

# PL3: Wireshark ICMP y DHCP en IPv4

**Nombre: Raúl López Llana**

**Grupo: Tarde**

## OBJETIVOS.

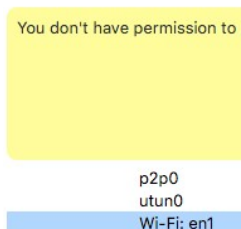
El objetivo de esta práctica es comprender el funcionamiento de los protocolos ICMP y DHCP. Para ello emplearemos el analizador de protocolos Wireshark. Hay que instalar Wireshark y Forticlient (se explica mas adelante) en un ordenador conectado a una red Wi-Fi.

## EJERCICIO 1, ICMP

Ejecute Wireshark y capture en el interfaz Wi-Fi o el interfaz de red de área local con el que esté conectado, seleccionándolo de la lista de la parte de abajo.

### Capture

...using this filter:



Seguir las instrucciones específicas para cada sistema operativo que se indican a continuación.

### LINUX

```
$ sudo wireshark
```

Para averiguar la ruta “default” prueba con alguno de estos tres comandos

```
$ netstat -rn
$ route -n
$ ip route list
```

### MAC OS

Puede haber problemas con permisos, en tal caso abrir un terminal y ejecutar

```
$ sudo chmod g+r /dev/bpf*
$ sudo chgrp admin /dev/bpf*
```

Para averiguar la ruta default:

```
[Jones-iMac:Downloads jmarco$ netstat -rn
Routing tables
```

```
Internet:
Destination      Gateway          Flags           Refs      Use    Netif  Expire
default          192.168.1.1     UGSc            107       0      en1
```

### WINDOWS

Abrir un terminal en “Buscar” teclear la orden “cmd” y ejecutar

```
$ ipconfig
```

La entrada default es la IP “Puerta de enlace predeterminada”

```
Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::e0cd:514e:fd5
    Dirección IPv4. . . . . : 192.168.1.45
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

## EN CUALQUIER SISTEMA OPERATIVO

Vamos a hacer un ping al router Wi-Fi con el que salimos a Internet (entrada “default” de la tabla de rutas). Haga un ping de tres o cuatro mensajes a la IP de la entrada default, ejecutando el comando y parándolo con Ctrl + C.

```
$ ping 192.168.1.1
```

Cuando se complete la ejecución de la orden, detenga Wireshark (para evitar capturar mucho tráfico basura, se recomienda estar capturando durante el menor tiempo posible), filtre el tráfico ICMP (filtro icmp) que tenga como origen o destino su equipo y localice las tramas que corresponden a los mensajes ICMP generados por el ping. Responda a las siguientes cuestiones:

### 1.1. ¿Cuáles son las direcciones IP origen y destino de las tramas ICMP que observa?

La dirección origen es la 192.168.11.2 y la destino 192.168.11.152.

3	0.351088801	192.168.11.2	192.168.11.152	ICMP	98 Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 4)
---	-------------	--------------	----------------	------	--

La dirección destino es mi default gateway y la dirección origen es la dirección con la que salgo hacia el exterior a través de la interfaz wifi.

### 1.2. Identifique los distintos tipos de mensajes ICMP que se producen con su tipo y código.

Se producen tres tipos de mensajes. El primero de ellos es de tipo 8 y código 0 que es un echo ping request, una petición ping,

```

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x97d9 [correct]

```

Otro es de tipo 0 y código 0 que es la respuesta a ese ping(reply)

```

Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x9fd9 [correct]
[Checksum Status: Good]

```

y el otro es de tipo 3 y código 13 que nos indica que es imposible llegar a la dirección de destino, esto se debe a que nosotros hemos interrumpido el propio comando.

Arranque de nuevo el Wireshark y aumente el tamaño del mensaje que emplea el ping del apartado anterior (con tres mensajes es suficiente, parar con Ctrl + C) hasta 2000 bytes (en Linux hay que usar la opción -s)

LINUX Y MAC

