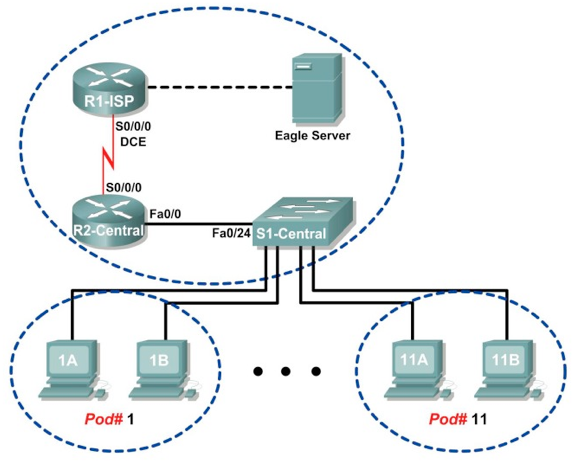
**Práctica de laboratorio: Observar el funcionamiento de la capa de red (IP)**

**Diagrama de topología (Tarea 1)**

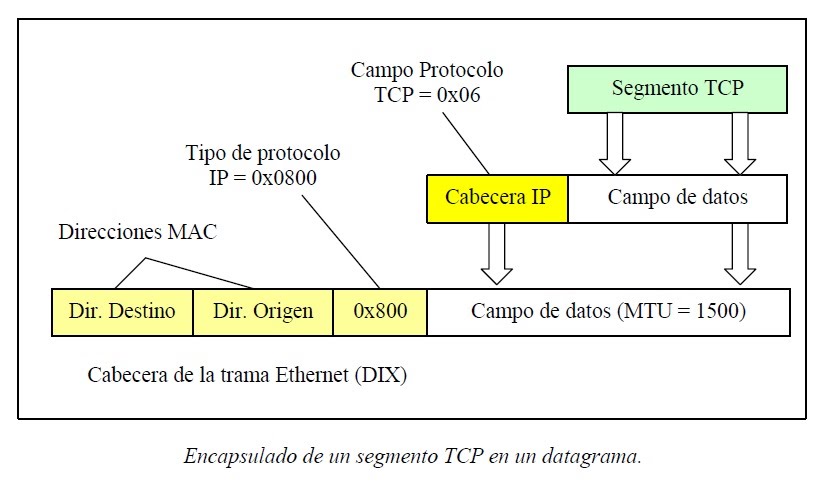
****

**Objetivos**

* **Tarea 1: Examinar los encabezados de los datagramas IP.**
* **Tarea 2: Capturar y examinar la fragmentación IPv4.**

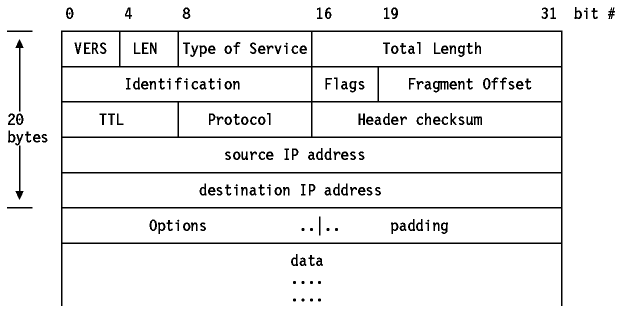
**Información básica**

Los datagramas IP se encapsulan dentro de una trama, ocupando el espacio dedicado al campo de datos de la misma (figura 1).



**Figura 1.** Encapsulado de un segmento TCP en un datagrama IP y en una trama Ethernet.

El tamaño máximo de un datagrama son 64 KB según el estándar del protocolo IP. Sin embargo, el tamaño del datagrama está limitado por el tamaño máximo del campo de datos de la trama que lo va a llevar. Esta es una limitación que depende de la tecnología de red que tengamos. Cada tecnología de red define el tamaño máximo del campo de datos de la trama, también conocido como MTU (Maximun Transfer Unit), que maneja. Así, por ejemplo, Ethernet define un MTU de 1500 bytes u octetos.



**Figura 2.** Formato del datagrama IPv4.

El datagrama IP se divide en dos campos: Cabecera y datos. La cabecera contiene información que el protocolo necesita para ofrecer su servicio, y el campo de datos contiene el mensaje en si que tiene que ser entregado en el host destino. En la figura 2 se muestra el formato de un datagrama IPv4:

