Informe Laboratorio 2: Análisis del funcionamiento del protocolo ARP usando Wireshark y Packet Tracer

Sección 1 Grupo 1

Paula Villarroel; Ezequiel Morales; Dylan Barahona;
paula.villarroel@mail.udp.cl, ezequiel.morales@mail.udp.cl,
dylan.barahona@mail.udp.cl

Septiembre de 2024

Índice

1. Equipos y materiales

Para realizar las diferentes actividades se utilizaron los computadores de todos los integrantes en el caso de la actividad 2.1 se utilizó el computador de Paula Villarroel el cual consta de las siguientes caracteristicas:

CPU: Intel(R) Core(TM) i7-7500U
RAM: 8GB
OS: Windows 10

En el caso de la actividad 2.2 se utilizo el computador del integrante Ezequiel Morales, el cual consta de las siguientes caracteristicas:

CPU: AMD Ryzen 5 5600X
RAM: 32GB
OS: Windows 11

Para la última actividad la 2.3 se utilizo el computador del integrante Dylan Barahona, el cual consta de las siguientes caracteristicas:

CPU: AMD Ryzen 3 3300X
RAM: 16GB
OS: Windows 10

Para la actividad 2.1 fue necesario tener como material un router, el cual se utilizo el de la integrante Paula Villarroel, para la actividad 2.2, fue necesario utilizar el software WireShark y para la ultima actividad la 2.3 fue necesario utilizar Cisco Packet Tracer.

2. Actividades

2.1. Uso del comando *arp*

1. En su computador, se pide abrir una ventana de línea de comandos (usando CMD) o consola y escribir el comando *ipconfig* (Windows) o *ifconfig* (Linux y macOS) y obtenga los parámetros de configuración de red de su computador (dirección IP, máscara, IP gateway por defecto, etc).

   Respuesta: A partir de la siguiente figura se pueden obtener los datos explícitamente.

```
Sufijo DNS específico para la conexión. . :
Descripción . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
Dirección física. . . . . . . . . . . . : E4-42-A6-4B-BF-1D
DHCP habilitado . . . . . . . . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . . . . . . . . : ::e4dd:2b14:d991:564d(Preferido)
Dirección IPv6 temporal. . . . . . . . : ::c942:ab5c:afb5:2b78(Preferido)
Vínculo: dirección IPv6 local. . . . : fe80::ed78:5ef2:1166:8247%5(Preferido)
Dirección IPv4. . . . . . . . . . . . . : 192.168.0.8(Preferido)
Máscara de subred . . . . . . . . . . . : 255.255.255.0
Concesión obtenida. . . . . . . . . . . : viernes, 20 de septiembre de 2024 12:19:09
La concesión expira . . . . . . . . . . : viernes, 27 de septiembre de 2024 15:43:30
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . . . . . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . . . . . . . . . . : 82068134
DUID de cliente DHCPv6. . . . . . . . . : 00-01-00-01-2D-07-1B-37-E4-42-A6-4B-BF-1D
Servidores DNS. . . . . . . . . . . . . : 190.160.0.15
                                        200.83.1.5
                                        200.30.192.14
NetBIOS sobre TCP/IP. . . . . . . . . . : habilitado
```

Figura 1: Salida de ipconfig /all: Datos de red y conexión (cmd)

Dirección IP: 192.168.0.8
Dirección MAC: E4-42-A6-4B-BF-1D
Máscara de subred: 255.255.255.0
IP *gateway* por defecto: 192.168.0.1
Servidores DNS:

- **DNS 1:** 190.160.0.15
- **DNS 2:** 200.83.1.5
- **DNS 3:** 200.30.192.14

2. Obtener la dirección IP y MAC de su router. Indicar cómo obtuvo dicha información.

   Se puede obtener la dirección IP del router con la información de **'IP *gateway* por defecto'** como muestra la figura 1. También es posible obtenerla accediendo a la interfaz de administración del dispositivo, como muestra la figura a continuación.

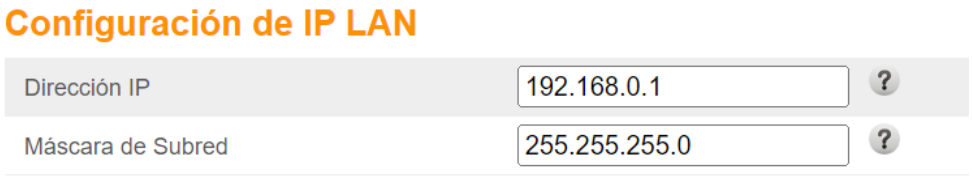


Figura 2: Configuración de IP LAN

La dirección MAC se puede obtener de la etiqueta ubicada en la parte posterior del router, se utilizó la dirección de **'gateway'**, ya que es la más relevante para la comunicación entre la red local e Internet.

