**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.
2. Si tenemos un fallo en la red podemos realizar algunas comprobaciones:
   1. Compruebe si tu tarjeta de red funciona correctamente haciendo un ping a su propio ordenador: ping 127.0.01. Pon una captura de pantalla.
   2. Compruebe su IP, ¿qué estaría pasando si tiene asignada la IP 169.254.12.35?
   3. ¿Cómo puede comprobar si está conectado al router? Realice una captura.
   4. Compruebe si tiene salida por ejemlo, si se conecta al servidor DNS de Google 8.8.8.8 y realice una captura.
   5. ¿Cuál es su IP pública? Pista: [https://www.whatismyip.com/](https://www.whatismyip.com/es/)
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.
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:
   1. ¿Cuál es la dirección MAC de origen y de destino?
   2. *¿*Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.
   3. ¿La dirección MAC de origen coincide con la interfaz de tu PC?
   4. ¿La dirección MAC de destino en WireShark coincide con la dirección MAC de algún equipo?
   5. ¿De qué manera su PC obtiene la dirección MAC del PC a la que hizo ping?
   6. ¿Cuál es el tamaño total del mensaje ICMP? ¿Cuántos datos se envían dentro del mensaje ICMP?
   7. ¿Cuál es el puerto origen y destino del mensaje ICMP?
5. Repita el ejercicio anterior pero haciendo ping a [www.amazon.es](http://www.amazon.es) y conteste a las preguntas siguientes:
   1. ¿Puede ver en el mensaje la dirección IP de la puerta de enlace? ¿Y su MAC? Justifique todas las respuestas.
   2. ¿La dirección MAC de origen coincide con la interfaz de tu PC?
   3. ¿La dirección MAC de destino en WireShark coincide con la dirección MAC del miembro del equipo?
   4. ¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?
   5. Indique el tamaño del mensaje ICMP y el puerto de origen y destino.

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.
  1. 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.