* **VERS (Versión):** Especifica la versión del protocolo IP a la que pertenece el datagrama (0100/v4, 0110/v6).
* **LEN (Longitud cabecera):** Define el tamaño de la cabecera IP en palabras de 32 bits, ya que esta puede ser de tamaño variable. El valor mínimo para este campo es 5 (es decir, 5×32=160 bits = 20 bytes), y el valor máximo es 15 (es decir, 15×32 = 480 bits = 60 bytes). A efectos prácticos consideraremos la cabecera IP de tamaño fijo (sin campo de opciones) con un valor 5.
* **TOS/Type of Service (Tipo de servicio):** Contiene información acerca de cómo debe ser tratado el datagrama en su viaje al destino. Incluye algunos ítems acerca de la calidad de servicio que va a recibir este datagrama. Sin no se aplican políticas de QoS, este campo no es utilizado y su valor suele ser 0.
* **Total Length (Longitud total):** Como su nombre indica, define el tamaño total del datagrama (cabecera + datos) en bytes. La longitud máxima son 64 KB.
* **Identification (Identificación):** Es un entero de 16 bits que identifica a este datagrama y lo distingue de otros datagramas enviados. Es una especie de número de secuencia que se incrementa cada vez que IP envía un datagrama.
* **Flags (Indicadores):** Son 3 bits que informan sobre el estado del fragmento. El bit 1 (R) está reservado y su valor por defecto es 0. El bit 2 (DF) indica si el paquete puedo o no fragmentarse; y si su valor es 1 es que no está permitida la fragmentación. El bit 3 (MF) cuando el valor es 0 indica que es el último fragmento.
* **Fragment Offset (Desplazamiento de fragmento):** Estos 13 bits permiten al destino recomponer los fragmentos del datagrama original. A su vez, los fragmentos son datagramas (partes del campo datos del datagrama original con nuevas cabeceras) que viajan hacia el destino de forma independiente, donde son recogidos por el protocolo IP para reconstruir el datagrama original. Se calcula como múltiplo de 8 (bits).
* **TTL/Time To Live (Tiempo de vida):** Define el tiempo de que dispone el datagrama para llegar a su destino, con el fin de evitar la existencia de datagramas que, por errores en el encaminamiento, estén dando vueltas indefinidamente en la red. Cada vez que el datagrama cruza un router, este campo es decrementado en una unidad, de forma que cuando alcanza el valor nulo, es eliminado de la red.
* **Protocol (Protocolo):** Identifica el protocolo de capa superior al que pertenecen la información almacenada en el campo de datos del datagrama. Así́, para los protocolos ICMP, UDP y TCP los valores de este campo serán 1, 17 y 6 respectivamente.
* **Header Checksum (Suma de comprobación de cabecera):** En este campo se almacena un checksum de los campos de la cabecera. Es un mecanismo simple para detectar posibles errores en los campos de la cabecera del datagrama, los cuales podrían provocar situaciones erróneas en la red.
* **Source/Destination IP address (Direcciones IP origen/destino):** Direcciones origen y destino del datagrama. Aunque el datagrama viaje a través de varios routers, estos campos nunca cambian.
* **Options (Opciones) y Padding (Relleno):** Este campo es de longitud variable y complementario al encabezado para acciones opcionales. Por último, existe un campo de relleno con el fin de ajustar el tamaño del paquete a múltiplos de 32 bits.

En esta práctica de laboratorio, utilizarás Wireshark para examinar los encabezados de los datagramas IP que se generan entre un navegador Web del PC mediante el protocolo de transferencia de hipertexto (HTTP) y un servidor Web, como http://eagle-server.example.com. También, forzaremos la capa de red del PC para generar paquetes con un tamaño mayor a 1500 bytes que es la MTU de la red Ethernet a la que te conectas, para observar y analizar el proceso de fragmentación IP.

**Recursos necesarios**

* 1 PC con acceso a la red y Wireshark instalado

**Tarea 1: Examinar los encabezados de los datagramas IP.**

**Paso 1. Identificar información de encapsulamiento del paquete IP.**

A partir de la captura de Wireshark (**AL06-1\_T1.pcapng**) que encontrarás en la carpeta adjunta a esta actividad, examina el encapsulamiento del paquete correspondiente a la **consulta DNS** para el nombre de dominio **eagle-server.example.com**. Fíjate en los campos de cabecera del paquete IP y la trama Ethernet. Completa la Tabla 1 (si es posible) **SÓLO** con la información contenida en esa captura. En caso de no localizar la información, escribe el motivo en el espacio correspondiente:

|  |  |
| --- | --- |
| **Dirección física (MAC address) del cliente** |  |
| **Dirección IP del cliente** |  |
| **Dirección máscara de subred del cliente** |  |
| **Dirección IP puerta de enlace predeterminada del cliente** |  |
| **Direcciones IP servidores DNS locales del cliente** |  |
| **Dirección física (MAC address) del servidor** |  |
| **Dirección IP del servidor** |  |
| **Dirección máscara de subred del servidor** |  |
| **Dirección IP puerta de enlace predeterminada del servidor** |  |
| **¿A quién corresponde la dirección MAC destino del paquete examinado?** |  |

