# U2. Práctica 2:
# Comandos de red y WireShark

**1** Realiza un pantallazo de los comandos ipconfig, ifconfig o ip addr e indica la dirección IP del ordenador, indica tu IPv6, la puerta de enlace y la dirección MAC del interfaz empleado.

```
Sufijo DNS específico para la conexión. . :
Descripción . . . . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Dirección física. . . . . . . . . . . . : 8C-70-5A-47-2B-14
DHCP habilitado . . . . . . . . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::d150:182f:c972:ca1c%10(Preferido)
Dirección IPv4. . . . . . . . . . . . . : 192.168.0.20(Preferido)
Máscara de subred . . . . . . . . . . . : 255.255.255.0
Concesión obtenida. . . . . . . . . . . : sábado, 7 de noviembre de 2020 15:39:30
La concesión expira . . . . . . . . . . : domingo, 8 de noviembre de 2020 21:52:17
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . . . . . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . . . . . . . . . . : 76312666
DUID de cliente DHCPv6. . . . . . . . . : 00-01-00-01-26-F0-23-7C-A0-B3-CC-C9-09-BE
Servidores DNS. . . . . . . . . . . . . : 192.168.0.1
NetBIOS sobre TCP/IP. . . . . . . . . . : habilitado
```

**2** Si tenemos un fallo en la red podemos realizar algunas comprobaciones:

**2.a** Compruebe si tu tarjeta de red funciona correctamente haciendo un ping a su propio ordenador: ping 127.0.01. Pon una captura de pantalla.

```
C:\Users\juanf>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\juanf>
```

**2.b** Compruebe su IP, ¿qué estaría pasando si tiene asignada la IP 169.254.12.35?

```
C:\Users\juanf>ping 169.254.12.35

Haciendo ping a 169.254.12.35 con 32 bytes de datos:
Respuesta desde 192.168.0.20: Host de destino inaccesible.
Respuesta desde 192.168.0.20: Host de destino inaccesible.
Respuesta desde 192.168.0.20: Host de destino inaccesible.
Respuesta desde 192.168.0.20: Host de destino inaccesible.

Estadísticas de ping para 169.254.12.35:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

C:\Users\juanf>
```

Tendría un fallo en el envío de paquetes ICMP, me avisaría de tal error

**2.c** ¿Cómo puede comprobar si está conectado al router? Realice una captura.

```
C:\Users\juanf>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=3ms TTL=64

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 3ms, Media = 2ms
```

Para comprobar si estoy conectado al router haré ping a mi puerta de enlace.

**2.d** Compruebe si tiene salida por ejemlo, si se conecta al servidor DNS de Google 8.8.8.8 y realice una captura.

```
C:\Users\juanf>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=11ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=12ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=12ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=12ms TTL=118

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 11ms, Máximo = 12ms, Media = 11ms

C:\Users\juanf>
```

