

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

## Sección 7 Grupo 4

Sebastian Quintero; Sebastian Saldivia; Lucas Herrada; Matias Caceres  
e-mail: sebastian.quintero@mail.udp.cl; lucas.herrada@mail.udp.cl.

Abril - 2025

## Índice

<b>1. Equipos y materiales</b>	<b>2</b>
<b>2. Actividades</b>	<b>2</b>
2.1. Uso del comando <i>arp</i> . . . . .	2
2.2. Captura y análisis de mensajes ARP usando Wireshark . . . . .	6
2.3. Análisis del funcionamiento del protocolo ARP usando Packet Tracer . . . .	11
<b>3. Conclusiones</b>	<b>13</b>

## 1. Equipos y materiales

Este experimento se realizó gracias a que contamos con un computador, junto al programa de detección de paquetes Wireshark y Packet Tracer. También se accedió a un router para obtener la información de la Red.

## Lista de Materiales

Tabla 1: Lista de materiales

Ítem	Descripción	Cantidad
1	Router inalámbrico doméstico	1
2	Computadora personal (PC)	1
3	Aplicación: Wireshark (software)	1
4	Aplicación: Packet Tracer (software)	1

## 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).

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : 
Descripción . . . . . : Intel(R) Ethernet Connection I219-LM
Dirección física. . . . . : EC-8E-B5-9D-F8-3E
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv4. . . . . : 192.168.101.6(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : sábado, 12 de abril de 2025 21:00:03
La concesión expira . . . . . : viernes, 18 de abril de 2025 21:00:04
Puerta de enlace predeterminada . . . . . : 192.168.101.1
Servidor DHCP . . . . . : 192.168.101.1
Servidores DNS. . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Figura 1: Comando *ipconfig*

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

**R:**

Dirección ip: 192.168.101.6

Dirección MAC: EC-8E-B5-9D-F8-3E

La información se obtuvo al ejecutar el comando *ipconfig* y localizando en los datos correspondientes de *ip* y la dirección física que nos proporcionó la interfaz.

3. En la ventana de comandos escribir el comando *arp* y analice los resultados.

```
C:\Users\lbhvl>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

C:\Users\lbhvl>
```

Figura 2: Comando *arp*.

4. ¿Qué comando usaría para mostrar todas las entradas de la tabla ARP?  
-**R:**Para mostrar todas las entradas de la tabla ARP el comando adecuado es arp -a, dicho comando se encarga de mostrar todas las entradas ARP conocidas por el sistema.
5. ¿Qué comando usaría para borrar todas las entradas de la tabla ARP (purgar la tabla ARP)?  
-**R:**El comando para borrar todas las entradas de la tabla ARP es arp -d, se encarga de eliminar todas las entradas actuales de la tabla.
6. ¿Qué comando usaría para eliminar una entrada específica de la tabla ARP?  
-**R:**Para borrar una entrada en específico dentro de la tabla ARP el comando que se debe utilizar es el siguiente arp -d (dirección ip), donde la dirección ip es la dirección específica que se quiere eliminar.
7. ¿Qué comando usaría para agregar una entrada ARP estática en la tabla ARP?  
-**R:**El comando arp -s (dirección ip) (dirección Mac) permite agregar una entrada ARP estática dentro de la tabla, se asigna una dirección ip con una dirección física de forma manual.
8. Indique la diferencia entre una entrada ARP dinámica y una estática.  
-**R:**Las entradas ARP dinámicas se crean automáticamente cuando un dispositivo necesita comunicarse y es eliminada después de un tiempo de no uso, por otro lado, una entrada ARP estática se debe configurar manualmente y es permanente lo cual significa que no importa el estado de inactividad de la entrada, además no cambia aunque la dirección MAC varíe.