**Tabla 1.** Información sobre el direccionamiento de la red.

**Paso 2: Identificar cabeceras de un datagrama IP.**

Filtra el resto de tráfico y quédate únicamente con los paquetes intercambiados por la **capa de aplicación** en la acción anterior. Analiza la información de los encabezados de los paquetes IP correspondientes a: **consulta DNS, respuesta DNS**, **petición Web y respuesta Web**. Responde las siguientes cuestiones:

1. ¿Cuál son los protocolos de la capa de aplicación utilizados? \_\_\_\_\_\_\_\_\_\_

Indica el nº de paquete en tu captura correspondiente a cada uno de los mensajes anteriores: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Indica el filtro de visualización utilizado (si es posible intenta usar un único filtro):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Con respecto al campo **Tiempo de vida (TTL)** de la cabecera IP de los paquetes capturados, ¿son siempre iguales? \_\_\_\_\_\_. Todos los paquetes IP que envía un mismo PC ¿tienen el mismo TTL? \_\_\_\_\_\_

Indica el nº de paquetes en tu captura que justifican tu respuesta: \_\_\_\_\_\_

1. Consulta el campo de la cabecera **Tipo de servicio** de los paquetes IP que contienen la **consulta DNS** y la **petición Web** respectivamente ¿a que conclusión llegas? **Nota:** Wireshark mostrará este campo como **Differentiated Services Field**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Consulta el campo de la cabecera **Longitud cabecera** de los paquetes IP que contiene la **consulta DNS** y la **petición Web** respectivamente ¿coincide este valor en ambos paquetes? \_\_\_\_\_\_ ¿cuál el valor para este campo en bytes? \_\_\_\_\_\_\_
2. Consulta el campo de la cabecera **Protocolo** de la **consulta DNS** ¿cuál es el valor que contiene? \_\_\_\_\_ ¿A cuál protocolo de capa de transporte se corresponde? \_\_\_\_\_
3. Consulta el campo de la cabecera **Protocolo** de la **petición Web** ¿cuál es el valor que contiene? \_\_\_\_\_ ¿A cuál protocolo de capa de transporte se corresponde? \_\_\_\_\_ ¿Coincide con el resultado el de la pregunta anterior? \_\_\_\_\_\_\_

**Tarea 2: Capturar y examinar la fragmentación IPv4.**

**Paso 1: Configuración IP**

Recopila la información de la configuración IP de tu PC en la Tabla 2, ¿qué comandos en Windows debes usar para ello? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Dirección física (MAC address)** |  |
| **Dirección IP** |  |
| **Dirección Máscara de subred** |  |
| **Dirección IP puerta de enlace predeterminada** |  |
| **Direcciones IP servidores DNS locales** |  |

**Tabla 2.** Información de la configuración IP del PC.

**Paso 2: Capturar paquetes**

No podemos observar la fragmentación que se produce en los routers pero puedes generar fragmentación en la propia interfaz del PC:

1. Inicia la captura de paquetes con Wireshark en la interfaz Laboratorio desde la lista de interfaces con el filtro “**ip.proto==1**”.
2. Abre una ventana de interfaz de comandos en Windows con el comando **cmd**, y ejecuta el siguiente comando:

**C:\> ping –n 1 –l 4000 dir\_ip\_puerta\_de\_enlace**

**Nota:** Con ello estamos forzando al envió de un mensaje con 4000 bytes de datos (sin bytes de cabecera) mediante el parámetro “-l” al destino especificado. Como estás conectado a una red Ethernet cuya MTU son 1500 bytes, el envió solicitado exigirá́ la fragmentación del mensaje en tres paquetes IP. El protocolo ICMP añadirá 8 bytes más de sus cabeceras al último fragmento.

1. Para la captura de datos.
2. Guarda la captura realizada en un archivo con nombre **AL06-1\_T2.pcap.**

**Paso 3: Localizar e identificar datagramas IP en la captura**

Compara las cabeceras de los fragmentos y completa la Tabla 3.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Longitud total** | **Indicadores** | | | **Desplazamiento del fragmento** |
| **R** | **DF** | **MF** |
| **1er fragmento** |  |  |  |  |  |
| **2do fragmento** |  |  |  |  |  |
| **3er fragmento** |  |  |  |  |  |

**Tabla 3.** Información de los fragmentos IP resultantes.

1. ¿Cuál es el valor del campo **Protocolo**de la cabecera de los tres fragmentos? \_\_\_\_\_ ¿Debería ser el mismo para todos los fragmentos con un mismo identificador de paquete? \_\_\_\_\_\_ ¿Por qué?
2. ¿Cuántos bytes de datos viajan en cada paquete?
3. Calcula la longitud total del paquete IP (no de tipo ICMP) que deberíamos enviar para que se generaran 4 fragmentos de tamaño máximo de carga útil (1480 bytes):