Figura 3: Etiqueta del router

Entonces:
Dirección IP: 192.168.0.1
Dirección MAC: 18-35-D1-AF-E4-05

3. En la ventana de comandos escribir el comando *arp* y analice los resultados.
Respuesta: El comando 'arp' muestra la tabla de direcciones ARP (Address Resolution Protocol), que asocia direcciones IP con direcciones MAC en una red local. Esta tabla permite identificar los dispositivos conectados, mostrando las direcciones IP, sus respectivas direcciones MAC y el tipo de entrada.

```
C:\Users\pawav>arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones
físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Pide los datos de protocolo actuales y muestra las
                entradas ARP actuales. Si se especifica inet_addr, solo se
                muestran las direcciones IP y física del equipo especificado.
                Si existe más de una interfaz de red que utilice ARP, se
                muestran las entradas de cada tabla ARP.
  -g            Igual que -a.
  -v            Muestra las entradas actuales de ARP en modo detallado.
                Se mostrarán todas las entradas no válidas y las entradas
                en la interfaz de bucle invertido.
  inet_addr     Especifica una dirección de Internet.
  -N if_addr    Muestra las entradas ARP para la interfaz de red especificada
                por if_addr.
  -d            Elimina el host especificado por inet_addr. inet_addr puede
                incluir el carácter comodín * (asterisco) para eliminar todos
                los host.
  -s            Agrega el host y asocia la dirección de Internet inet_addr
                con la dirección física eth_addr. La dirección física se
                indica como 6 bytes en formato hexadecimal, separados por
                guiones. La entrada es permanente.
  eth_addr      Especifica una dirección física.
  if_addr       Si está presente, especifica la dirección de Internet de la
                interfaz para la que se debe modificar la tabla de conversión
                de direcciones. Si no está presente, se utilizará la primera
                interfaz aplicable.
Ejemplo:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09 .... Agrega una entrada estática
  > arp -a                                   .... Muestra la tabla ARP
```

Figura 4: Salida del comando arp (cmd)

4. ¿Qué comando usaría para mostrar todas las entradas de la tabla ARP?.
   Respuesta: Para mostrar todas las entradas de la tabla ARP se puede utilizar el comando 'arp -a' o 'arp -g'.

```
C:\Users\pawav>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.4           24-e8-53-41-a6-7a     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  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
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\Users\pawav>arp -g

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.4           24-e8-53-41-a6-7a     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  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
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

Figura 5: Salida del comando arp -a y arp -g (cmd)

5. ¿Qué comando usaría para borrar todas las entradas de la tabla ARP (purgar la tabla ARP)?.
   Respuesta: Para borrar todas las entradas se utiliza 'arp -d *'.

```
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.4           24-e8-53-41-a6-7a     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  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
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 6: Salida del comando arp -d * (cmd)

6. ¿Qué comando usaría para eliminar una entrada específica de la tabla ARP?.
   Respuesta: Para eliminar una entrada específica de la tabla ARP se usa el comando 'arp -d' seguido de la dirección IP de la entrada que se desea eliminar. Por ejemplo 'arp -d 192.168.0.4'.

```
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático

C:\WINDOWS\system32>arp -d 192.168.0.252

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 7: Salida del comando arp -d IP (cmd)

7. ¿Qué comando usaría para agregar una entrada ARP estática en la tabla ARP?
   Respuesta: Para agregar una entrada RP estática, usaría el comando 'arp -s' seguido de la dirección IP y dirección MAC correspondiente. Por ejemplo 'arp -s 192.168.1.100 01-cb-48-8d-a5-e3'

```
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático

C:\WINDOWS\system32>arp -s 192.168.1.100 01-cb-48-8d-a5-e3

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  192.168.1.100         01-cb-48-8d-a5-e3     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 8: Salida del comando arp -s IP MAC (cmd)

8. Indique la diferencia entre una entrada ARP dinámica y una estática.
   Respuesta: Las entradas ARP dinámicas se generan automáticamente cuando un dispositivo se comunica por primera vez con otro, pueden caducar si no se usan, en cambio las entradas ARP estáticas son permanentes, no caducan a menos que se eliminen.

9. Verifique el contenido de su tabla ARP, para esto utilice el comando *arp -a*. Comente los resultados.
   Respuesta: La salida del comando 'arp -a' muestra direcciones IP y sus MAC asociadas. Las entradas dinámicas, como 192.168.0.1 y 192.168.0.252, se crean automáticamente cuando hay interacción con dispositivos en la red, es por esto que el dispositivo con la dirección IP: 192.168.0.252 y MAC: 00-00-ca-01-02-03 volvió a aparecer cuando se ejecutó el comando de 'arp -s'. Por otro lado, las estáticas, como 192.168.1.100, son configuradas manualmente y son permanentes hasta que sean eliminadas.

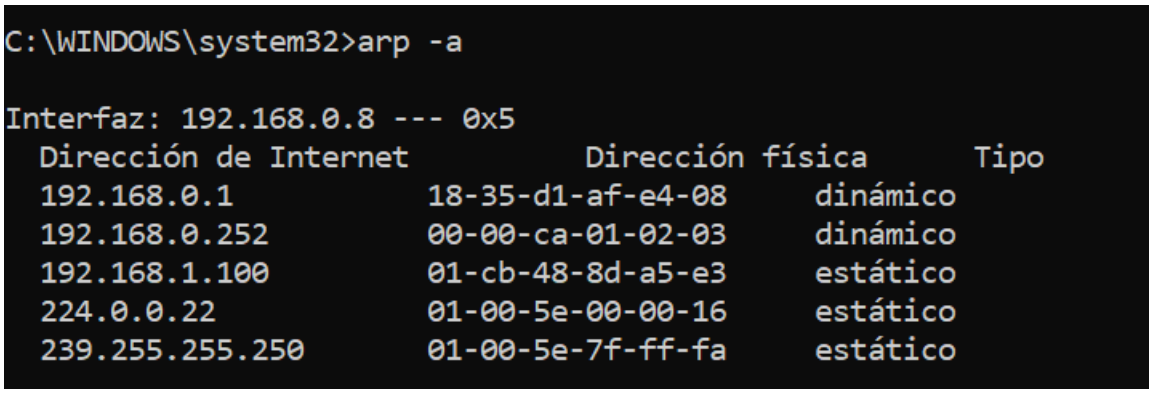


Figura 9: Salida del comando arp -a (cmd)