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

Interfaz: 26.116.236.45 --- 0x4
Dirección de Internet      Dirección física      Tipo
26.0.0.1                  02-00-00-00-51-00    dinámico
26.255.255.255            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
239.255.255.250           01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.101.6 --- 0x14
Dirección de Internet      Dirección física      Tipo
192.168.101.1             58-25-75-2e-0f-91    dinámico
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251               01-00-5e-00-00-fb    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático
```

Figura 3: Comando *arp -a*

9. Verifique el contenido de su tabla ARP, para esto utilice el comando *arp -a*. Comente los resultados.

**-R:**La lista en pantalla muestra los dispositivos que se encuentran activos en la red local y a su vez sus propias direcciones físicas, esto permite identificar posibles dispositivos desconocidos en la red.

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.

**-R:**La tabla se vació eliminando las conexiones entre direcciones ip y direcciones MAC previamente establecidas. Debido a esto el sistema está obligado a enviar nuevas solicitudes ARP en el momento que necesite comunicarse con algún otro dispositivo en la red.

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

C:\WINDOWS\system32>arp -a

Interfaz: 26.116.236.45 --- 0x4
Dirección de Internet      Dirección física      Tipo
224.0.0.22                01-00-5e-00-00-16    estático

Interfaz: 192.168.101.6 --- 0x14
Dirección de Internet      Dirección física      Tipo
192.168.101.1             58-25-75-2e-0f-91    dinámico
224.0.0.22                01-00-5e-00-00-16    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático
```

Figura 4: Tabla ARP post comando *arp -d*

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?

**R:** El comando ping se realizo pero no genero respuestas debido a seguridad de los dispositivos los cuales bloquean los ping de broadcast, aun asi al verificar nuevamente

la tabla de ARP se observa que se detectaron 2 dispositivos en la red LAN, en los cuales sus direcciones MAC aparecen como dinámicas lo que demuestra que hubo comunicación con estos.

12. ¿Cuántos dispositivos de red existen en su WLAN?. ¿Podría dibujar la topología lógica?.

**R:** Existen 2 dispositivos de red.

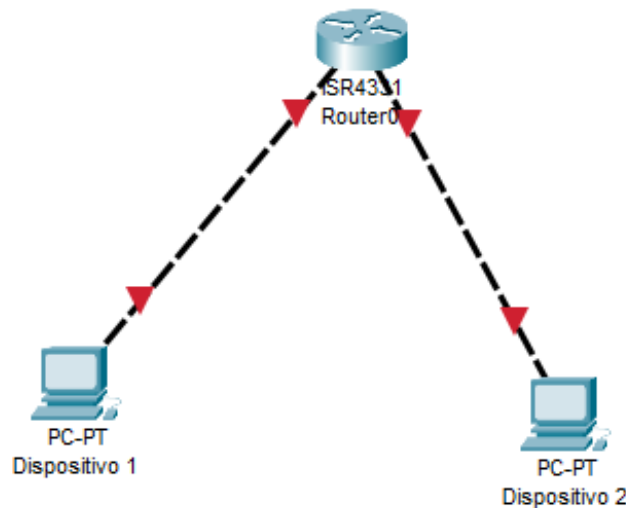


Figura 5: Topología logica.

## 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.
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:

The screenshot shows a Wireshark packet capture. The packet list on the left shows a series of packets. The selected packet is an ARP request (No. 6013). The packet details pane on the right shows the structure of the ARP request:

- Ethernet II, Src: HuaweiTechno\_2e:0f:91 (58:25:75:2e:0f:91), Dst: 12:65:64:7c:13:55 (12:65:64:7c:13:55)
- Internet Protocol Version 4, Src: 192.168.101.1, Dst: 192.168.101.2
- Address Resolution Protocol (request)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: request (1)
  - Sender MAC address: HuaweiTechno\_2e:0f:91 (58:25:75:2e:0f:91)
  - Sender IP address: 192.168.101.1
  - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  - Target IP address: 192.168.101.2

Figura 6: Primer paquete ARP capturado.

