Protocolo ARP

Address Resolution Protocol

Protocolo de Resolución de Direcciones

ARP RFC826. ¿Por qué?

- La dirección MAC (control de acceso al medio) es la dirección de la capa de enlace de datos y depende del hardware que se utilice. También conocida como dirección Ethernet.
- Un host con configuración IP, no conoce las direcciones MAC de los nodos de la red.
- Se necesita un protocolo estándar que los relacione para que un datagrama pueda llegar a su destino en una trama unicast.

ARP ¿Cómo funciona?

- Un host A debe enviar un datagrama a una dirección IP, si no conoce la dirección MAC que tiene, mandará una petición ARP en difusión
- La peticion incluye la IP la MAC del solicitante
- El que tiene la IP de la petición procederá a almacenar el par de direcciones del solicitante y después contestará en unicast.
- Al llegar al origen el par que se solicitaba se almacenará en una memoria cache .

Caché ARP

- Debido a que la red debe de estar continuamente comunicándose para la resolución de direcciones ésta puede convertirse en un problema debido al consumo de recursos en la red.
- Debido a que la petición es en difusión todos los host deben de gastar un tiempo de CPU para examinar el paquete de petición.

Caché ARP

Se solucionó con una tabla local en la que guardar los pares de direcciones.
Existen dos formas de almacenamiento en la cache:

- Estático
- Dinámico

Puede ser vulnerable a un ataque de falsificación de paquetes ARP: ARP Spoofing.

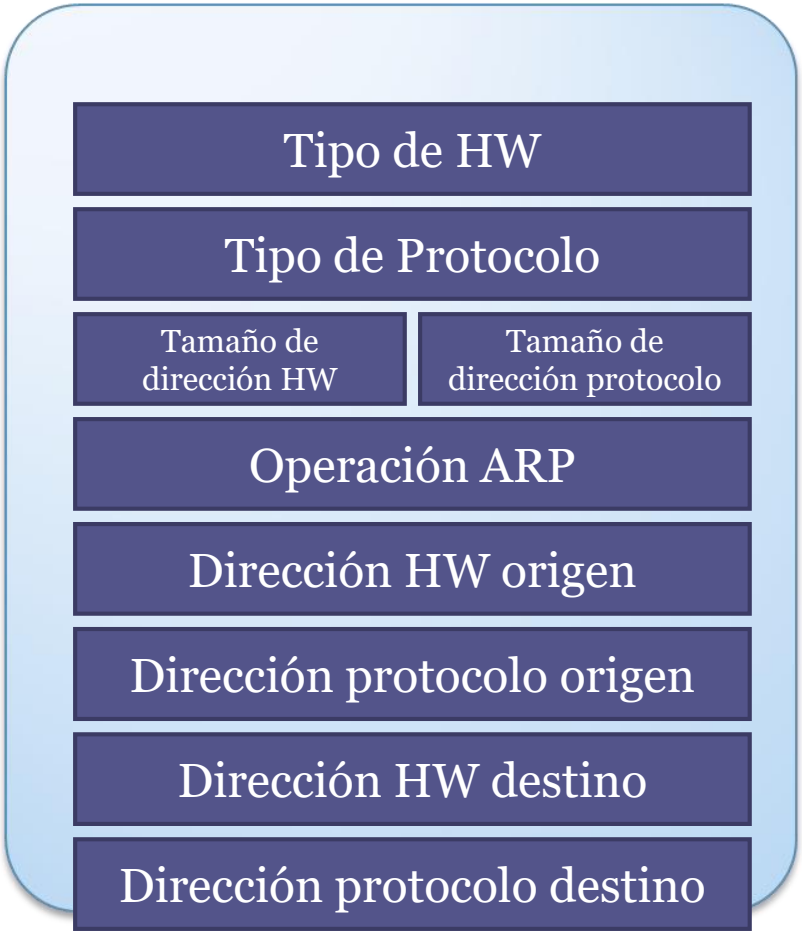
Caché ARP

En los sistemas operativos Microsoft, en la línea de comandos:

- arp -a Lista el cache
- Arp -d * Limpia la tabla ARP
- arp -s 157.55.85.212 00-aa-00-62-c6-09 .... . agrega una entrada estática

ARP El mensaje

- Tipo de HW: Ethernet, ATM, .
- Tipo de Protocolo: IPv4
- Tamaño de dirección HW: para Ethernet (MAC) 6 bytes.
- Tamaño de dirección de protocolo: Para la IPv4 4 bytes.
- Operación ARP: Petición o respuesta.



ARP El mensaje

- Utilizando Wireshark

```
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: LansTech_b0:11:eb (00:c0:26:b0:11:eb)
  Sender IP address: 192.168.0.10 (192.168.0.10)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.12 (192.168.0.12)
```