10. Utilice el comando *arp -d ** (Windows) o *sudo arp -d -a* (Linux y macOS). Verifique el contenido de su tabla ARP. Comente los resultados.
    Respuesta: Después de usar el comando 'arp -d *', los resultados muestran que solo quedaron las entradas estáticas: 224.0.0.22 y 239.255.255.250. La única entrada dinámica que queda es 192.168.0.1, que corresponde al router. Este se regeneró inmediatamente porque la computadora interactúa con el router continuamente.

```
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.252         00-00-ca-01-02-03     dinámico
  192.168.1.100         01-cb-48-8d-a5-e3     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático

C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 10: Salida del comando arp -d * (cmd)

11. Utilice el comando *ping* a su dirección IP *broadcast*. Verifique nuevamente el contenido de su tabla ARP y comente los resultados. ¿Cuántos dispositivos de red existen en su red LAN?.
    Respuesta: Para usar el comando *ping* primeramente se necesita la dirección IP *broadcast*, como la dirección IP de la computadora es 192.168.0.8 y su máscara de subred es 255.255.255.0, la dirección IP de *broadcast* será: 192.168.0.255.
    Debido a que el router presentó problemas de conectividad, posiblemente por que tenga medidas de seguridad que limiten las respuestas a *ping* y *broadcast*, se optó por utilizar **'Angry IP Scanner'** para realizar un escaneo de la red.

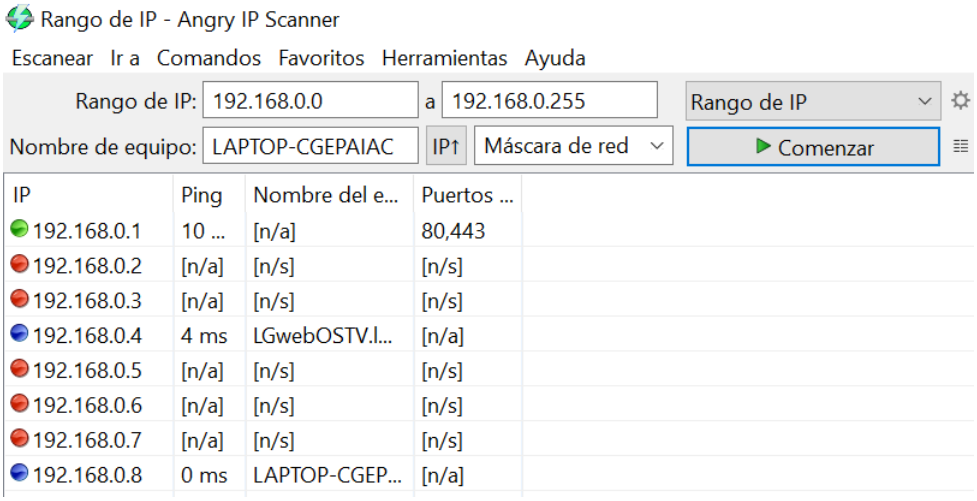


Figura 11: Direcciones IP de dispositivos en la red (Angry IP Scanner)

Al hacer un ping, la tabla ARP solo se actualiza si el dispositivo no está ya registrado, por lo tanto la tabla ARP no presentará cambios, los dispositivos ya son conocidos por la red.

```
C:\WINDOWS\system32>arp -a

Interfaz: 192.168.0.8 --- 0x5
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           18-35-d1-af-e4-08     dinámico
  192.168.0.4           24-e8-53-41-a6-7a     dinámico
  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
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 12: Salida del comando arp -a (cmd)

12. ¿Cuantos dispositivos de red existen en su WLAN?. ¿Podría dibujar la topología lógica?. **Respuesta:** Para el diagrama de topología lógica, se deben identificar los dispositivos en la red, en este caso serán tres:

    - **Router:** IP: 192.168.0.1; MAC: 18-35-D1-AF-E4-05
    - **Computadora 'LAPTOP-CGEPAIAC':** IP : 192.168.0.8; MAC: E4-42-A6-4B-BF-1D
    - **Televisor 'LGwebOSTV':** IP: 192.168.0.4; MAC: 24-E8-53-41-A6-7A

