Práctica 2

Redes y Sistemas Distribuidos
Grado de Ingeniería del Software (Grupo A)

UNIVERSIDAD DE MÁLAGA

E.T.S. INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE MÁLAGA

Conocimiento: IP


```
Internet Protocol Version 4, Src: 216.58.215.142, Dst: 192.168.1.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x5d73 (23923)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 60
    Protocol: TCP (6)
    Header Checksum: 0xaf36 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 216.58.215.142
    Destination Address: 192.168.1.142
```

Cabecera IP:

- Significado de los campos
- Cómo hace la fragmentación

Versión	HLEN	Servicio	Longitud Total			
Identificador			R	D	M	Desplazamiento
TTL		Protocolo	Checksum			
IP Origen						
IP Destino						
Opciones						
Datos						

Wireshark y los campos calculados:

```
Internet Protocol Version 4, Src: 52.114.74.47, Dst: 192.168.1.138
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000  68 07 15 1f 99 a1 44 f4  36 e0 95 28 08 00 45 00   h·····D· 6··(··E·
0010  00 28 b0 79 40 00 72 06  17 83 34 72 4a 2f c0 a8   ·(·y@·r· ··4rJ/··
```

Dice que tamaño es 20, pero en binario pone 0101 (5) -> Da los campos ya calculados

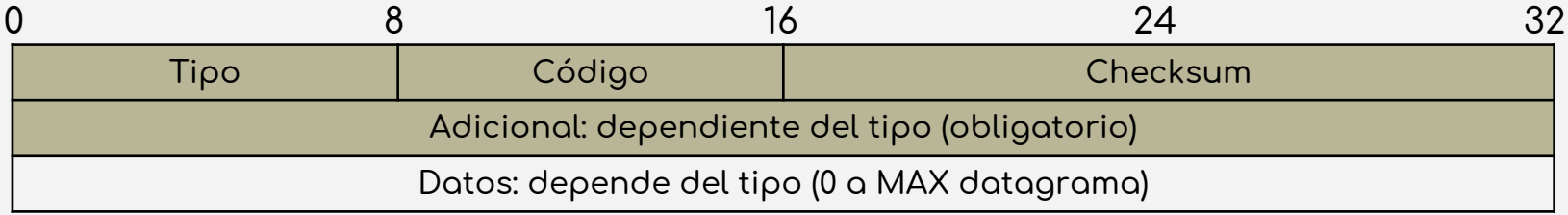
Lo que se envía de verdad (en hexadecimal):

- 4 (versión)
- 5 (HLEN)

Conocimiento: ICMP

ICMP:

- Control y aviso de errores
- Cabecera



Mensajes de interés (T = tipo y C = código):

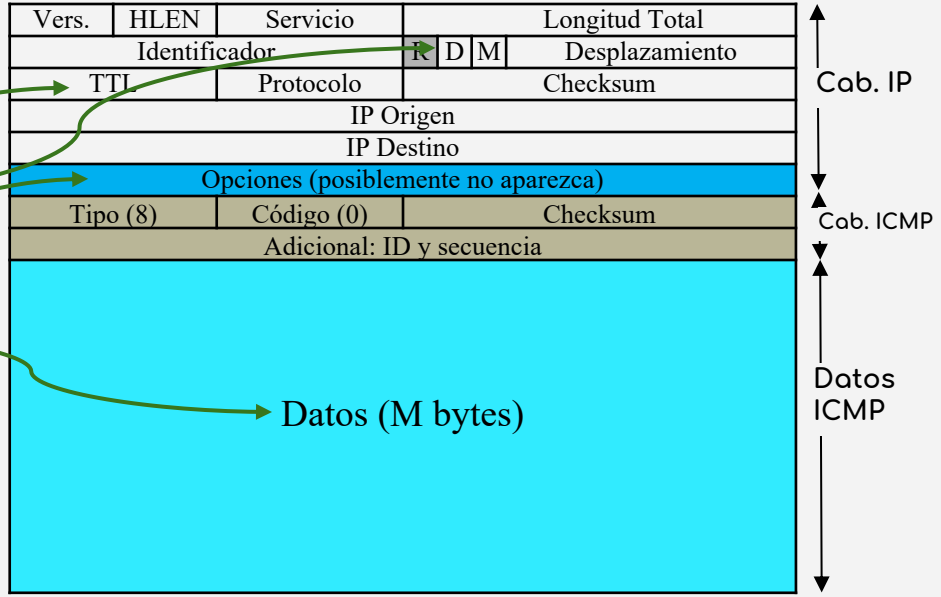
- *Echo Request* (T=8, C=0): ¿está activo el destino?
- *Echo Reply* (T=0, C=0): respuesta al anterior
- *Time Exceeded* (T=11, C=0): se acabó el TTL sin llegar al final
- *Destination Unreachable* (T=3):
  - *Fragmentation Needed* (C=4): No se pudo fragmentar y se debía hacer
  - *Destination Network Unknown* (C=6): No hay entrada en la tabla

Comando ping

`ping`: envía mensaje ICMP Echo Request al destino

Opciones (Windows):