**2.e** ¿Cuál es su IP pública? Pista: https://www.whatismyip.com/

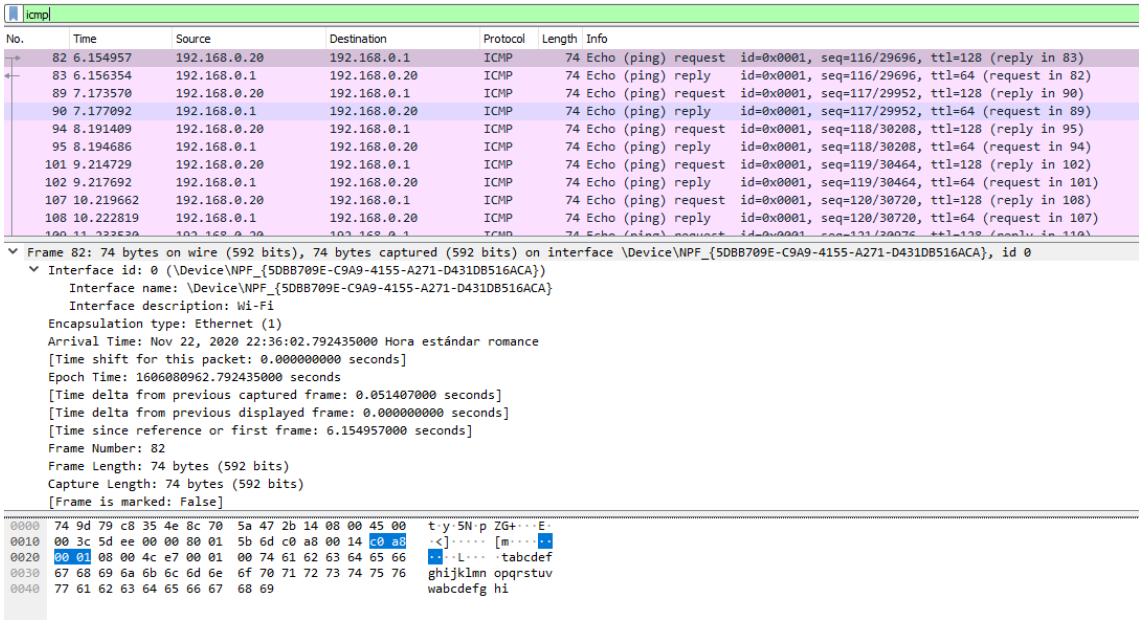

**3** Haciendo uso del comando arp, obtenga la tabla ARP de la máquina (Windows o Linux). Describa los distintos campos y adjunte una captura de pantalla.

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

Interfaz: 192.168.0.20 --- 0xa
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           74-9d-79-c8-35-4e     dinámico
  192.168.0.10          ac-9b-0a-d9-b7-d6     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\juanf>
```

Las 3 primeras líneas indican la equivalencia de la MAC respecto la IP del router, mi equipo y la dirección por defecto para preguntar a toda mi red respectivamente.

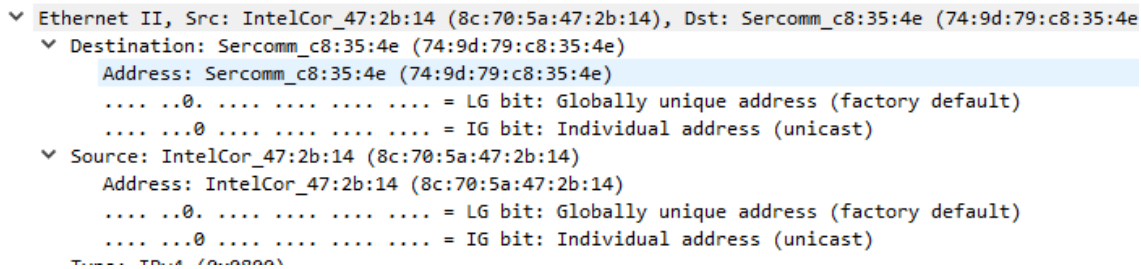
**4** Empleando el programa WireShark, realice los pasos propuestos para analizar el tráfico de red. Documente las pantallas con capturas y justifique las respuestas.

- Abra la aplicación y la consola de comandos y escriba el comando necesario para ejecutar 10 pings a puerta de enlace predeterminada de su red.
- Ponga a captura en la interfaz correspondiente y ejecute el comando.
- Detenga la captura tras los 10 mensajes y responda a las cuestiones siguientes:




**4.a** ¿Cuál es la dirección MAC de origen y de destino?

La MAC esta desplegada tanto en el destination como en el source del siguiente pantallazo.




**4.b** ¿Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.

La dirección de la puerta de enlace sale en el destino de la primera petición.
La MAC esta desplegada tanto en el destination como en el source del primer pantallazo. Es la dirección a la que se dirige la petición.

**4.c** ¿La dirección MAC de origen coincide con la interfaz de tu PC?

Mi puerta de enlace es la interfaz que usa mi equipo para comunicarse, así que la MAC de mi interfaz coincidirá con la MAC del router al que esté conectado.

**4.d** ¿La dirección MAC de destino en WireShark coincide con la dirección MAC de algún equipo?

Con la del router a la que esté conectado.

**4.e** ¿De qué manera su PC obtiene la dirección MAC del PC a la que hizo ping?

Por el protocolo NAT.

**4.f** ¿Cuál es el tamaño total del mensaje ICMP? ¿Cuántos datos se envían dentro del mensaje ICMP?

74 bytes en total, el mensaje ICMP ocupa 32 bytes de los 74.

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
  Interface id: 0 (\Device\NPF_{5DBB709E-C9A9-4155-A271-D431DB516ACA})
      Interface name: \Device\NPF_{5DBB709E-C9A9-4155-A271-D431DB516ACA}
      Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov  7, 2020 22:32:25.448202000 Hora estándar romance
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1604784745.448202000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x543d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 286 (0x011e)
    Sequence Number (LE): 7681 (0x1e01)
    [Request frame: 1]
    [Response time: 9,319 ms]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

**4.g** ¿Cuál es el puerto origen y destino del mensaje ICMP?