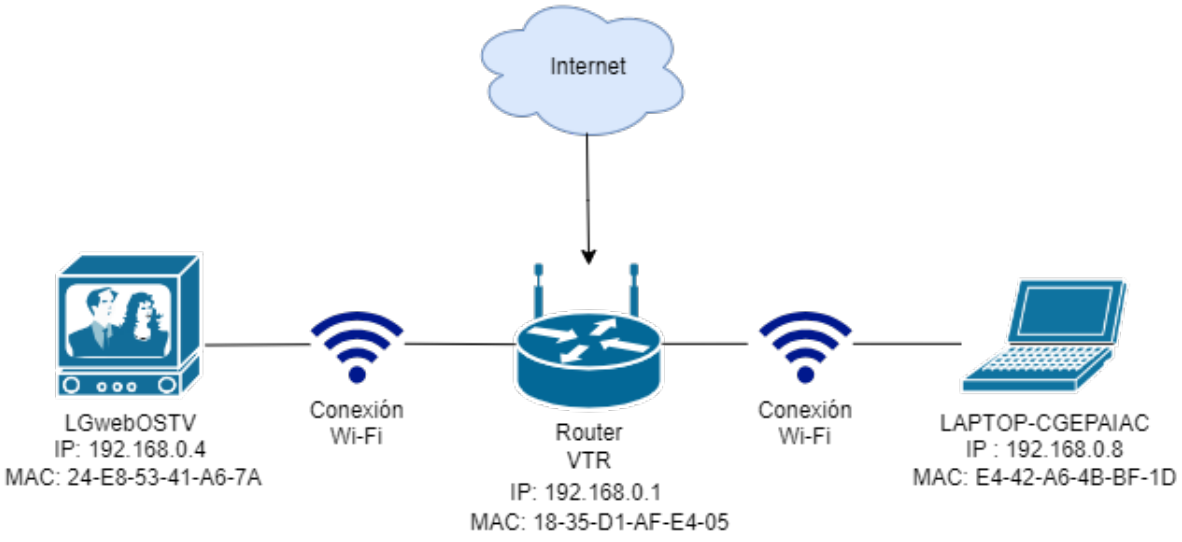
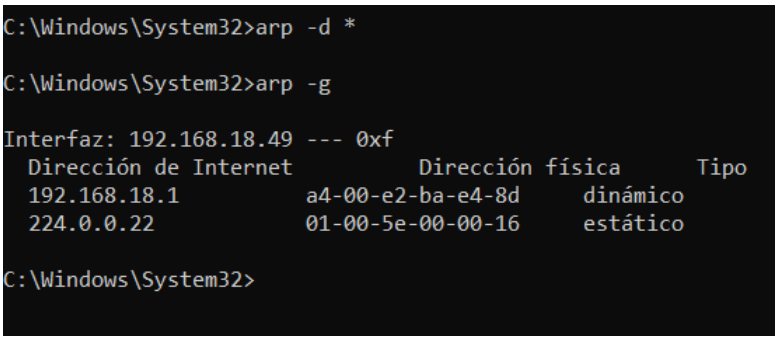


Figura 13: Diagrama topología lógica de la red local

2.2. Captura y análisis de mensajes ARP usando Wireshark

1. En su computador borre la tabla ARP y luego verifique su contenido. A continuación ejecute Wireshark, inicie la captura de paquetes y seleccione un filtro de captura para mostrar solamente los paquetes del protocolo ARP.

   Respuesta: Una vez eliminada la tabla ARP se puede verificar el contenido para iniciar la captura de paquetes ARP en WIRESHARK.

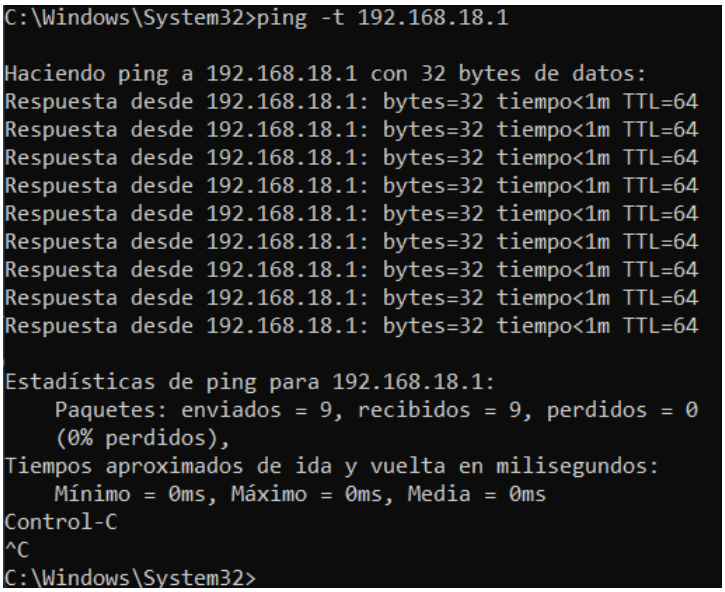


```
C:\Windows\System32>arp -d *

C:\Windows\System32>arp -g

Interfaz: 192.168.18.49 --- 0xf
  Dirección de Internet          Dirección física      Tipo
  192.168.18.1          a4-00-e2-ba-e4-8d     dinámico
  224.0.0.22            01-00-5e-00-00-16     estático

C:\Windows\System32>
```

Figura 14: Salida del comando arp -d * y arp -g (cmd)

2. Realice un *ping* a la dirección IP del *gateway* por defecto. Una vez finalizado el *ping* detenga la captura de Wireshark y examine los mensajes ARP capturados e indique:

   Respuesta: Al mismo tiempo se hace un *ping* al *gateway* por defecto el cual es 192.168.18.1.



```
C:\Windows\System32>ping -t 192.168.18.1

Haciendo ping a 192.168.18.1 con 32 bytes de datos:
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.18.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.18.1:
    Paquetes: enviados = 9, recibidos = 9, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Windows\System32>
```

Figura 15: Salida del comando ping -t 192.168.18.1(cmd)

- Primer mensaje ARP capturado.

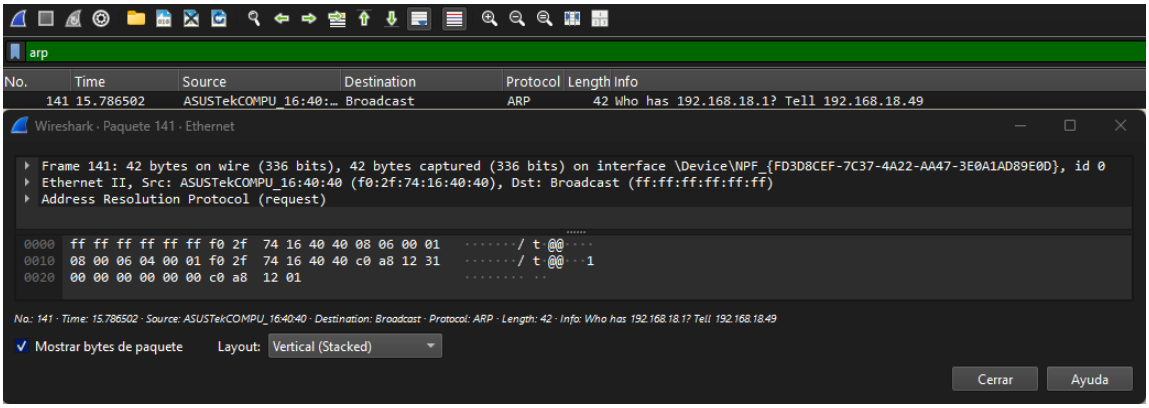


Figura 16: ARP *request* del PC al Router

- Complete la Tabla 1 con la información de las direcciones MAC del primer mensaje (ARP *request*).

