

TRABAJO PRÁCTICO N°2

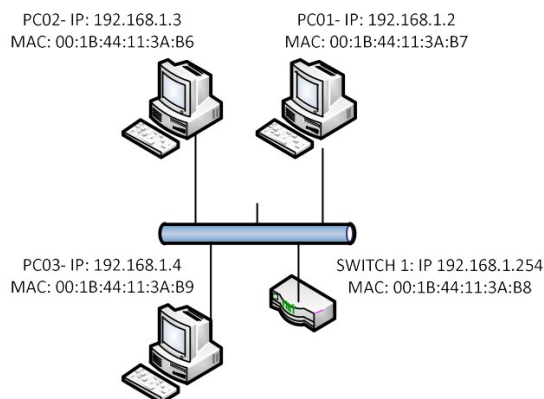
EJERCICIO N°1

Observando la figura 1 y suponiendo que todos los dispositivos se acaban de encender. Represente lo siguiente:

- a) Como están las tablas ARP de cada uno. Justifique.
 Las tablas ARP de cada host están vacías porque todavía no interactúan con otro dispositivo, para hacerlo deben conocer sus direcciones IP.
- b) Como es el intercambio de mensajes cuando la PC 1 le hace un ping a la PC2.
 La PC 1 envía un mensaje al broadcast, el switch al recibirlo pregunta quien es la PC 2 y cual es su numero de MAC, después la PC1 se comunica con la PC2.
- c) Dibuje como quedaría la tabla ARP de cada una de las PC y del switch. Explique cada caso.

Dispositivo	IP	MAC	Tipo
PC01	192.168.1.3	00:1B:44:11:3A:B6	Dinámico
PC02	192.168.1.2	00:1B:44:11:3A:B7	Dinámico
PC03	Vacío	Vacío	Vacío

Figura 1



EJERCICIO N° 2

En base a la figura 2 de una red, determine como sería la trama Ethernet y el paquete IP en los siguientes casos:

- a) Si la PC1, quiere mandarle un mensaje a la PC2.

La PC1 envía un mensaje de difusión con la IP de la PC2 para obtener su MAC.
 La PC2 le responde con un mensaje unicast y su dirección MAC.

Paquete IP

IP Origen: 192.168.1.2
 IP Destino: 192.168.1.3

Trama Ethernet

Mac Origen: 00:1B:44:11:3A:B7
 Mac Destino: 00:1B:44:11:3A:B6

- b) Si la PC1, quiere mandarle un mensaje a la PC3.

La PC1 envía el paquete al Router 1 con dirección MAC 00:1B:44:11:3A:B8.

Luego el Router 1 lo transmite al PC3 con dirección MAC 00:1B:44:11:1A:B8.

Paquete IP	Trama Ethernet
IP Origen: 192.168.1.2	Mac Origen: 00:1B:44:11:3A:B7
IP Destino: 10.0.0.3	Mac Destino: 00:1B:44:11:3A:B6
Puerta Enlace ETH 0: 192.168.1.1	Puerta Enlace ETH 0: 00:1B:44:11:3A:B8
Puerta Enlace ETH 1: 10.0.0.1	Puerta Enlace ETH 1: 00:1B:44:11:3A:B8

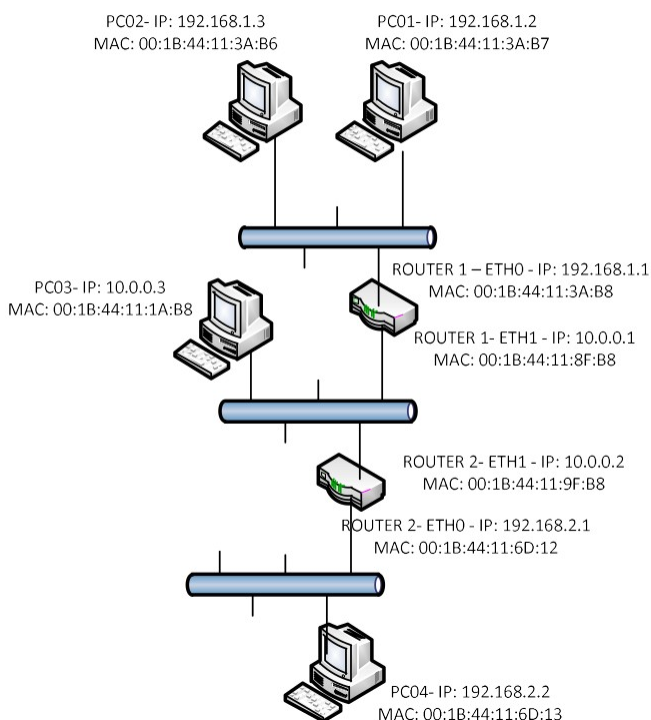
- c) Si la PC1, quiere mandarle un mensaje a la PC4.

La PC1 envía el paquete al Router 1 con dirección MAC 00:1B:44:11:3A:B8, luego lo transmite al Router 2 con dirección MAC 00:1B:44:11:9F:B8, finalmente lo envía a la PC4 con dirección MAC 00:1B:44:11:6D:13.