```
Transmission Control Protocol, Src Port: 443, Dst Port: 49502, Seq: 32, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 49502
```

**5** Repita el ejercicio anterior pero haciendo ping a www.amazon.es y conteste a las preguntas siguientes:

**5.a** ¿Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.

| No. | Time | Source | Destination |
|---|---|---|---|
| 1 | 0.000000 | 192.168.0.20 | 192.168.0.1 |
| 2 | 0.005726 | 192.168.0.1 | 192.168.0.20 |
| 3 | 0.016345 | 192.168.0.20 | 13.224.118.171 |
| 4 | 0.113907 | 13.224.118.171 | 192.168.0.20 |

Las sombreadas en rosa son las direcciones de las puertas de enlace de los routers de origen y destino

```
Destination: Sercomm_c8:35:4e (74:9d:79:c8:35:4e)
    Address: Sercomm_c8:35:4e (74:9d:79:c8:35:4e)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: IntelCor_47:2b:14 (8c:70:5a:47:2b:14)
    Address: IntelCor_47:2b:14 (8c:70:5a:47:2b:14)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Las direcciones entre paréntesis separadas por dos puntos son las direcciones MAC de los routers de origen y destino.

**5.b** ¿La dirección MAC de origen coincide con la interfaz de tu PC?

Mi puerta de enlace es la interfaz que usa mi equipo para comunicarse, así que la MAC de mi interfaz coincidirá con la MAC del router al que esté conectado.

**5.c** ¿La dirección MAC de destino en WireShark coincide con la dirección MAC del miembro del equipo?

Con la del router a la que esté conectado.

**5.d** ¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?
Por el protocolo NAT.

**5.e** Indique el tamaño del mensaje ICMP y el puerto de origen y destino.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3 | 0.016345 | 192.168.0.20 | 13.224.118.171 | ICMP | 74 | Echo |
| 4 | 0.113907 | 13.224.118.171 | 192.168.0.20 | ICMP | 74 | Echo |
| 5 | 1.036782 | 192.168.0.20 | 13.224.118.171 | ICMP | 74 | Echo |

La pestaña Length informa del tamaño en Mb

A continuación, ejecute en la consola de comandos:

- En Windows: netsh interface ip delete arpcache ipconfig /flushdns
- En Linux: sudo ip neigh flush dev eth0
  sudo /etc/init.d/nscd restart
- Nota: En Linux es possible que el interfaz de llame de otra manera, míralo haciendo ping.

**5.f** Localiza todos los mensajes que han permitido obtener la IP de Amazon (tanto DNS como ARP). ¿Ha cambiado algo respecto al caso analizado en el punto anterior? Justifique la respuesta.

Se ha limpiado la tabla y mi router a vuelto a preguntar a los todos los equipos quién era.