Campo	Valor
MAC emisor	f0:2f:74:16:40:40
MAC destino	ff:ff:ff:ff:ff:ff

Tabla 1: Direcciones MAC del mensaje ARP *request*

- ¿Qué valor en hexadecimal toma una dirección MAC del tipo broadcast?.
Respuesta: Una dirección MAC del tipo broadcast toma valor hexadecimal de ff:ff:ff:ff:ff:ff ya que esta destinada a enviarse a todos los dispositivos en la red local.

- Complete la Tabla 2 con la información de los campos del mensaje ARP *request*.

Address Resolution Protocol (request)	
Hardware type	Ethernet (1)
Protocol type	IPv4 (0x0800)
Hardware size	6
Protocol size	4
Opcode	request (1)
Sender MAC address	ASUSTekCOMPU-16:40:40
Sender IP address	192.168.18.49
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.18.1

Tabla 2: Estructura del mensaje ARP *request*.

- Segundo mensaje ARP capturado.

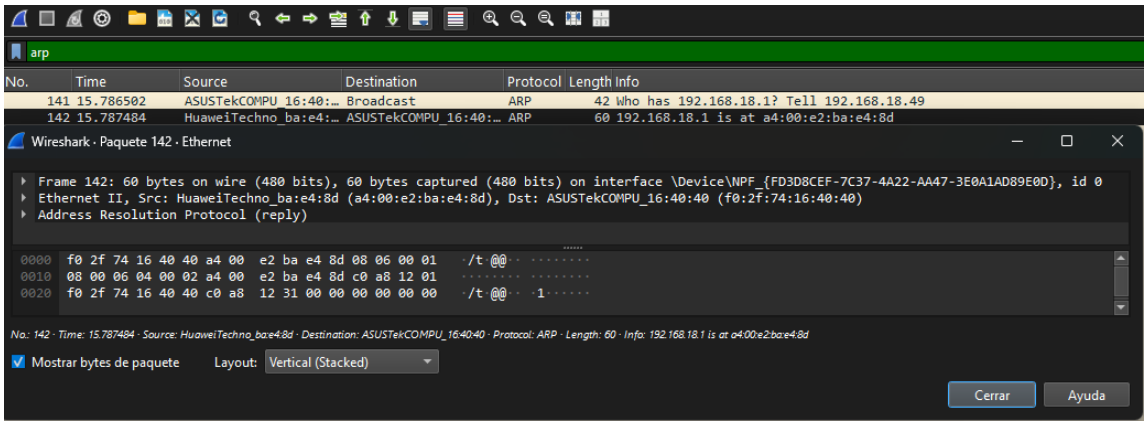


Figura 17: ARP *reply* del Router al PC

- Complete la Tabla 3 con la información de las direcciones MAC del segundo mensaje (ARP *reply*).

Campo	Valor
MAC emisor	a4:00:e2:ba:e4:8d
MAC destino	f0:2f:74:16:40:40

Tabla 3: Direcciones MAC del mensaje ARP *reply*

- Complete la Tabla 4 con la información de los campos del mensaje ARP *reply*.

Address Resolution Protocol (request)	
Hardware type	Ethernet (1)
Protocol type	IPv4 (0x0800)
Hardware size	6
Protocol size	4
Opcode	reply (2)
Sender MAC address	HuaweiTechno-ba:e4:8d
Sender IP address	192.168.18.1
Target MAC address	AsusTekCOMPU-16:40:40
Target IP address	192.168.18.49

Tabla 4: Estructura del mensaje ARP *reply*.

3. ¿Es necesario que los mensajes ARP request sean transmitidos en un frame con una dirección MAC de destino del tipo *broadcast*?

Respuesta: No, no es totalmente necesario que los mensajes ARP request sean transmitidos en un frame con una dirección MAC de destino del tipo broadcast. Aunque generalmente los ARP requests se envían en broadcast para descubrir la dirección MAC correspondiente a una dirección IP desconocida, también pueden ser transmitidos en unicast.

4. ¿Diría que los mensajes ARP *reply* son de tipo del tipo *broadcast*?. ¿Por qué?.

   Respuesta: No, ninguno de los mensajes ARP reply son del tipo broadcast, ya que su propósito es responder directamente al dispositivo que hizo la solicitud ARP request. El ARP reply contiene la dirección MAC correspondiente a la dirección IP solicitada, y esta respuesta se envía únicamente al dispositivo que realizó el ARP request, utilizando unicast.

5. ¿Se le ocurre algún motivo para enviar un mensaje ARP *request* dentro de un frame con destino *unicast*?. Analice sus capturas y verifique la existencia de este tipo de mensajes (screenshot). Complete las Tablas 5 y 6. Sugerencia: leer el RFC 1122, section 2.3.2.1 - ARP Cache Validation.

