Práctica 2

Objetivos de la práctica

Análisis con Wireshark de los protocolos IP e ICMP.

Conocimientos previos:

- Cabecera IP y el significado de sus campos
- Fragmentación en IP
- Protocolo ICMP

Información básica

El principal objetivo del protocolo IP en las redes que usan la arquitectura de protocolos TCP/IP es enviar información desde una máquina origen a otro destino que posiblemente no tengan conexión directa entre ellos. Para ello añade a la carga útil una cabecera con una serie de campos con información adicional que permiten que los datos lleguen al destino. Para conseguir cumplir con su objetivo, IP hace uso de otros protocolos como ARP, ICMP o IGMP. En particular ICMP se utiliza para enviar mensajes de error o de consulta relacionados con IP entre distintas máquinas.

Fundamentos: Cabecera de IP e ICMP. Comandos ping y tracert.

El formato de la cabecera de IP se muestra en la Figura 1.

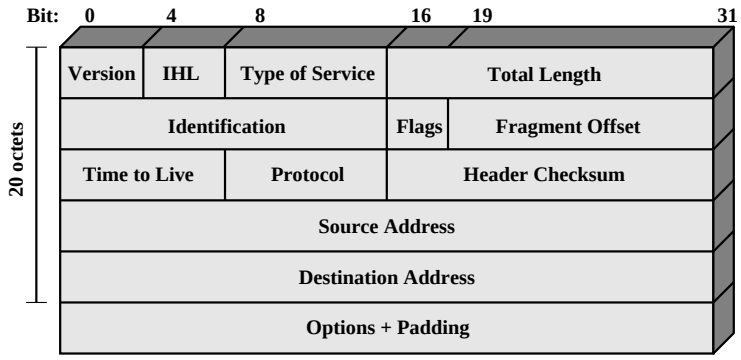

Figura 1. Formato de la cabecera de IP

Los detalles de los campos son:

Campo	Valor (ejemplo)	Descripción
Versión	4	Versión del protocolo (será 4 en nuestro caso).
IHL	5	Longitud de la cabecera en palabras de 4 bytes. Su valor es 5 (20/4) cuando no hay opciones.
Tipo de servicio	0000	Parámetros de velocidad, prioridad, retardo, rendimiento. Normalmente no se usa y está a 0.
Longitud del paquete	1500	Longitud del paquete. El máximo valor es 65535 bytes, pero en las redes Ethernet será de 1500, ya que la MTU tiene ese valor.
Identificación	0x8302	Identifica de forma única al paquete. Se usa en la fragmentación.
Flags	000	Son tres bits, de los cuales los dos últimos, DF y MF, se usan para indicar que el paquete no se puede fragmentar o que hay más fragmentos siguientes a este, respectivamente.
Desplazamiento	185	Indica la posición donde hay que colocar los datos de este fragmento cuando se reensamble el datagrama (en palabras de 8 bytes).
Tiempo de vida	64	Indica el número máximo de saltos que puede realizar el paquete.
Protocolo	6	Indica a qué protocolo hay que entregar el datagrama. Cada protocolo tiene un número asociado. Algunos valores son TCP=6, UDP=17, ICMP=1, IGMP=2, IPv4=4. Puede consultarlos todos en https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
Checksum	0xd206	Suma de comprobación de la cabecera. Wireshark lo comprueba e indica si es correcto o no.

Campo	Valor (ejemplo)	Descripción
Dirección origen	`192.168.1.1`	Dirección IP de la máquina origen de los datos.
Dirección destino	`150.214.18.1`	Dirección IP de la máquina destino de los datos.
Opciones		Campo opcional de tamaño variable (0-40 B). Típicamente vacío.

Nota sobre Wireshark: Fíjese que en muchos casos lo que nos muestra Wireshark en los detalles de la cabecera, no es exactamente lo mismo que se transmite. Eso es debido a que Wireshark pre-procesa los datos. Por ejemplo, observe los campos de tamaño de la cabecera o el campo de desplazamiento.