Paquete IP	
Router 1	IP Origen: 192.168.1.2
	Puerta Enlace ETH 0: 192.168.1.1
	Puerta Enlace ETH 1: 10.0.0.1
Router 2	IP Destino: 192.168.2.2
	Puerta Enlace ETH 0: 192.168.2.1
	Puerta Enlace ETH 1: 10.0.0.2
Trama Ethernet	
Router 1	MAC Origen: 00:1B:44:11:3A:B7
	Puerta Enlace ETH 0: 00:1B:44:11:3A:B8
	Puerta Enlace ETH 1: 00:1B:44:11:8F:B8
Router 2	MAC Destino: 00:1B:44:11:6D:13
	Puerta Enlace ETH 0: 00:1B:44:11:6D:12
	Puerta Enlace ETH 1: 00:1B:44:11:9F:B8

- d) Justifique cada una de las respuestas.

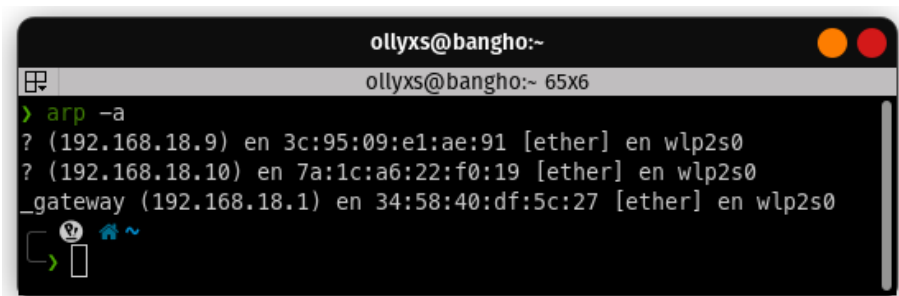
Figura 2



EJERCICIO N° 3

Uso del comando arp:

- a) Ejecute el comando `arp -a`. Mostrar resultado y comentar que significa cada campo de la respuesta.



```
ollyxs@bangho:~  
ollyxs@bangho:~ 65x6  
> arp -a  
? (192.168.18.9) en 3c:95:09:e1:ae:91 [ether] en wlp2s0  
? (192.168.18.10) en 7a:1c:a6:22:f0:19 [ether] en wlp2s0  
_gateway (192.168.18.1) en 34:58:40:df:5c:27 [ether] en wlp2s0
```

Para comentar que significa cada campo usare de ejemplo la primer linea de salida:

?: Es el nombre de host asociado con la dirección IP. En algunos casos, puede aparecer como un signo de interrogación si el nombre de host no está disponible.

(192.168.18.9): Es la dirección IP del dispositivo.

3C:95:09:e1:ae:91: Es la dirección MAC del dispositivo.

[ether]: Es el tipo de dirección MAC que se muestra. En este caso, ether significa que se trata de una dirección MAC de Ethernet.

wlp2s0: Es la interfaz de red a través de la cual se ha comunicado el sistema con el dispositivo. En este caso, wlp2s0 es el nombre de la interfaz inalámbrica.

- b) Ejecute el comando `arp -d *`, y luego `arp -a`. Mostrar resultado y comentar que significa cada campo de la respuesta.

```
ollyxs@bangho:~  
ollyxs@bangho:~ 73x8  
> for ip in $(arp -a | awk '{print $2}' | grep -oP '\d+\.\d+\.\d+\.\d+');  
do  
sudo arp -d $ip  
done  
> arp -a  
_gateway (192.168.18.1) en 34:58:40:df:5c:27 [ether] en wlp2s0  
[?] [?] [?]
```

Nota: El comando 'sudo arp -d *' no funciona correctamente en Linux por lo que hice un for para sacar la lista de ip's del comando 'arp -a' con 'awk' y 'grep', luego este le pasa cada ip a 'sudo arp -d' para poder vaciar la tabla y no tener que escribir ip por ip.

arp -d: en Linux se utiliza para borrar una entrada específica de la tabla ARP del sistema.

arp -a: muestra la tabla ARP del sistema, que es una lista de las direcciones IP y MAC de los dispositivos que se han comunicado con el sistema recientemente.

EJERCICIO N° 4

Ejecute el comando `arp -d*`.

Inicie el sniffer Wireshark, coloque el filtro arp, y comience una captura.

Ejecute el comando ping a www.google.com. Pare la captura e indique:

- a) Represente los campos de los paquetes con el protocolo arp.