   Respuesta: Un ARP request puede enviarse en unicast cuando un dispositivo ya tiene la dirección MAC del destinatario en su caché ARP y solo desea validar que no ha cambiado, evitando así el broadcast. Esto ocurre para reducir tráfico en la red o verificar la información de la caché. Tal como se observa en la Figura 18 un ARP request unicast del router al PC, lo que indica que el router ya conocía la dirección MAC del PC y no necesitaba hacer un broadcast.

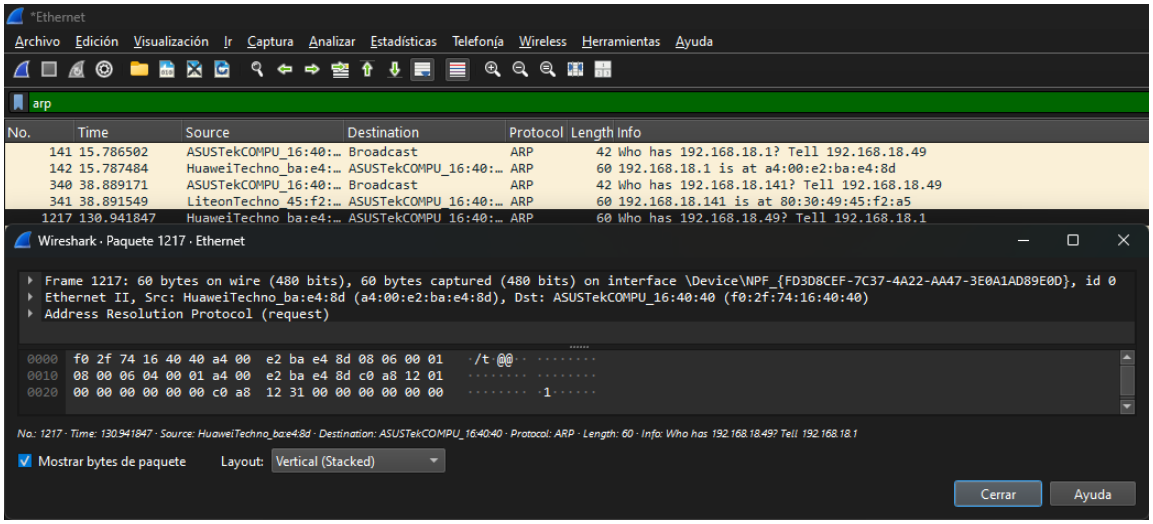


Figura 18: ARP *request* del Router al pc

Campo	Valor
MAC emisor	f0:2f:74:16:40:40
MAC destino	00:00:00:00:00:00

Tabla 5: Direcciones MAC del mensaje *gratuitous* ARP

Address Resolution Protocol (ARP Announcement)	
Hardware type	Ethernet (1)
Protocol type	IPv4 (0x0800)
Hardware size	6
Protocol size	4
Opcode	request (1)
Is gratuitous	True
Is announcement	True
Sender MAC address	AsusTekCOMPU-16:40:40
Sender IP address	192.168.18.49
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.18.49

Tabla 6: Estructura del mensaje ARP *announcement*.

6. Inicie una nueva captura de paquetes con Wireshark e implemente un filtro de captura que permita visualizar los mensajes ARP e ICMP (*arp* or *icmp*). A continuación ejecute el comando *ping* a la siguiente dirección:

   - `www.google.com`
   - `www.youtube.cl`
   - `www.facebook.com`

   Detenga la captura y analice las direcciones MAC de origen y destino de los paquetes ICMP (ping) *request* y *reply*. ¿Qué dirección MAC se utilizó para sacar los paquetes (*echo ping request*) hacia los servidores?. ¿Qué dirección MAC de origen tenían los mensajes de respuesta (*echo ping reply*) de los servidores?. Comente.

Direcciones	MAC Echo (ping) request	MAC Echo (ping) reply
www.google.com	f0:2f:74:16:40:40	a4:00:e2:ba:e4:8d
www.youtube.cl	f0:2f:74:16:40:40	a4:00:e2:ba:e4:8d
www.facebook.com	f0:2f:74:16:40:40	a4:00:e2:ba:e4:8d

Tabla 7: MAC echo ping request y reply

Respuesta: Como se puede ver las direcciones MAC de los paquetes de *echo ping request* y *echo ping reply* son iguales para las tres direcciones distintas, ya que cuando

se hace ping a una dirección que no pertenece a la red local, las direcciones MAC no se comparten. En este caso, el router se encarga de direccionar la conexión a través de las direcciones IP, permitiendo la comunicación con destinos externos.

7. Investigue acerca de las vulnerabilidades del protocolo ARP y los tipos de ataques.

   Respuesta: Uno de las posibles vulnerabilidades del protocolo ARP es la falta de autenticación, ya que ARP no verifica la identidad de los dispositivos que envían solicitudes y respuestas, permitiendo que cualquier dispositivo pueda introducir información falsa. Además, el protocolo es vulnerable a ataques de spoofing, donde un atacante puede enviar respuestas ARP falsificadas, asociando su dirección MAC con la dirección IP de otro dispositivo, lo que le permite interceptar o redirigir el tráfico destinado a ese dispositivo. Otro ataque posible es el de Man-in-the-Middle (MitM), donde un atacante intercepta y altera las comunicaciones entre dos dispositivos en la red al hacerse pasar por ambos mediante respuestas ARP engañosas, capturando así información sensible. También existen ataques de Denegación de Servicio (DoS), donde un atacante puede inundar la red enviando múltiples solicitudes ARP, provocando que la tabla ARP de los dispositivos se sature y colapse, impidiendo la correcta resolución de direcciones IP y afectando la conectividad de la red.

8. Investigue sobre el funcionamiento del protocolo RARP.

   Respuesta: RARP (Reverse Address Resolution Protocol) es un protocolo utilizado para mapear direcciones MAC a direcciones IP, permitiendo que dispositivos sin configuración de IP obtengan su dirección IP basada en su dirección MAC. Cuando un dispositivo necesita conocer su dirección IP, envía una solicitud RARP en broadcast a la red, incluyendo su dirección MAC. Esta solicitud es recibida por los servidores RARP en la red, que buscan en sus tablas de asignaciones de direcciones para encontrar la dirección IP correspondiente a la dirección MAC solicitante. Si hay una coincidencia, el servidor responde al dispositivo con la dirección IP correspondiente.

2.3. Análisis del funcionamiento del protocolo ARP usando Packet Tracer

a) Descargue el archivo `Actividad_RP.pkt`. Abrir el archivo desde Packet Tracer. A partir de la topología (Figura 19) se pide:

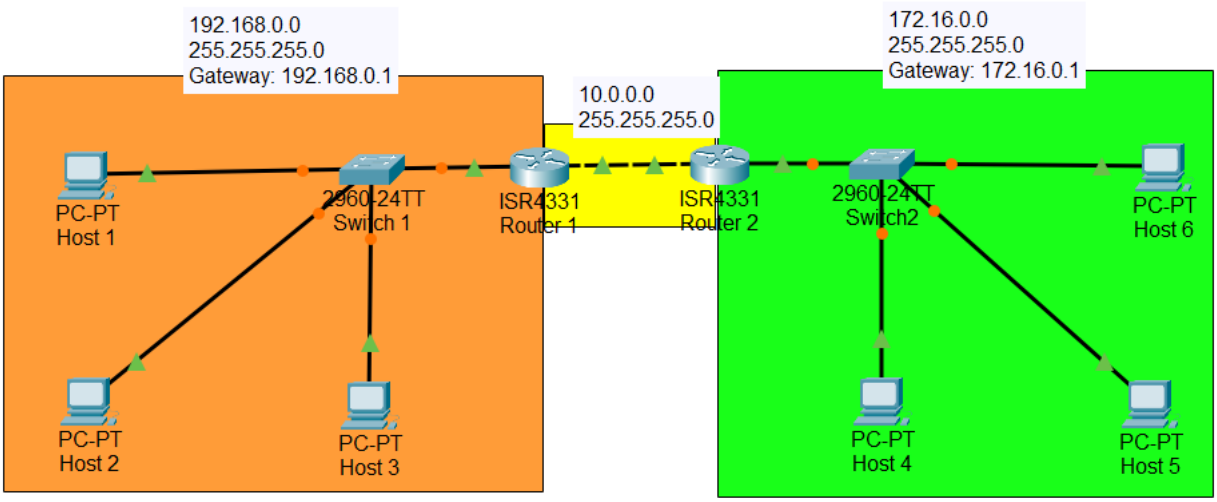


Figura 19: Topologia de red Cisco

- Indicar el número de dominios de colisiones.
- Indicar el número de dominios de `broadcast`.
  Respuesta: Note que cada puerto del switch genera un dominio de colision, y ello genera un solo dominio de broadcast. En el caso de los router tenemos que cada puerto es un dominio de colisión y además de broadcast, sin embargo, tenemos dos router de manera paralela por lo cual solo se genera un dominio de broadcast.
  Contando todos los dominios de colision, que serian basicamente todos los puertos (lineas) tendriamos 9 dominios de colision. Y 3 dominios de broadcast, 2 switch separados(cada switch es un dominio de broadcast) y 2 router en paralelo (1 dominio de broadcast).
  9 dominios de colision 3 dominios de broadcast

b) Complete la Tabla 8 con las direcciones IP de los hosts y de las interfaces de los routers. Sugerencia: Para obtener esta información de los hosts entre a la ventana de comando y ejecute el comando ipconfig. Para el caso de los routers se debe ingresar al modo Config y luego seleccionar las distintas interfaces.

c) Verfique que las tablas ARP de los hosts se encuentren vacías, de lo contrario utilice el comando `arp -d *` para borrarla. Luego verifique la tabla ARP del router, para esto debe ingresar al modo CLI (interfaz de línea de comandos) y ejecute los siguientes comandos:

Router > enable
Router# show ip arp `Router >`

Dispositivo	Interface	IP Add.	Mask	Default Gateway
Host 1	FastEthernet0	192.168.0.2	255.255.255.0	192.168.0.1
Host 2	FastEthernet0	192.168.0.3	255.255.255.0	192.168.0.1
Host 3	FastEthernet0	192.168.0.4	255.255.255.0	192.168.0.1
Host 4	FastEthernet0	172.16.0.2	255.255.255.0	172.16.0.1
Host 5	FastEthernet0	172.16.0.3	255.255.255.0	172.16.0.1
Host 6	FastEthernet0	172.16.0.4	255.255.255.0	172.16.0.1
Router 1	GigabitEthernet0	10.0.0.1	255.255.255.0	192.168.0.1
Router 2	GigabitEthernet0	10.0.0.2	255.255.255.0	172.16.0.1

Tabla 8: Tabla de direccionamiento.