Algunos posibles formatos de la cabecera ICMP se muestran en la Figura 2.

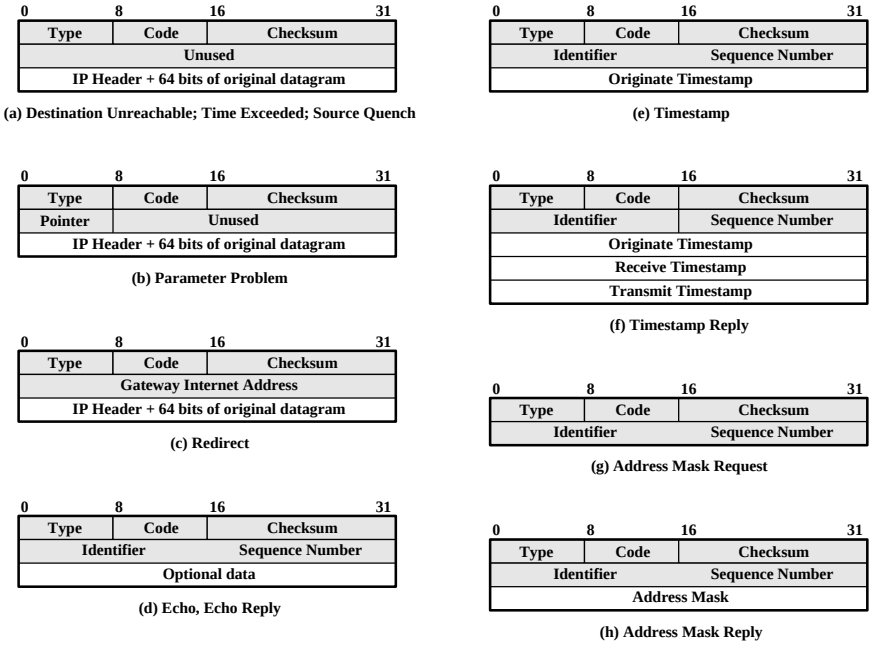

Figura 2. Posibles formatos de la cabecera de ICMP (lista no exhaustiva)

Los campos comunes a todos los mensajes son:

Campo	Valor (ejemplo)	Descripción
Tipo[1]	`11`	Tipo de mensaje (*Echo Reply*, *Echo Request*, *Time Exceeded*, etc.).
Código[1]	`0`	Detalla la razón del mensaje.
Checksum	`0xfb74`	Suma de comprobación.

La información adicional que aparece en el mensaje ICMP depende del tipo de mensaje. Por ejemplo, cuando el mensaje es de tiempo excedido se incluye la cabecera IP del paquete que provocó el mensaje y los primeros 8 bytes de la carga útil del paquete.

El comando **ping** se utiliza para comprobar si una máquina está activa o no. Este comando usa el protocolo ICMP y permite modificar algunos campos de la cabecera de IP, así como establecer el tamaño del mismo. El primer argumento del comando es el nombre (o IP) de la máquina destino. Algunas de las opciones de este comando son:

Win	Linux	Mac	Descripción
`-l` `tam`	**`-s`** `tam`	**`-s`** `tam`	Indica el tamaño del campo de datos del mensaje ICMP.
`-i` `ttl`	**`-t`** `ttl`	**`-m`** `ttl`	Indica el valor para el campo TTL (*time to live*) de IP.
`-f`	**`-M do`**	**`-D`**	Indica que se debe activar el bit DF (*don't fragment*).
`-n` `num`	**`-c`** `num`	**`-c`** `num`	Indica cuántas peticiones ICMP se envían. En los ejercicios use **–n 1** o **–c 1**.
`-r` `num`	**`-R`**	`-`	Almacena en las opciones de la cabecera las IPs de los equipos por los que pasa el mensaje ICMP (tanto de ida como de vuelta)

[1] La lista de tipos/códigos se puede consultar en https://www.rfc-es.org/rfc/rfc0792-es.txt

Otro comando que resultará de utilidad es **tracert** (**traceroute** en Linux/Mac). Este comando obtiene la lista de nodos intermedios entre la máquina desde la que se ejecuta y otra máquina en la red. La información sobre estos nodos intermedios no siempre es completa ya que hay algunos de ellos que descartan los paquetes que son enviados por **tracert**. Al comando se le pasa como argumento la máquina destino. En Mac use **traceroute** siempre con la opción `-I`.