```
$ ping -s 2000 x.x.x.x
```

WINDOWS

```
$ ping -l 2000 x.x.x.x
```

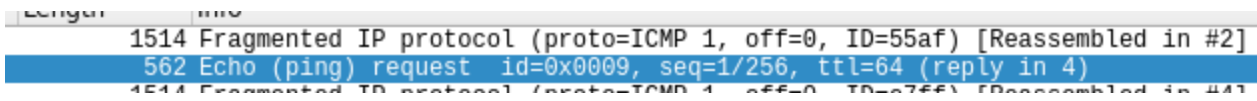
### 1.3. ¿Cuántos paquetes IP recibe como respuesta por cada mensaje ICMP original? En Wireshark se recomienda leer detenidamente el campo “Info”, desplegar y analizar las pestañas de “Internet Protocol” e “Internet Message Control Protocol”

Recibe por cada mensaje ICMP 2 fragmentos que compondrán la respuesta a la petición, el primero de 1514 bytes y el segundo de 562 bytes. Teóricamente el tamaño máximo de un datagrama ip es 65536 pero realmente es más pequeño.

2	0.000026314	192.168.11.2	192.168.11.152	ICMP	562 Echo (ping) request id=0x0009, seq=1/256, ttl=64 (reply in 4)
3	0.019675971	192.168.11.152	192.168.11.2	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e7ff) [Reassembled in #4]
4	0.019676120	192.168.11.152	192.168.11.2	ICMP	562 Echo (ping) reply id=0x0009, seq=1/256, ttl=64 (request in 2)

## 1.4. ¿Cuál es el tamaño de cada uno?

El primero de 1514 bytes y el segundo de 562 bytes.

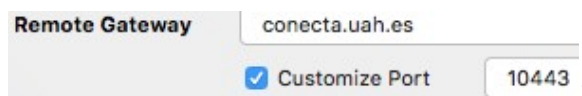


## 1.5. ¿Puede explicar qué está ocurriendo?

Lo que ocurre es que el tamaño del datagrama que queremos enviar (ping de 2000Bytes) es superior al ancho de banda por lo que tendrá que dividirlo para poder enviarlo.

## EJERCICIO 2

Realizamos ahora un ping a una dirección web siguiendo las mismas instrucciones de captura que en el ejercicio anterior. Para evitar algunos problemas vamos a realizarlos como si físicamente estuviéramos en la Universidad, para ello nos conectamos a la VPN de la UAH usando el FortiClient con la cuenta UAH y la configuración que se indica en esta figura:



## LINUX

Averiguar el interfaz que usamos en la VPN, en un terminal:

```
$ ip -c a
```

Aparecerá como “vpn:”

## MAC OS

Averiguar el interfaz que usamos en la VPN, en un terminal

```
$ ifconfig
```

Ver cuál es el interfaz point to point:

```
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1354
    inet 192.168.17.33 --> 1.1.1.1 netmask 0xfffff000
```

arrancar las capturas en ese interfaz.

## WINDOWS

Averiguar el interfaz que usamos en la VPN, en un terminal:

```
$ ipconfig
```

Es el primer interfaz de la lista, sale con el nombre “Adaptador de red Ethernet Ethernet 3”

## EN CUALQUIER SISTEMA OPERATIVO

```
$ ping www.rediris.es
```

A los tres mensajes parar el ping y la captura, para quedarnos con el tráfico del ping, filtrar por ICMP y responder a las siguientes preguntas:

2.1. ¿Cuáles son las direcciones IP origen y destino del tráfico ICMP?, ¿son direcciones IP públicas o privadas?

La dirección origen es la 192.168.11.2 y la destino 130.206.13.20.

Time	Source	Destination	Protocol	Length	Info
5 0.466305592	192.168.11.2	130.206.13.20	ICMP	98	Echo (ping)
6 0.640198792	130.206.13.20	192.168.11.2	ICMP	98	Echo (ping)

La dirección destino es la dirección de la página web a la que le estoy haciendo el ping y la dirección origen hace referencia a la dirección con la que me conecto a la vpn.

2.2. Razonad si llevan estos paquetes ICMP puerto origen/destino del nivel de transporte. Se recuerda que la aplicación ping usa directamente ICMP, que a su vez usa IP.

No, no usa puertos de origen o de destino de nivel de transporte ya que ICMP pertenece a la capa de Red, que es un nivel por debajo de la de transporte.

## EJERCICIO 3, TRACEROUTE

Vuelva a arrancar una captura con Wireshark (solo en el interfaz de la VPN) mientras ejecuta:

LINUX

