

# GP6-PL3: Wireshark ICMP y DHCP en IPv4

Nombres: Álvaro Camacho y Ainara García

Puesto: 5

Grupo: 1

## OBJETIVOS.

El objetivo de esta práctica es comprender el funcionamiento de los protocolos ICMP y DHCP. Para ello emplearemos el analizador de protocolos Wireshark, ya conocido por los alumnos, junto con algunas órdenes que ayudaran a comprender el funcionamiento de ambos protocolos. Esta práctica se hará en los PCs del laboratorio con Windows, aunque si el profesor lo estima conveniente se puede hacer en Linux.

## EJERCICIO 1, ICMP

Ejecute Wireshark, capturar tráfico en el interfaz de red de área local que será la primera que aparezca en con una gráfica pequeña de tráfico. Intentar capturar tráfico durante el menor tiempo posible (para analizar el tráfico con más rapidez).

Abra un terminal, buscando *terminal* o *cmd*. Envíe un `ping` a un equipo situado en su misma red de área local, en caso de usar Windows el Firewall bloquea la respuesta al ping, pero hay otros equipos que contestan:

- 10.0.8.2
- 10.0.11.34
- 10.0.8.46

## LINUX

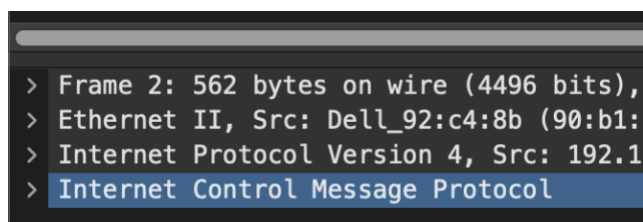
```
$sudo wireshark
```

Abra un segundo terminal. Envíe un `ping` a un PC físicamente más próximo a su puesto de laboratorio<sup>1</sup> y haga un ping a dicho equipo.

```
$ ping 10.x.x.x
```

Tras 2 o 3 pings parar el comando con Ctrl+C, 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`.

Se recuerda que en la parte central del Wireshark hay desplegados (picando en el símbolo ">") con información de los protocolos que componen un mensaje, empezando por nivel físico que no usaremos, ni tampoco ahora Ethernet, sobre IP (Internet Protocol) y por último en el ejemplo ICMP



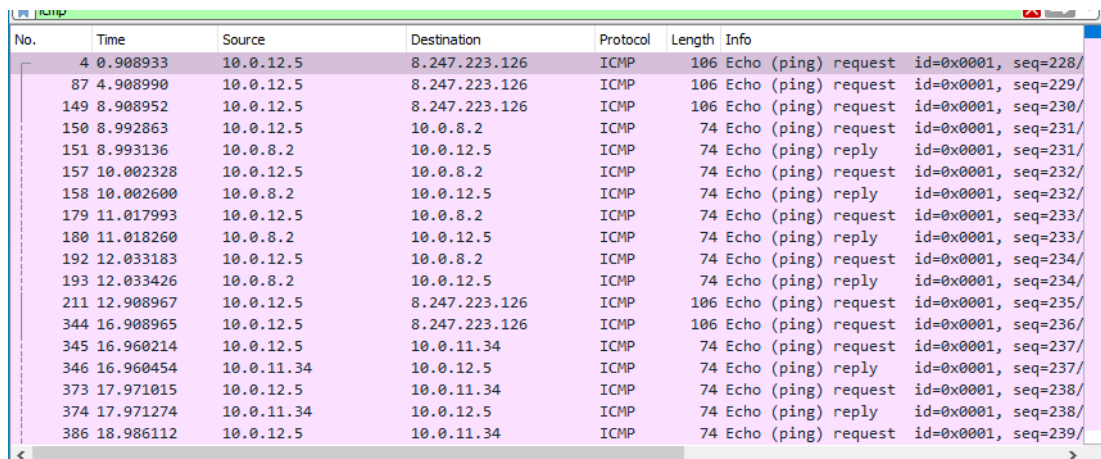
Responda a las siguientes cuestiones:

---

<sup>1</sup> Observe que cada PC tiene una etiqueta con la dirección IP que tiene asignada.