- Obligatorio: destino
- -n N: envía N mensajes (N=1)
- -i T: indica el TTL a usar
- -f: se activa el flag D
- -r X: IPs almacenadas
- -l M: cantidad de datos
- Se pueden poner tantas opciones como queramos y en cualquier orden



Comando tracert y otros

`tracert`: Muestra los nodos por los que va pasando un datagrama hacia su destino

Si no funciona arp:
- `netsh interface ip delete arpcache`

Otros (Windows):

- `arp`: Manejo de la tabla ARP (requiere permisos de administrador)
  - `-a`: muestra la tabla
  - `-d`: borra las entradas dinámicas de la tabla
- `ipconfig`: Interfaces de red y otra información relacionada
  - `/all`: muestra información detallada de los interfaces de red
  - `/flushdns`: borra la tabla de conversión de URL a IPs (DNS)
- `netsh interface ipv4 show subinterfaces`: Muestra otra información sobre los interfaces de red como la MTU

Ejercicio 1

Generación de tramas: `p2e1-2.pcapng`

- En el navegador :
  - Acceda a `http://www.lcc.uma.es`
- En el terminal (modo administrador):
  - `ipconfig /flushdns`
  - `ping –n 1 www.informatica.uma.es`
  - `ipconfig /renew`

Sobre el ejercicio:

- (Para todos) En cada ejercicio se indica qué cabecera (o cabeceras) debe analizar
- En la tabla:
  - Valor Campo protocolo (texto): nombre del protocolo
  - Valor Campo protocolo (HEX): número del protocolo en hexadecimal

Ejercicio 2

Generación de tramas: `p2e1-2.pcapng`

- Se usa la misma que en el ejercicio anterior

Sobre el ejercicio:

- Note que debe siempre se debe elegir mensajes cuyo origen sea su equipo (enviados por tu equipo):
  - ICMP: mensajes Echo Request
  - DNS: en su resumen (Info) pone Standard Query 0x...

- Note que debe consultar diferentes cabeceras (IP y Ethernet)

Ejercicio 3

Generación de tramas: `p2e3.pcapng`

- Generer dos `ping` (use siempre la opción `-n 1`) uno con datos de tamaño 1300 y otro 3400 (el tamaño se especifica con la opción `-l`)

Sobre el ejercicio:

- Note que si filtra por ICMP solo muestra el fragmento final (donde consigue reensamblarlo)
- En cada casilla de la tabla debe poner tantos valores como fragmentos se generen (si genera 10 fragmentos, habrá 10 valores)
- En la tabla
  - **Número de tramas**: números de las tramas consultadas en Wireshark
  - **Flags**: Tres bits (RF, MF y DF) por cada fragmento (ej: 000)
  - **Desplazamientos**: El valor del desplazamiento que se envía de verdad en cada fragmento (NO CALCULADO)

Ejercicio 4

Generación de tramas: `p2e4.pcapng`

- Use las opciones `–n 1` (solo envía 1 mensaje), `-f` (no fragmentar) y `–l M` (tamaño de datos) del `ping`
- Calcule el mayor M que permite hacer el envío. Ese valor se puede calcular mediante la MTU (`netsh interface ipv4 show subinterfaces`) sin necesidad de prueba y error
- Pruebe dos `ping` uno con el valor calculado y otro con el valor calculado más 1

Sobre el ejercicio:

- Tome capturas de pantalla también del terminal donde ejecuta los comandos `ping`
- CASO EXCEPCIONALES: puede que el mensaje se pueda enviar en su red pero luego al pasar por otras redes con MTU menor sea descartado

Ejercicio 5

Generación de tramas: `p2e5-6.pcapng`

- Generer tres `ping` (siempre con la opción `-n 1`): uno con `-r 1`, otro con `-r 3` y el último con `-r 9`

Sobre el ejercicio:

- Observe bien los campos HLEN y de opciones

Ejercicio 6

Generación de tramas: `p2e5-6.pcapng`

- Use la misma del ejercicio previo

Sobre el ejercicio:

- Elija un paquete ICMP de petición cualquiera
- Analice el campo TTL de la petición y su respuesta
- Tenga en cuenta que el que recibe de respuesta habrá sido decrementado por los nodos intermedios por lo que pasa

Ejercicio 7

Generación de tramas: `p2e7.pcapng`

- Pruebe `ping` con TTL variable `-i TTL` hasta que conteste bien
- Pruebe los valores: 1, 2, 3…
- Respuestas incorrectas:

```
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
```

```
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 37.134.240.1: TTL expirado en tránsito.
```

- Respuesta correcta:

```
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 150.214.54.249: bytes=32 tiempo=35ms TTL=53
```

Sobre el ejercicio:

- Puede que algunos nodos intermedios estén configurados para no enviar mensajes ICMP y que a veces no reciba respuesta

Ejercicio 8

Generación de tramas: `p2e8.pcapng`

- Ejecute el comando `tracert` con destino a `www.informatica.uma.es`

Sobre el ejercicio:

- Cuando muestra `*` es que no consiguió determinar información de ese nodo intermedio
- Lo que se hizo en el ejercicio anterior le puede ayudar a entender como funciona internamente este comando
- Además de los mensajes que usa para obtener la ruta observe los mensajes enviados cercanos a ellos porque lo mismo son utilizados también por el comando para obtener información adicional