```
$ traceroute www.google.es
```

MAC

```
$ traceroute -n www.google.es
```

WINDOWS

La implementación del traceroute la hacen de forma mas sencilla, mandan un ping al destino subiendo el TTL, por lo que al llegar al destino, no provocan el error de puerto inalcanzable:

```
$ tracert -d www.google.es
```

## EN CUALQUIER SISTEMA OPERATIVO

Detener Wireshark, del resultado del comando copiar la dirección IP de [www.google.es](http://www.google.es) (supongamos que es la 216.58.209.67)

LINUX Y MAC

Filtrar los mensajes con ICMP o UDP, si aparecen muchos mensajes se puede añadir la IP de Google,

```
icmp || udp && ip.addr == 216.58.209.67
```

## WINDOWS

Filtrar los mensajes con ICMP, si aparecen muchos mensajes se puede añadir la IP de Google, icmp && ip.addr == 216.58.209.67

## EN CUALQUIER SISTEMA OPERATIVO

OPCIONAL, si se quiere reducir el número de tramas filtradas, averiguar la IP de nuestro PC en la VPN, en Wireshark en el filtro, indicar que visualice las tramas que tenga la IP de Google o DNS:

```
ip.addr == 216.58.209.67 || dns
```

Habrà una línea donde aparezca la consulta www.google.es al servidor DNS, en este caso hecha desde 192.168.16.220

192.168.16.220	192.168.153.1...	DNS	73	Standard query 0xf7c9 A www.google.es
192.168.153.141	192.168.16.220	DNS	89	Standard query response 0xf7c9 A www.google.es A 216.58.209.67

y añadir a los filtros anteriores:

```
&& ip.addr == 192.168.16.220
```

Responda a las siguientes preguntas:

3.1. Identifique los mensajes que genera su PC. ¿Cuál es valor del campo TTL de todos los datagramas que genera su PC? Analice su secuencia.

Nota: el TTL normal vale 64, cuando tiene un valor muy bajo, puede salir con una línea roja en el Wireshark (Linux/Mac)

Los 3 primeros paquetes tiene un TTL de 1 y van aumentando de uno en uno los tres paquetes que envío ya que necesito hacer una media de cada uno de los nodos intermedios hasta llegar a www.google.es