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

<u>Origen</u>	<u>Destino</u>
10.0.12.5	10.0.8.2
10.0.12.5	10.0.11.34
10.0.12.5	10.0.8.46



No.	Time	Source	Destination	Protocol	Length	Info
4	0.908933	10.0.12.5	8.247.223.126	ICMP	106	Echo (ping) request id=0x0001, seq=228/
87	4.908990	10.0.12.5	8.247.223.126	ICMP	106	Echo (ping) request id=0x0001, seq=229/
149	8.908952	10.0.12.5	8.247.223.126	ICMP	106	Echo (ping) request id=0x0001, seq=230/
150	8.992863	10.0.12.5	10.0.8.2	ICMP	74	Echo (ping) request id=0x0001, seq=231/
151	8.993136	10.0.8.2	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=231/
157	10.002328	10.0.12.5	10.0.8.2	ICMP	74	Echo (ping) request id=0x0001, seq=232/
158	10.002600	10.0.8.2	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=232/
179	11.017993	10.0.12.5	10.0.8.2	ICMP	74	Echo (ping) request id=0x0001, seq=233/
180	11.018260	10.0.8.2	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=233/
192	12.033183	10.0.12.5	10.0.8.2	ICMP	74	Echo (ping) request id=0x0001, seq=234/
193	12.033426	10.0.8.2	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=234/
211	12.908967	10.0.12.5	8.247.223.126	ICMP	106	Echo (ping) request id=0x0001, seq=235/
344	16.908965	10.0.12.5	8.247.223.126	ICMP	106	Echo (ping) request id=0x0001, seq=236/
345	16.960214	10.0.12.5	10.0.11.34	ICMP	74	Echo (ping) request id=0x0001, seq=237/
346	16.960454	10.0.11.34	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=237/
373	17.971015	10.0.12.5	10.0.11.34	ICMP	74	Echo (ping) request id=0x0001, seq=238/
374	17.971274	10.0.11.34	10.0.12.5	ICMP	74	Echo (ping) reply id=0x0001, seq=238/
386	18.986112	10.0.12.5	10.0.11.34	ICMP	74	Echo (ping) request id=0x0001, seq=239/

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

10.0.8.2→10.0.12.5	type 0 code 0 reply
10.0.12.5→10.0.8.2	type 8 code 0 request
10.0.11.34→10.0.12.5	type 0 code 0 reply
10.0.12.5→10.0.11.34	type 8 code 0 request
10.0.8.46→10.0.12.5	type 0 code 0 reply
10.0.12.5→10.0.8.46	type 8 code 0 request

Aumente el tamaño del mensaje que emplea el `ping` del apartado anterior hasta 2000 bytes y capture con Wireshark el tráfico que se genera.

```
ping -l 2000 10.0.x.y
```

LINUX

```
ping -s 10.0.x.y
```

Tras 2 o 3 pings parar el comando con Ctrl+C, detenga Wireshark. Antes de contestar analice la MTU del interfaz **Ethernet** de donde ha capturado el tráfico con alguno de estos comandos

```
netsh interface ipv4 show subinterfaces
```

LINUX

```
ifconfig interface-name
```

Para analizar las tramas se recomienda quitar el filtro ICMP

1.3. ¿Cuántos paquetes IP se mandan 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”

Se envían 2 fragmentos.



1.4. ¿Cuál es el tamaño de cada uno?

El primer fragmento 1480 y el segundo 528.

1.5. ¿Puede explicar qué está ocurriendo?

Como el ping que hemos hecho, hemos puesto que transporte 2000 bytes, pero como la MTU es de 1500 entonces habría que fragmentarlo en 2 paquetes ip, uno de 1480 bytes (el máximo de datos ya que 20 son de cabecera) y el resto de datos 528 que serían los restantes para llegar a 2000 con el segundo paquete.

## EJERCICIO 2

Realizamos ahora un ping a una dirección web siguiendo las mismas instrucciones de captura que en el ejercicio anterior:

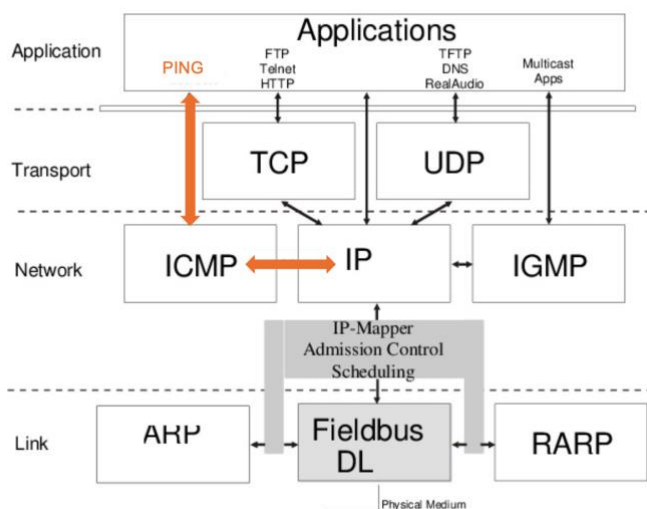
```
$ ping www.rediris.es
```

Responda a las siguientes preguntas:

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

<u>Origen</u>	<u>Destino</u>
10.0.12.5	130.206.13.20
Privada	Publica

Se recuerda la torre de protocolos que usa PING y ICMP



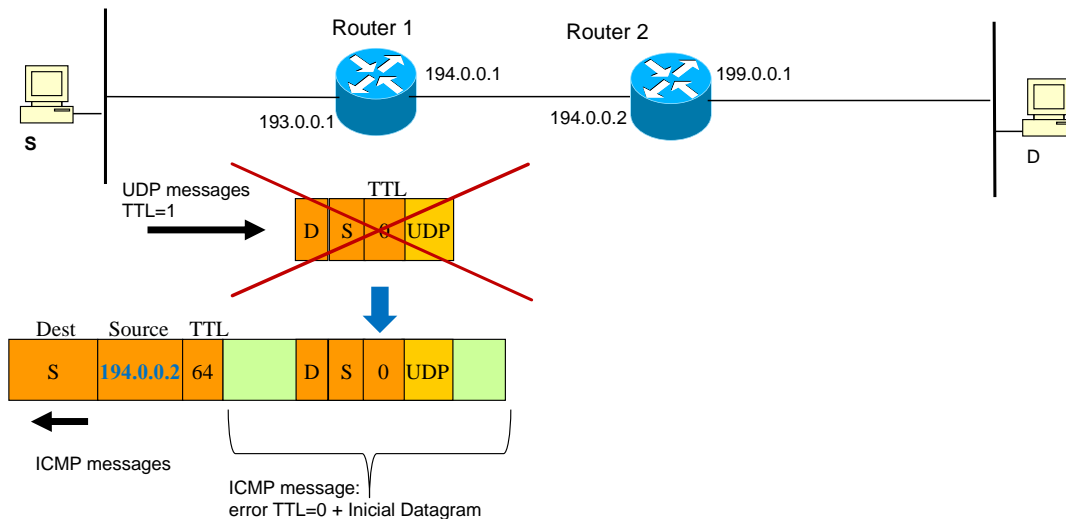
2.2. ¿Llevan estos paquetes ICMP puerto origen/destino? Razone la respuesta.

No llevan puerto porque los mensajes de error y control de red, como ping o traceroute se envían con ICMP

## EJERCICIO 3, TRACEROUTE

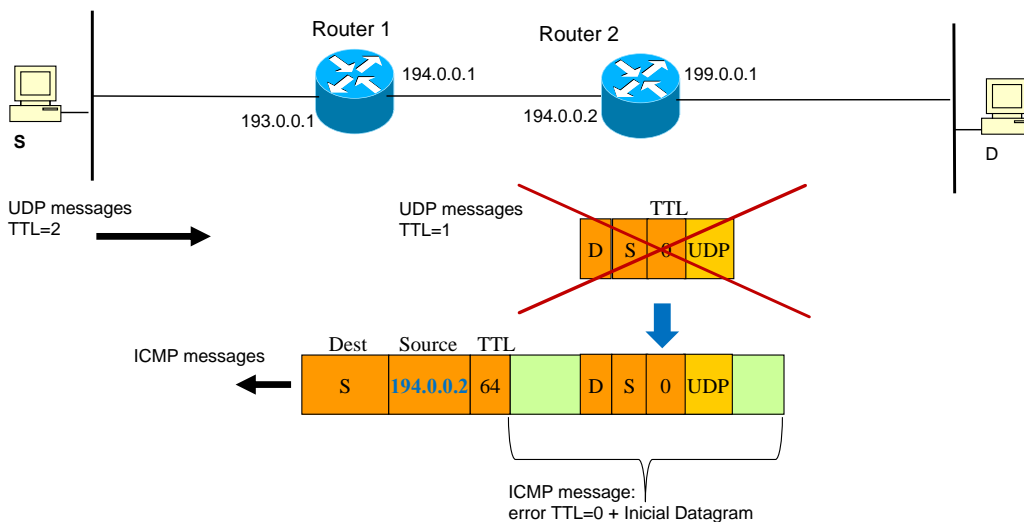
### RECORDATORIO FUNCIONAMIENTO TRACEROUTE

El programa traceroute averigua la secuencia de rutas seguida a un destino. Para ello manda primero mensajes con TTL=1 que al llegar al primer router, decrementa su valor y como es 0 tira el mensaje y genera una notificación ICMP que incluye también dicho mensaje.



De esta manera se averigua el primer router.

Se repite el proceso con TTL=2 y en este caso será el segundo router quien lleve el TTL a 0 y se averigüe su identificación.



El proceso se repite hasta llegar al destino.