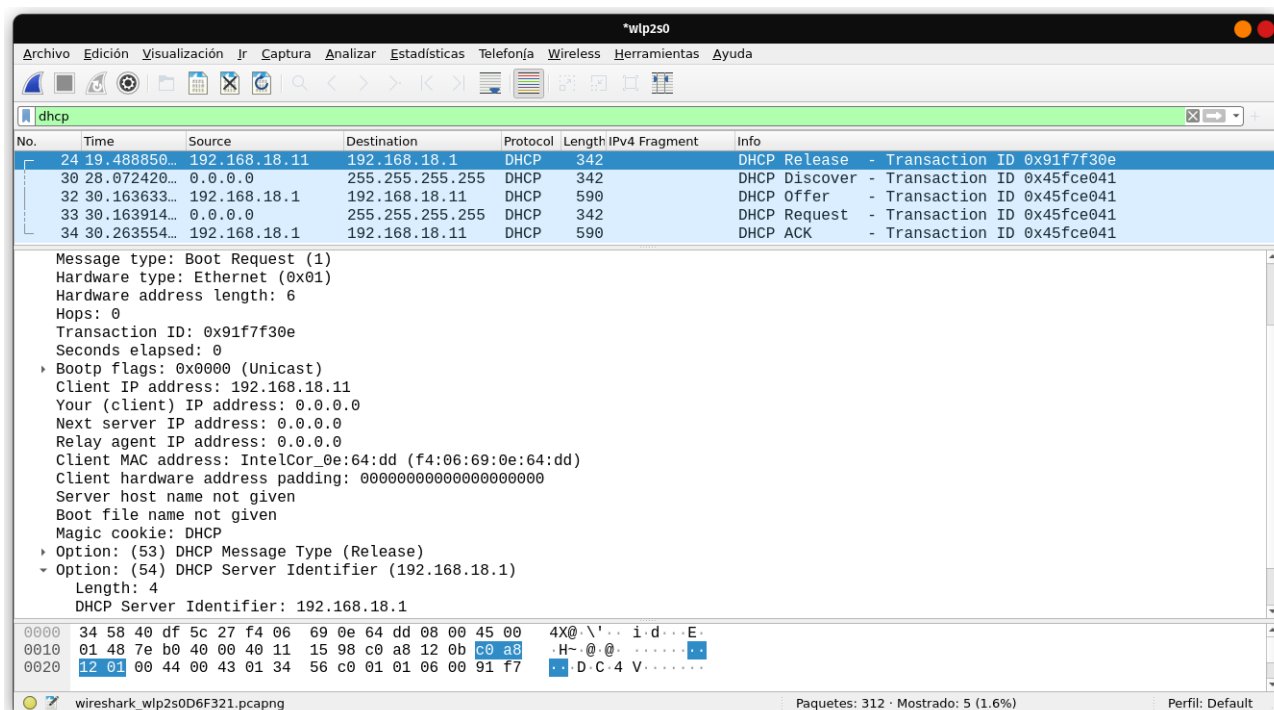
```
▶ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0  
▶ Ethernet II, Src: HuaweiTe_df:5c:27 (34:58:40:df:5c:27), Dst: IntelCor_0e:64:dd (f4:06:69:0e:64:dd)  
▼ Address Resolution Protocol (reply)  
  Hardware type: Ethernet (1)  
  Protocol type: IPv4 (0x0800)  
  Hardware size: 6  
  Protocol size: 4  
  Opcode: reply (2)  
  Sender MAC address: HuaweiTe_df:5c:27 (34:58:40:df:5c:27)  
  Sender IP address: 192.168.18.1  
  Target MAC address: IntelCor_0e:64:dd (f4:06:69:0e:64:dd)  
  Target IP address: 192.168.18.11
```

- b) Indique específicamente los campos de direcciones origen y destino en dichos paquetes y comente.

Sender MAC address: HuaweiTe_df:5c:27 (34:58:40:df:5c:27)
Sender IP address: 192.168.18.1
Target MAC address: IntelCor_0e:64:dd (f4:06:69:0e:64:dd)
Target IP address: 192.168.18.11

EJERCICIO N° 5

Utilizando la herramienta Wireshark, realice una captura de las tramas correspondientes a la realización de un intercambio de mensajes DHCP. Resuelva:



Para poder capturar en Wireshark los paquetes DHCP debemos inicializar el mismo, y luego proceder a ejecutar los comandos 'sudo dhclient -r' y 'sudo dhclient -v'.

- a) ¿Cuántos servidores DHCP existen en su red?

Existe solo 1.

- b) ¿Cuál es la IP del servidor DHCP?

La dirección IP del servidor DHCP es 192.168.18.1

- c) Definir qué mensajes son unicast y cuales son broadcast. ¿Por qué?

Unicast: En este caso, los paquetes con las líneas 1, 3 y 5 son unicast, ya que tienen una dirección IP de origen y una dirección IP de destino específicas.

Broadcast: En este caso, los paquetes con las líneas 2 y 4 son broadcast, ya que tienen la dirección IP de destino 255.255.255.255, lo que significa que están dirigidos a todos los dispositivos de la red.

- d) ¿Qué IP ofreció el DHCP?

```
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.18.11
```

- e) ¿Qué IP acepto el cliente?

```
Option: (50) Requested IP Address (192.168.18.11)
Length: 4
Requested IP Address: 192.168.18.11
```

- f) Que otros datos puede ver en los mensajes DHCP. Explique.

- Tipo de mensaje DHCP (Discover, Offer, Request, Acknowledge, Release)
- Dirección IP del cliente
- Dirección IP del servidor
- Máscara de red
- Puerta de enlace predeterminada
- Servidores DNS primarios y secundarios
- Duración del alquiler de la dirección IP
- Identificador de transacción DHCP