Tarea 1: Encapsulamiento en IP

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Seleccione el interfaz del que desea capturar en el listado ofrecido y luego haga clic en el botón de inicio.

Paso 2: Generación de tráfico.

Abra una ventana terminal de Windows (clic en **Inicio > Ejecutar**, escriba **cmd**). Para preparar el sistema y obtener el comportamiento esperado escriba el siguiente comando:

```
ipconfig /flushdns
```

Si tenéis acceso como administrador, también es conveniente:

```
arp -d
netsh interface ip delete arpcache
```

En la ventana de comandos ejecute un **ping** entre su ordenador y **www.informatica.uma.es**.

`ping -n 1 www.informatica.uma.es`Abra una ventana privada o de incógnito del navegador y conéctese a la página web de **http://www.lcc.uma.es**. A partir de una ventana de comandos haga **ping** a **www.informatica.uma.es**. En la misma línea de comandos haga **ipconfig /renew**. Cuando el comando haya finalizado la carga, detenga la captura. Guarde la traza como **p2e1-2.pcapng**.

Paso 3: Analizar la captura de Wireshark.

Filtre la captura para que sólo parezcan las tramas pertenecientes a los protocolos icmp, dns, dhcp y http. Observe una trama cualquiera de las filtradas e identifique los campos de la cabecera IP con ayuda de la Figura 1. Analizando la traza capturada de Wireshark, conteste a las siguientes cuestiones:

Ejercicio 1. Observe la cabecera IP de los diferentes datagramas, ¿qué protocolo se indica en el campo "protocolo" en la cabecera de los datagramas que transportan mensajes DNS, ICMP, DHCP y HTTP? Rellene la tabla con dicha información. ¿Qué indica este campo? ¿Por qué este campo tiene el mismo valor si el protocolo de aplicación es diferente?

Protocolo	Valor Campo protocolo (texto)	Valor Campo protocolo (HEX)	Número de trama
ICMP			
HTTP			
DNS			
DHCP			

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *Echo Request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición DNS (en la Info pone *Standard query 0x…*). ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

	ICMP	DNS
Dirección IP destino (cabecera IP)		
Dirección MAC destino (cabecera Ethernet)		
Número de trama		

Tarea 2: Fragmentación en IP

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Haga clic en **Captura > Interfaz**, y luego haga clic en el botón de inicio que corresponde a la tarjeta de red.

Paso 2: Hacer ping a la dirección www.informatica.uma.es con distintas opciones.

El comando ping permite modificar ciertos campos del paquete IP. En particular, podemos cambiar el tamaño del mensaje ICMP que se envía. Esto nos resultará especialmente útil para poder comprobar cómo funciona la fragmentación en IP. Vamos a hacer ping a la máquina **www.informatica.uma.es** con 2 valores para el tamaño del mensaje: primero haga un ping con tamaño 1300 y luego otro con tamaño 3400 bytes. Recuerde en usar la opción **–n 1** (**–c 1** en Linux/Mac)**.** Guarde la traza como **p2e3.pcapng**.

Ejercicio 3. ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)? Para el resto de preguntas y rellena la tabla considere solo las peticiones. ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto? Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos).

Tamaño	Número de tramas	Identificadores	Flags	Desplazamientos
1300				
3400				

Los datagramas IP tienen un tamaño máximo dependiente de la red (*MTU*). Por ejemplo, en redes Ethernet el MTU es 1500 pero llevará menos datos de usuario ya que ese valor considera las cabeceras. Para validar el tamaño máximo de datos que podemos enviar, vamos a usar el bit DF (*don't* fragment). Note que si indica este bit y se pone un tamaño mayor al máximo debería fallar. La opción **–f** (opción –**D** en mac y **–M** en linux) permite activar dicho flag en el comando ping. Puede consultar el MTU usadas en sus redes en Windows con **netsh interface ipv4 show subinterfaces** (**ifconfig** en Mac y **ifconfig** o **ip –c address** en Linux).