```
...0 0000 0000 0000 = Fragment Offset: 0
▶ Time to Live: 1
Protocol: UDP (17)
...0 0000 0000 0000 = Fragment Offset: 0
▶ Time to Live: 2
Protocol: UDP (17)
Header Checksum: 0x1df2 [validation disabled]
...0 0000 0000 0000 = Fragment Offset: 0
▶ Time to Live: 3
Protocol: ICMP (1)
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 4
Protocol: ICMP (1)
```

En mi caso solo le hace falta realizar 4 saltos para alcanzar el destino por lo que el máximo TTL de un paquete será 4 y será común para los 3 paquetes que se han enviado al mismo nodo.

3.2. ¿Cuáles son los valores de tipo y código de los mensajes seis primeros ICMP que se reciben? ¿Qué error se está produciendo?

Tipo 11 y código 0 ya que en todos estos se produce el mismo error, Time to live exceeded, ya que tienen un TTL demasiado corto como para llegar a [www.google.es](http://www.google.es) y se mueren antes de llegar

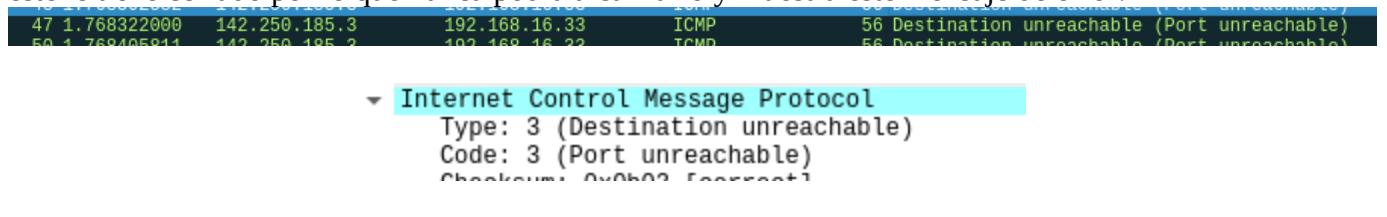
```
Destination Address: 192.168.16.33
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x0e01 [correct]
```

### 3.3. ¿Qué datos contienen dichos mensajes? ¿Guardan relación con los mensajes enviados?

El mensaje contiene datos como la dirección de destino la que nos ha reportado la dns, la dirección de google a la que estábamos intentando llegar, contiene nuestra dirección y contiene un posible comando traceroute con el número de salto y el número de intento .

3.4. ¿Cuál es el tipo y código de los mensajes ICMP recibidos del ordenador destino del traceroute? ¿Qué error se está produciendo?

Tipo 3 y código 3 que significan Destinatario inalcanzable ya que está intentando conectarse a un puerto y este le tiene cerrado por lo que nunca podrá alcanzarlo y muestra este mensaje de error.



## EJERCICIO 4, DHCP

Para esta parte hay que cerrar Forticlient.

Arranque Wireshark y configúrelo para capturar tráfico en el interfaz de red de área local Wi-Fi. Vamos a forzar al PC a que vuelva a adquirir su dirección mediante DHCP. Para ello proceda como se indica a continuación para liberar y obtener nuevos parámetros de red:

### LINUX

`$ sudo /sbin/dhclient -r` (OJO que a veces al pegar el comando el carácter “-” sale mal como “\_”)

Con esto eliminaremos la configuración de red asignada al interfaz de red para obtener una nueva configuración de red:

`$ sudo /sbin/dhclient {interfaz_de_red, esto es opcional}`

### MAC

Ojo ahora hay que trabajar con el interfaz Wi-Fi, el en1, también para la captura con Wireshark. Esto libera y obtiene nuevos parámetros:

`$ sudo ipconfig set en1 DHCP`

### WINDOWS

`$ ipconfig /release`

para obtener nuevos parámetros:

`$ ipconfig /renew`

### EN CUALQUIER SISTEMA OPERATIVO

Cuando el comando se complete, detenga Wireshark, filtre el tráfico DHCP (filtro bootp) que tenga como origen o destino su equipo y responda a las siguientes cuestiones.

4.1. ¿Cuál es el servidor DHCP que está enviando una dirección IP para su equipo?



El servidor DHCP que me está enviando una dirección IP es 192.168.11.152, la dirección broadcast de mi red ya que es por ese sitio donde solicito una dirección IP.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
192.168.11.152	192.168.11.3	DHCP	354	DHCP Offer
0.0.0.0	255.255.255.255	DHCP	344	DHCP Request
192.168.11.152	192.168.11.3	DHCP	354	DHCP ACK

4.2. ¿Cuál es la secuencia de mensajes DHCP que observa desde que se solicita una nueva dirección IP para su equipo hasta que éste la consigue? Recordad de la teoría la secuencia “DORA”.

Realizo un DHCP discover y el servidor me responde ofreciéndome una dirección IP (DHCP offer), mi ordenador le responde con un Request en el que acepta la IP ofrecida y por último el servidor me escribe un ACK a mi mensaje.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
192.168.11.152	192.168.11.3	DHCP	354	DHCP Offer
0.0.0.0	255.255.255.255	DHCP	344	DHCP Request
192.168.11.152	192.168.11.3	DHCP	354	DHCP ACK

4.3. ¿Cuál es la configuración de red IP completa, en concreto, dirección IP, máscara, router, servidor DNS que le asignan a su equipo?

Se asigna a mi equipo:

La dirección IP: 192.168.11.3

Máscara: 255.255.0.0

router: 192.168.11.152

servidor DNS: 192.168.11.152

```

BOOT file name not given
Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Offer)
  ▶ Option: (54) DHCP Server Identifier (192.168.11.152)
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (58) Renewal Time Value
  ▶ Option: (59) Rebinding Time Value
  ▼ Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
  ▶ Option: (28) Broadcast Address (192.168.11.255)
  ▼ Option: (3) Router
    Length: 4
    Router: 192.168.11.152
  ▼ Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 192.168.11.152
  ▶ Option: (43) Vendor-Specific Information
  ▶ Option: (255) End
  Padding: 00

```