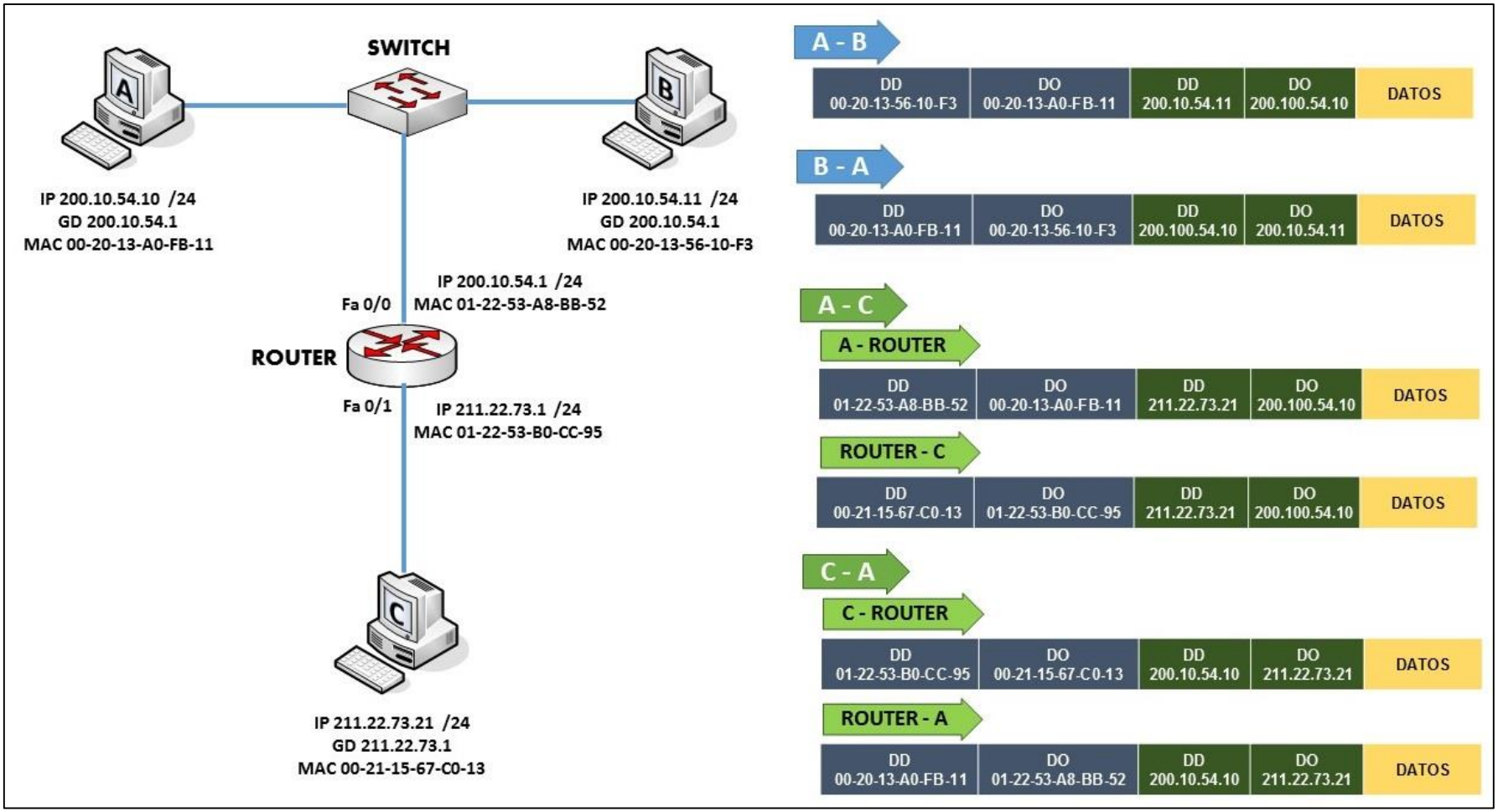
```
Address Resolution Protocol (reply)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (0x0002)
  Sender MAC address: QuantumD_e6:20:76 (00:10:5c:e6:20:76)
  Sender IP address: 192.168.0.12 (192.168.0.12)
  Target MAC address: LansTech_b0:11:eb (00:c0:26:b0:11:eb)
  Target IP address: 192.168.0.10 (192.168.0.10)
```

Envenenamiento ARP

- Este tipo de vulnerabilidad consiste en el envenenamiento de las tablas ARP de los host implicados.
- También conocido como ARP Spoofing, Falsificación ARP…
- Se aprovecha de que las tablas son dinámicas y cambian conforme le llegan respuestas ARP, aunque no hayan pedido petición ninguna.

Envenenamiento ARP: Escenario

- Tenemos un router, y dos host una la víctima y otra el atacante.
- El objetivo es que la victima y el router coloquen en la tabla ARP asociadas a la IP del otro la MAC del atacante.
- Este método se conoce como MITM (Man in the Middle).
- El atacante analiza el trafico y lo reenvía a la MAC real del destinatario


SWITCH
A
B
C
IP 200.10.54.10 /24
GD 200.10.54.1
MAC 00-20-13-A0-FB-11
IP 200.10.54.11 /24
GD 200.10.54.1
MAC 00-20-13-56-10-F3
Fa 0/0
IP 200.10.54.1 /24
MAC 01-22-53-A8-BB-52
ROUTER
Fa 0/1
IP 211.22.73.1 /24
MAC 01-22-53-B0-CC-95
IP 211.22.73.21 /24
GD 211.22.73.1
MAC 00-21-15-67-C0-13
A - B
DD 00-20-13-56-10-F3
DO 00-20-13-A0-FB-11
DD 200.10.54.11
DO 200.100.54.10
DATOS
B - A
DD 00-20-13-A0-FB-11
DO 00-20-13-56-10-F3
DD 200.100.54.10
DO 200.10.54.11
DATOS
A - C
A - ROUTER
DD 01-22-53-A8-BB-52
DO 00-20-13-A0-FB-11
DD 211.22.73.21
DO 200.100.54.10
DATOS
ROUTER - C
DD 00-21-15-67-C0-13
DO 01-22-53-B0-CC-95
DD 211.22.73.21
DO 200.100.54.10
DATOS
C - A
C - ROUTER
DD 01-22-53-B0-CC-95
DO 00-21-15-67-C0-13
DD 200.10.54.10
DO 211.22.73.21
DATOS
ROUTER - A
DD 00-20-13-A0-FB-11
DO 01-22-53-A8-BB-52
DD 200.10.54.10
DO 211.22.73.21
DATOS