Router > enable

Router# show ip arp

Respuesta: Para vaciar el arp de los Host, los computadores se ingresa a la terminal de comandos CMD y se usa el comando arp -d, en el caso de los router primero se necesita utilizar CTRL+Z luego escribir el comando enable, para finalmente vaciar la tabla ARP con clear arp.

d) Seleccione el modo Simulation, edite el filtro de paquetes y habilite sólo los protocolos ARP e ICMP. Luego realice un ping entre el host1 y el host6 y realice un seguimiento de los distintos paquetes generados en este proceso, para esto haga *click* en el botón de *Forward* (avanzar) en forma secuencial. Explique cómo el protocolo ARP hace posible que se realice en intercambio de paquetes entre las 2 redes.

Respuesta: El host 1 envia un ping, el cual es recibido por el switch, luego el switch intenta enviar el paquete a todos los equipos conectados del area local 192.168.0.0, recibiendo como respuesta un error, luego el switch intenta enviar el paquete al router 1, el cual retorna error de igual manera, se lo envia al router 2, pasandoselo al switch 2, el cual nuevamente envia el paquete a todos los equipos conectados del area local 172.16.0.0, recibiendo error, este proceso lo realiza dos veces por lo cual siempre se pierden dos paquetes, sin embargo, en este proceso las direcciones IP y MAC se almacenan en los ARP de los router, por lo cual los siguientes dos paquetes se mandan directamente sin problemas desde el host1, hacia el switch 1, hacia el router 1, hacia el router 2, hacia el switch 2 y hacia el host6, luego se devuelve hasta llegar al host 1 haciendo la confirmación del ping. *Es así como al final del proceso el protocolo ARP guardara todas las direcciones IP y MAC de los dispositivos que desean comunicarse.*

e) Pase al modo Realtime y verifique el estado de las tablas ARP y borre su contenido. Verifique las entradas de las tablas ARP de los routers.

Realice un ping a la direccion IP de broadcast de la red 172.16.0.0 usando el siguiente comando Router ping ip 172.16.0.255. Verifique el contenido de la tabla ARP del router. Comente.

Respuesta:

Se muestran a continuacion las tablas del router 1, y el router 2 después de haber realizado el experimento de ping entre el host 1 y el host 6, posterior a ello se muestra la tabla arp del router 2 después de hacer un ping en broadcast.

```
Router2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1               1   00E0.A302.1701  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.2               -   0004.9A0A.6401  ARPA   GigabitEthernet0/0/0
Internet  172.16.0.1              -   0004.9A0A.6402  ARPA   GigabitEthernet0/0/1
Internet  172.16.0.4              1   00D0.58B9.0E96  ARPA   GigabitEthernet0/0/1
Router2#
```

Figura 20: Tabla ARP Router 2 después de la simulacion

```
Router1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1                -   00E0.A302.1701  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.2                5   0004.9A0A.6401  ARPA   GigabitEthernet0/0/0
Internet  192.168.0.1              -   00E0.A302.1702  ARPA   GigabitEthernet0/0/1
Internet  192.168.0.2              5   000C.CF47.5318  ARPA   GigabitEthernet0/0/1
Router1#
```

Figura 21: Tabla ARP Router 1 después de la simulacion

Note que las tablas de los router ARP tienen la dirección ip del host asociado a su area local, la tabla ARP del router 1 tiene la direccion del host1
192.168.0.2 además de su mac, y la tabla ARP del router 2 tiene la dirección del host2 172.16.0.4, además ambos router ahora tienen la dirección ip del otro, además de su mac, esto para una correcta comunicación.

A continuacion se muestra la figura de la tabla ARP del router2 después de hacer un ping broadcast.

```
Router2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.1               9   00E0.A302.1701  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.2               -   0004.9A0A.6401  ARPA   GigabitEthernet0/0/0
Internet  172.16.0.1              -   0004.9A0A.6402  ARPA   GigabitEthernet0/0/1
Internet  172.16.0.2              0   0001.42CB.ED77  ARPA   GigabitEthernet0/0/1
Internet  172.16.0.3              0   000A.F332.222C  ARPA   GigabitEthernet0/0/1
Internet  172.16.0.4              9   00D0.58B9.0E96  ARPA   GigabitEthernet0/0/1
Router2#
```

Figura 22: Tabla ARP Router 2 después del ping broadcast

Note que ahora la tabla ARP del router2 guarda las direcciones ip y mac de toda el área local, esto ya que basicamente se hizo un ping a través del protocolo ICMP a todos los computadores del área local.

f) `Nuevamente borre las tablas ARP de los hosts y de los routers. Abra la ventana de comandos del host1 y realice un ping al host6. Explique lo ocurrido con el primer paquete.`

Respuesta:

Lo que ocurre con el primer paquete es que este se termina perdiendo, esto debido a que la tabla ARP tanto del router 1, como del router 2 se encuentran totalmente vacias por lo cual desconocen el área local, es decir las direcciones IP y MAC asociadas a cada computador, sin embargo este primer paquete no se pierde sin ningún proposito, generalmente al hacer un ping a través de ICMP y una red ARP los primeros dos paquetes se encargan de rellenar las tablas ARP de los router, para que los siguientes ping, paquetes a enviar se envien sin ninguna clase de problema.

3. Conclusiones y comentarios

En este laboratorio se estudio acerca del protocolo ARP en mayor profundidad, para ello fue necesario analizarlo de forma explicita a través del OS, sea Windows o Ubuntu, luego se examinó con mayor profundidad a través de los software WireShark y Cisco Packet Tracer. Se concluye que ahora se posee mayor conocimiento acerca del protocolo anteriormente mencionado.

Como comentarios se puede decir que hubo dificultades en la actividad de 2.3 por parte del integrante Dylan Barahona, esto debido a la poca experiencia en el programa Cisco Packet Tracer. Sin embargo, estos se pudieron solucionar con una mayor interacción y dedicación de tiempo al programa.