Vuelva a arrancar una captura con Wireshark mientras ejecuta:

```
tracert -n www.google.es
```

LINUX

```
tracert -n www.google.es
```

Nota, el “-n” evita traducir IP de los routes a sus nombres simbólicos. Al finalizar detener Wireshark, del resultado del comando copiar la dirección IP de [www.google.es](http://www.google.es) (se ve al ejecutar el comando, supongamos que es la 216.58.209.67). Filtrar los mensajes con ICMP o UDP, si aparecen muchos mensajes se puede añadir la IP anterior de Google,

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

3.1. Identifique los mensajes que genera su PC. ¿Cuál es valor del campo TTL de 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)

El TTL va aumentando según se van enviando los paquetes para mostrar el número de saltos de la ruta.

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

Type 11 code 0 el tipo de error es time to live exceeded in transit.

Es el mismo en los 6 mensajes.

Time	Source	Destination	Protocol	Length	Info
25.1.863757	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=341/21761, ttl=1 (no response found!)
26.1.864063	10.0.12.5	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
27.1.864608	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=342/22017, ttl=1 (no response found!)
28.1.864897	10.0.12.5	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
29.1.865367	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=343/22273, ttl=1 (no response found!)
30.1.865620	10.0.12.5	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
48.2.869707	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=344/22529, ttl=2 (no response found!)
49.2.870340	172.29.20.1	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
50.2.873184	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=345/22785, ttl=2 (no response found!)
51.2.873574	172.29.20.1	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
52.2.875901	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=346/23041, ttl=2 (no response found!)
53.2.876344	172.29.20.1	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
66.3.885451	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=347/23297, ttl=3 (no response found!)
67.3.885902	172.29.0.254	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
68.3.887996	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=348/23553, ttl=3 (no response found!)
69.3.889110	172.29.0.254	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
70.3.891459	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=349/23809, ttl=3 (no response found!)
71.3.891761	172.29.0.254	10.0.12.5	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
81.4.899691	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=350/24065, ttl=4 (no response found!)
82.4.900998	193.145.14.126	10.0.12.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
83.4.903294	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=351/24321, ttl=4 (no response found!)
84.4.904391	193.145.14.126	10.0.12.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85.4.906468	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=352/24577, ttl=4 (no response found!)
86.4.907610	193.145.14.126	10.0.12.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
90.5.914018	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=353/24833, ttl=5 (no response found!)
91.5.915753	130.206.216.1	10.0.12.5	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
92.5.916083	10.0.12.5	142.250.178.163	ICMP	106	Echo (ping) request id=0x0001, seq=354/25089, ttl=5 (no response found!)

Source Address: 10.0.0.1

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

No contienen datos.

No.

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

Type 8 code 0

El error que se produce es: no response found!

## EJERCICIO 4, DHCP

Arranque Wireshark y configúrelo para capturar tráfico en el interfaz de red de área local. Vamos a forzar al PC del laboratorio a que vuelva a adquirir su dirección mediante DHCP. Para ello proceda como se indica a continuación:

```
ipconfig /release
```

LINUX

```
sudo /sbin/dhclient -r
```

Con el comando anterior eliminaremos la configuración de red asignada al interfaz de red. Para obtener una nueva configuración de red del servidor DHCP, ejecute: `ipconfig /renew`

Si tarda mas de 10 segundos en devolver el indicador del sistema operativo, dar un Ctrl-C.

```
LINUX $ sudo /sbin/dhclient
```

Cuando el comando se complete, detenga Wireshark, filtre el tráfico DHCP (filtro **dhcp**) 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?

10.0.8.46

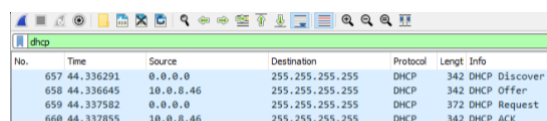
4.2. ¿Cuál es la secuencia de mensajes DHCP que observa desde que se solicita una nueva dirección IP para su equipo hasta que éste la consigue?

1. Enviamos un mensaje a la red de difusión para encontrar al servidor. DHCP Discover

2.El servidor nos envía también a la red de difusión una oferta de dirección IP. DHCP Offer.

3.Nosotros enviamos a la red de difusión una solicitud de dirección IP. DHCP Request.

4. Por último, el servidor envía un mensaje de confirmación (ACK) de que se ha asignado la nueva dirección.



No.	Time	Source	Destination	Protocol	Length	Info
657	44.336291	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover
658	44.336645	10.0.0.46	255.255.255.255	DHCP	342	DHCP Offer
659	44.337582	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request
660	44.337855	10.0.0.46	255.255.255.255	DHCP	342	DHCP ACK

4.3. ¿Cuál es la configuración de red IP completa, en concreto, dirección IP, máscara, router, servidores DNS (varios por fiabilidad) que le asignan a su equipo?

La dirección IP que nos asignan es 10.0.12.1, la máscara es 255.255.248.0, el Router 10.0.8.1 y los servidores DNS 10.0.11.34, 192.168.153.140 y 192.168.153.141.