Ejercicio 4. Calcule el tamaño máximo de datos (MAX) que puede llevar un ping en la red del laboratorio. Realice dos pings a **www.informatica.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). ¿Cuál es el valor máximo? ¿Por qué es ese tamaño? ¿En la traza de Wireshark aparece el primer ping? ¿Y el segundo? ¿Por qué? Guarde la traza como **p2e4.pcapng**.

Tarea 3: Cabecera en IP

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Haga clic en **Captura > Interfaz**, y luego haga clic en el botón de inicio que corresponde a la tarjeta de red.

Paso 2: Hacer ping a la dirección www.informatica.uma.es con distintas opciones.

Como hemos anteriormente el comando ping permite modificar ciertos campos del paquete IP. Pruebe ahora a hacer un ping a **www.informatica.uma.es** usando la opción -r 1, -r 3, y -r 9. Esta opción del ping -r X, hace uso del servicio "Record Route"[2] de IPv4 que almacena las IPs por las que pasa, donde X es la cantidad de direcciones IP se pueden almacenar. Esta tarea no puede realizarse en Mac y en Linux también es ligeramente diferente (usa la opción -R sin parámetros). Guarde la traza como **p2e5-6.pcapng**.

Ejercicio 5. El uso de -r X cambia la cabecera en dos aspectos: añade el campo opciones de tamaño apropiado dependiente de X y por lo tanto cambia el campo HLEN. ¿Cómo aumenta el tamaño de HLEN según X? Si prueba otros valores X, verá que solo permite valores entre 1 y 9, ¿Por qué cree que solo permite esos valores y no mayores? Finalmente observe que además de la opción IP "Record Route" se incorpora la opción "End of Options List" para indicar que ya no hay más opciones, ¿por qué es necesaria añadir esta opción y no nos vale solo con el HLEN?

[2] https://www.geeksforgeeks.org/options-field-in-ipv4-header/

Ejercicio 6. Localiza y observa un paquete de respuesta y presta atención al campo TTL. ¿Cuánto vale? Compárelo con el TTL del mensaje de petición. ¿Quién establece cada valor?

Tarea 4: Mensajes de error ICMP

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Seleccione el interfaz del que desea capturar en el listado ofrecido y luego haga clic en el botón de inicio.

Paso 2: Hacer ping a la dirección www.informatica.uma.es con distinto TTL.

El error más fácil de inducir usando ICMP es el de tiempo excedido. Esto se consigue asignando un valor suficientemente bajo al campo TTL en la cabecera de IP. El comando ping permite hacer esto. Guarde la traza como **p2e7.pcapng**.

Ejercicio 7. Haga varios pings a **www.informatica.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta correcta del servidor. Pruebe con los siguientes valores (pare cuando responda de forma adecuada): 1, 2, 3,… Observe en Wireshark el intercambio de paquetes que se produce. ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)? ¿Qué incluye dicho mensaje ICMP como información adicional (dentro del campo de datos)?

Tarea 5: Comando tracert

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Seleccione el interfaz del que desea capturar en el listado ofrecido y luego haga clic en el botón de inicio.

Paso 2: Usar tracert para obtener información de los routers intermedios.

El comando **tracert** (o **traceroute** en Linux/Mac) permite descubrir cuántos saltos son necesarios para llegar a una máquina y da información acerca de las máquinas intermedias. Tras limpiar todas las caches, use **tracert** para descubrir cuántos saltos hay de su máquina a **www.informatica.uma.es** y capture las tramas involucradas. Guarde la traza como **p2e8.pcapng**. Si usa un Mac, emplee la opción `-I` para usar mensajes con ICMP.

Ejercicio 8. ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función? Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios? ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete?