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. Para ello añade a la información 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.

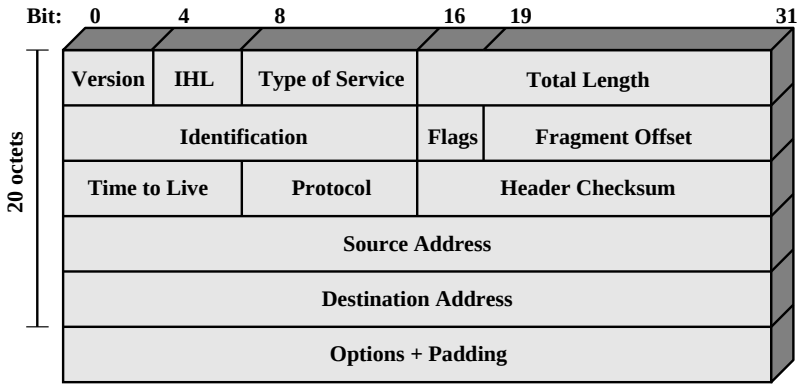

Figura 1. Formato de la cabecera de IP

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 típico es 20 (5x4) 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 a qué parte del paquete original pertenece el fragmento 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 http://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 (parte central de la pantalla), no es exactamente lo mismo que se transmite (parte inferior). 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.

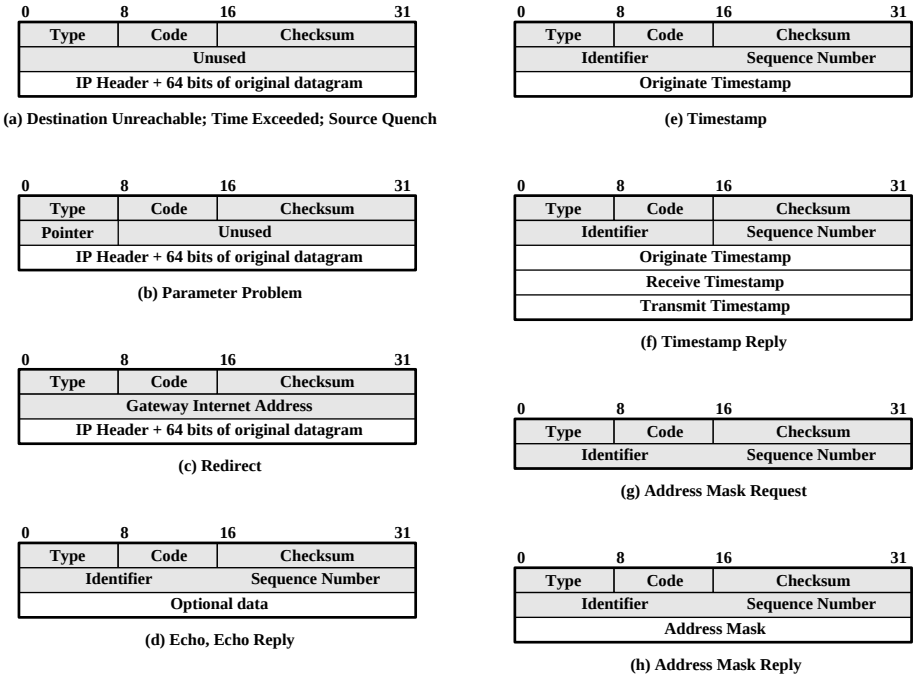

Figura 2. Posibles formatos de la cabecera de ICMP (lista no exhaustiva)

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. En Mac el **ping** siempre se ejecutará con la opción `-I`. 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**.

[1] La lista de tipos/códigos se puede consultar en http://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. Haga clic en **Captura > Interfaz**, y luego haga clic en el botón de inicio que corresponde a la tarjeta de red.

Paso 2: Generar tráfico a informatica.cv.uma.es.

Abra una ventana de navegador (por ejemplo, Firefox) y conéctese a la página web de **informatica.cv.uma.es**. En el mismo navegador indique también la dirección **ftp://ftp.uma.es** (asegúrese de copiar el ftp:// inicial). A partir de una ventana de comandos haga **ping** a **informatica.cv.uma.es**. 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, ftp 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 (haga capturas de pantalla donde aparezcan estos datos), 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 ICMP, FTP y HTTP? Rellene la tabla con dicha información. ¿Qué indica este campo?

Protocolo	Valor Campo protocolo	Valor (HEX)	Número de trama
ICMP			
HTTP			
FTP			

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 FTP (en la Info pone request). ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

	ICMP	FTP
Dirección IP destino (cab IP)		
Dirección MAC destino (cab 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 informatica.cv.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 **informatica.cv.uma.es** con 2 valores para el

tamaño del mensaje: 1200 y 3100 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
1200				
3100				

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 que puede llevar un ping en la red del laboratorio. Realice dos pings a **informatica.cv.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 segundo ping? ¿Por qué? Guarde la traza como **p2e4.pcapng** y una captura de pantalla del terminal mostrando como el primer funciona y el segundo falla.

Tarea 3: Mensajes de error ICMP

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 informatica.cv.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 **p2e5.pcapng**.

Ejercicio 5. Haga varios ping a **informatica.cv.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Pruebe con los siguientes valores (pare cuando responda de forma adecuada): 1, 2, 3, 4, 5, 10, 15, 20, 25 y 30. 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 (campos datos)?

Tarea 4: Comando tracert

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: 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 **informatica.cv.uma.es** y capture las tramas involucradas. Guarde la traza como **p2e6.pcapng**. Si usa un Mac, emplee la opción `-I` para usar mensajes con ICMP.

Ejercicio 6. ¿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?

Nota sobre la memoria

- Si elabora la memoria en Word, se aconseja utilizar la plantilla proporcionada para la práctica. En cualquier caso, la memoria debe contener toda la información que se pide en la plantilla y seguir su estructura.
- La memoria de esta práctica se entregará en conjunto a la memoria de la 1 y la 3.
- Dicha memoria debe constar de una portada donde se indique el conjunto de prácticas que incluye la memoria, así como todos los datos del alumno.
- La memoria de cada práctica debe empezar en una nueva página.
- No es necesario copiar el enunciado completo de la práctica pero sí debe copiarse el enunciado de cada ejercicio antes de indicar su respuesta. Debe utilizarse algún sistema de estilos que permita distinguir lo que es el enunciado de lo que es la respuesta al ejercicio.
- Para **cada ejercicio** que obtenga la información de algún proceso realizado en el ordenador (traza de Wireshark, comando,...) **realice una captura** (con <alt>+<impr pant> sólo capturaremos la ventana activa actual). Además de incluir la captura se deben utilizar las herramientas de dibujo del procesador de texto usado para marcar la parte donde se observa lo que pide el ejercicio. Finalmente en el texto añada una pequeña descripción de la captura.
- El formato de entrega de las prácticas será **PDF**.
- Cuando se entregue la memoria **se adjuntarán las trazas** utilizadas en la práctica (**p2e1-2.pcapng – p2e3.pcapng – p2e4.pcapng – p2e5.pcapng – p2e6.pcapng).**