- Complete la Tabla 2 con la información de las direcciones MAC del primer mensaje (ARP *request*).

Campo	Valor
MAC emisor	58:25:75:2e:0f:91
MAC receptor	12:65:64:7C:13:55

Tabla 2: Direcciones MAC del mensaje ARP *request*

- ¿Qué valor en hexadecimal toma una dirección MAC del tipo broadcast?
 

**R:** Una dirección MAC de tipo broadcast toma el valor hexadecimal FF:FF:FF:FF:FF:FF
- Complete la Tabla 3 con la información de los campos del mensaje ARP *request*.

Address Resolution Protocol (request)	
Hardware type	Ethernet
Protocol type	IPv4
Hardware size	6
Protocol size	4
Opcode	request
Sender MAC address	58:25:75:2e:0f:91
Sender IP address	192.168.101.1
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.101.2

Tabla 3: Estructura del mensaje ARP *request*.

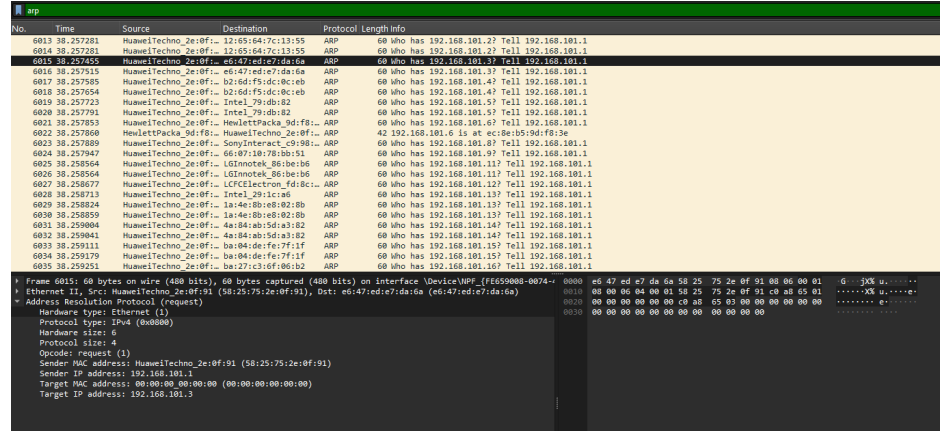


Figura 7: Segundo paquete ARP capturado.

- Complete la Tabla 4 con la información de las direcciones MAC del segundo mensaje (ARP *reply*).

Campo	Valor
MAC emisor	58:25:75:2e:0f:91
MAC receptor	e6:47:ed:e7:da:6a

Tabla 4: Direcciones MAC del mensaje ARP *reply*

- Complete la Tabla 5 con la información de los campos del mensaje ARP *reply*.

Address Resolution Protocol (reply)	
Hardware type	Ethernet
Protocol type	IPv4
Hardware size	6
Protocol size	4
Opcode	request
Sender MAC address	58:25:75:2e:0f:91
Sender IP address	192.168.101.1
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.101.13

Tabla 5: Estructura del mensaje ARP *reply*.

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

**R:** Sí, es necesario que los mensajes ARP request se transmitan en un frame con una dirección MAC de destino del tipo broadcast. Esto se debe a que el dispositivo que

envía el ARP request no conoce todavía la dirección MAC del destinatario, por lo que necesita que todos los dispositivos de la red local reciban el mensaje y, en particular, que lo responda aquel cuya dirección IP coincida con la consultada. El uso del broadcast garantiza que el mensaje llegue a todos los nodos dentro del dominio de broadcast de la red.

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

No, los mensajes ARP reply no son de tipo broadcast sino de tipo unicast ya que cuando un dispositivo necesita saber la dirección MAC correspondiente a una IP envía un mensaje ARP request como broadcast el cual va a todos los dispositivos de la red local, para así recibir como respuesta un ARP reply del dispositivo correspondiente a la IP, pero este mensaje ya no es enviado a todos sino directamente al dispositivo que realizó la pregunta por eso los ARP reply son de tipo unicast, ya que van a una dirección MAC específica.

5. ¿Se le ocurre algún motivo para enviar un mensaje ARP *request* dentro de un frame con destino *unicast*?

**R:** Un ARP request se envía dentro de un frame unicast para evitar el tráfico broadcast innecesario, si ya se conoce la MAC de destino. También se usa para revalidar entradas ARP activas.

Analice sus capturas y verifique la existencia de este tipo de mensajes (screenshot).

No.	Time	Source	Destination	Protocol	Length	Info
6013	38.257281	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.2? Tell 192.168.101.1
6014	38.257281	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.2? Tell 192.168.101.1
6015	38.257495	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.3? Tell 192.168.101.1
6016	38.257515	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.3? Tell 192.168.101.1
6017	38.257545	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.4? Tell 192.168.101.1
6018	38.257654	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.4? Tell 192.168.101.1
6019	38.257723	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.5? Tell 192.168.101.1
6020	38.257791	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.5? Tell 192.168.101.1
6021	38.257853	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.6? Tell 192.168.101.1
6022	38.257860	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	42	192.168.101.6 is at ecc8e:b5:9d:f8:3e
6023	38.257889	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.6? Tell 192.168.101.1
6024	38.257947	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.9? Tell 192.168.101.1
6025	38.258564	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.11? Tell 192.168.101.1
6026	38.258564	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.11? Tell 192.168.101.1
6027	38.258677	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.12? Tell 192.168.101.1
6028	38.258713	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.13? Tell 192.168.101.1
6029	38.258824	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.13? Tell 192.168.101.1
6030	38.258859	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.13? Tell 192.168.101.1
6031	38.259004	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.14? Tell 192.168.101.1
6032	38.259041	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.14? Tell 192.168.101.1
6033	38.259111	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.15? Tell 192.168.101.1
6034	38.259179	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.15? Tell 192.168.101.1
6035	38.259251	HuaweiTechno_2e:0f:12:65:64:7c:13:55	12:65:64:7c:13:55	ARP	60	who has 192.168.101.15? Tell 192.168.101.1

Frame 6017: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface DeviceNPF {FE520008-0074-...}	0000	b2 6d f5 dc 0c eb 58 25 75 2e 0f 91 08 06 00 01	...	X5 u...
Ethernet II, Src: HuaweiTechno_2e:0f:91 (58:25:75:2e:0f:91), Dst: b2:6d:f5:dc:0c:eb (b2:6d:f5:dc:0c:eb)	0010	08 00 06 04 00 01 58 25 75 2e 0f 91 c8 a8 65 01	...	XS u...e
Address Resolution Protocol (Request)	0020	00 00 00 00 00 00 c8 a8 65 06 00 00 00 00 00	...	e.....
Hardware type: Ethernet (I)	0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...	.....
Protocol type: IPv4 (0x0800)				
Opcode: request (1)				
Sender MAC address: HuaweiTechno_2e:0f:91 (58:25:75:2e:0f:91)				
Sender IP address: 192.168.101.1				
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)				
Target IP address: 192.168.101.4				

Figura 8: Tercer paquete unicast ARP.

Complete las Tablas 6 y 7. Sugerencia: leer el RFC 1122, section 2.3.2.1 - ARP Cache Validation.

Campo	Valor
MAC emisor	58:25:75:2e:0f:91
MAC receptor	b2:6d:f5:dc:0c:eb

Tabla 6: Direcciones MAC del mensaje *gratuitous* ARP

Address Resolution Protocol (ARP Announcement)	
Hardware type	Ethernet
Protocol type	IPv4
Hardware size	6
Protocol size	4
Opcode	request
Sender MAC address	58:25:75:2e:0f:91
Sender IP address	192.168.101.1
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.101.4

Tabla 7: 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.

**R:** La dirección MAC que se utilizó como origen para enviar los paquetes (ping request) fue `ec:8e:b5:9d:f8:3e`, mientras que la dirección MAC de origen de los mensajes de respuesta (ping reply) fue `58:25:75:2e:0f:91`.

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

**R:** El protocolo ARP no incluye autenticación, lo que provoca que sea vulnerable a ataques que sean como ARP Spoofing, que es utilizado para redireccionar el tráfico.

8. Investigue sobre el funcionamiento del protocolo RARP.

**R:** El protocolo RARP (Reverse Address Resolution Protocol) permitía que un dispositivo que solo conocía su dirección MAC pudiera obtener su dirección IP. Se utilizaba en

entornos donde los equipos no almacenaban su configuración de red localmente, como era común en dispositivos más antiguos o sin disco. Sin embargo, su uso ha quedado prácticamente obsoleto, ya que fue reemplazado por protocolos más completos y flexibles como DHCP, que no solo asignan direcciones IP, sino también otros parámetros de configuración de red.

### 2.3. Análisis del funcionamiento del protocolo ARP usando Packet Tracer

1. Descargue el archivo `Actividad_ARP.pkt`. Abrir el archivo desde Packet Tracer. A partir de la topología (Figura 9) se pide:
  - Indicar el número de dominios de colisiones.
 

**R:** Hay en total 8 dominios de colisiones, uno por cada interfaz de los Switches
  - Indicar el número de dominios de **broadcast**.
 

**R:** En total hay dos dominios de Broadcast, uno por cada router ya que es el que hace de frontera en los dominios broadcast

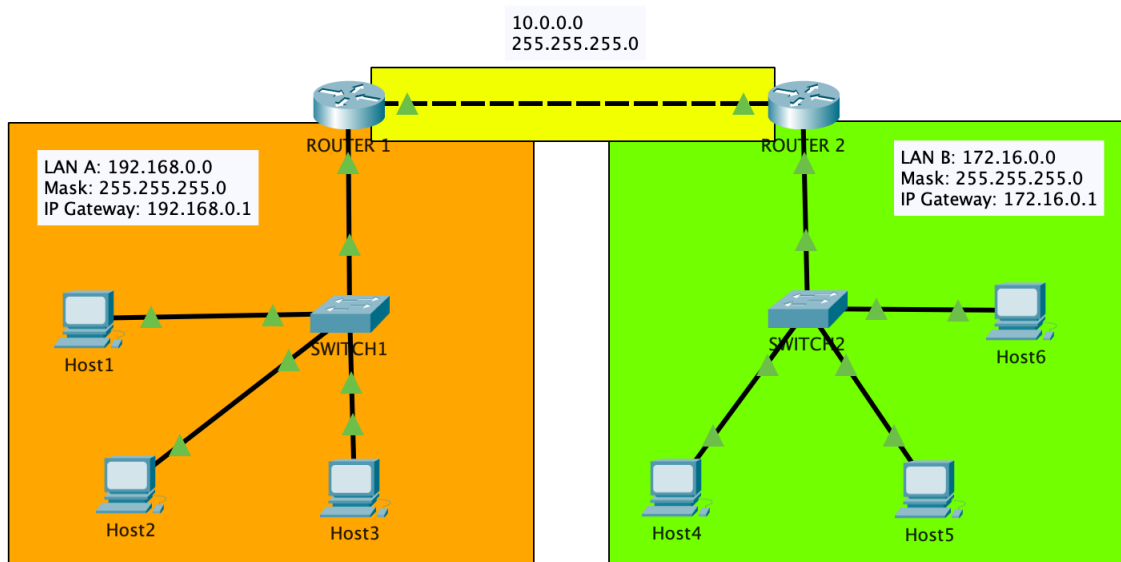


Figura 9: Topología de red utilizada para estudiar funcionamiento de ARP

2. 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.

Dispositivo	Interface	IP Add.	Mask	Default Gateway
Host 1	Fa0/1	192.168.0.2	255.255.255.0	192.168.0.1
Host 2	Fa0/2	192.168.0.3	255.255.255.0	192.168.0.1
Host 3	Fa0/3	192.168.0.4	255.255.255.0	192.168.0.1
Host 4	Fa0/1	172.16.0.2	255.255.255.0	172.16.0.1
Host 5	Fa0/2	172.16.0.3	255.255.255.0	172.16.0.1
Host 6	Fa0/3	172.16.0.4	255.255.255.0	172.16.0.1
Router 1	Gig0/0/1	192.168.0.1	255.255.255.0	
Router 2	Gig0/0/1	172.16.0.1	255.255.255.0	

Tabla 8: Tabla de direccionamiento.

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

- 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 dos redes.

**R:** A continuacion se muestra un paso a paso como el protocolo ARP hace posible la entrega del ping:

- Paso 1:** el pc manda un paquete de request a la puerta de enlace para saber su direccion MAC.
- Paso 2:** el router responde con su MAC y se la envia al pc.
- Paso 3:** el pc registra la MAC en su tabla ARP y arma la trama necesaria para mandar el ping al host6 y se la envia al router.
- Paso 4:** el router 1 recibe la trama y la revisa, se da cuenta que es un paquete ip y revisa su tabla de enrutamiento, como la ip no pertenece a ninguna red a la que posea comunicacion el router 1 arma una trama (esta trama se genera con la MAC del router 2 que es el que administra la otra red y esta MAC se conoce mediante ARP tambien) con el mismo contenido ip y la manda al siguiente Router que es el Router 2.

- e) **Paso 5:**el router 2 recibe la trama y revisa el contenido del protocolo ip y revisa si tiene acceso a esa red, si lo tiene, revisa su tabla ARP para saber que MAC posee la ip al que se desea enviar el mensaje,luego de esto, manda la trama hacia la MAC correspondiente.
- f) **Paso 6:**el host 6 recibe el ping y lo procesa y envia la respuesta.
5. 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 dirección IP de broadcast de la red *172.16.0.0* usando el siguiente comando del Router (ping ip *172.16.0.255*). Verifique el contenido de la tabla ARP del router. Comente.
- R:** Al hacer el ping a la direccion del broadcast desde el router y volver a revisar la tabla ARP del mismo, se puede ver como luego de haber realizado el ping a la direccion de broadcast, el router registro todas las MAC de las direcciones ip que les dio respuesta.
6. 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.
- R:** El primer paquete se demora unos milisegundos de mas en ser enviado, esto debido a que primero se estan obteniendo las MACs necesarias para poder armar la trama que sera enviada al router para que se efectue el ping con normalidad.

### 3. Conclusiones

Con esta actividad, aprendimos el protocolo ARP y cómo funciona. Pudimos comprender la forma en que asigna direcciones MAC a las direcciones IP y cómo dicha información se almacena en una red. También se utilizaron los comandos `arp -a`, `arp -d` y se analizaron las entradas dinámicas y estáticas. Esto aumentó nuestra comprensión de cómo se manejan dichas asociaciones. Con herramientas como Wireshark y Packet Tracer, observamos cómo se generan y transmiten los mensajes ARP en distintas situaciones, incluyendo comunicación dentro de la LAN y también al hacer pings a servidores externos como `google.com`, `facebook.com` o `youtube.cl`, donde analizamos las direcciones MAC involucradas en la entrada y salida de paquetes. También exploramos vulnerabilidades del protocolo, como el ARP spoofing, y repasamos el funcionamiento del protocolo RARP. En resumen, la práctica nos permitió aplicar conocimientos teóricos de las capas 2 y 3 del modelo OSI y adquirir habilidades para analizar, interpretar y diagnosticar el comportamiento de las redes a nivel de direccionamiento y resolución de direcciones.