          Dirección física      Tipo
  192.168.100.1         e8-a6-60-a8-52-15     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático

Interfaz: 192.168.56.1 --- 0x15
  Dirección de Internet          Dirección física      Tipo
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

Interfaz: 172.19.32.1 --- 0x39
  Dirección de Internet          Dirección física      Tipo
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
```

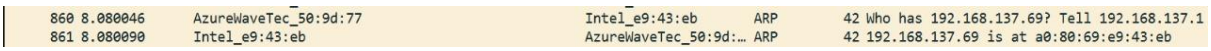
Si se verificó con “arp -a”, observando que casi al instante, apareció la dirección del host dado que es el punto de acceso a la red.

A continuación, se abrió wireshark y se dejó activo, usando el filtro arp con el fin de captar únicamente las transmisiones que usaran este protocolo.



Mientras wireshark estaba abierto, se realizaron transmisiones ping entre los equipos conectados a la red con el fin de obtener sus direcciones. Tras esperar un tiempo, se empezaron a ver las preguntas y respuestas de dirección MAC.





En este caso, se enviaron pings en ambos sentidos, así ambas máquinas podrían aprender la dirección de la otra.

3. Análisis

Tabla MAC con ARP

Integrante	Rol de su máquina	Dirección IP	Dirección MAC
Mateo Medranda	Host	192.168.137.1	80:91:33:50:9d:77
Gabriel López	Equipo conectado	192.168.137.9	2c:9c:58:e5:fa:8d
Marcelo Pareja	Equipo conectado	192.168.137.69	a0:80:69:e9:43:eb

4. Conclusiones

- Las direcciones MAC son fundamentales para la comunicación en capa 2
- El protocolo ARP es esencial para la obtención dinámica de direcciones
- La caché ARP optimiza el rendimiento de la red
- Wireshark es una herramienta efectiva para analizar el tráfico ARP

Recomendaciones

- Mantener actualizado el firmware de los dispositivos de red
- Implementar seguridad ARP en redes críticas
- Documentar las direcciones MAC de dispositivos importantes