PRACTICA 4

EL PROTOCOLO IP

Hasta ahora hemos visto aspectos relacionados con el hardware de red de nuestras máquinas: Acceso al adaptador de red y un mecanismo para la resolución de direcciones hardware. Esto nos suministra una acceso a nuestra red local que permite la comunicación a nivel de trama con todas las máquinas de la misma. Sin embargo, la interconexión de distintas redes, tanto locales como de área extensa o metropolitana, introduce un problema de comunicación al involucrarse distintos sistemas de direccionamiento a veces incompatibles entre sí (tal y como decíamos al hablar del protocolo ARP). El protocolo IP (*Internet Protocol*) es el que se encarga de resolver estas diferencias definiendo un espacio de direcciones universal por encima de las direcciones hardware que cada red define. Esto permite que máquinas conectadas a redes remotas, y probablemente con direccionamiento hardware incompatible, puedan comunicarse a través de este protocolo.

El protocolo IP es el pilar básico de Internet (red de redes, interconectadas a nivel mundial) que permite la interconexión de redes abstrayéndose de las diferentes tecnologías de red existentes. Es, en su totalidad, un protocolo software que está desligado de los detalles del hardware de red, característica fundamental para la interconexión redes.

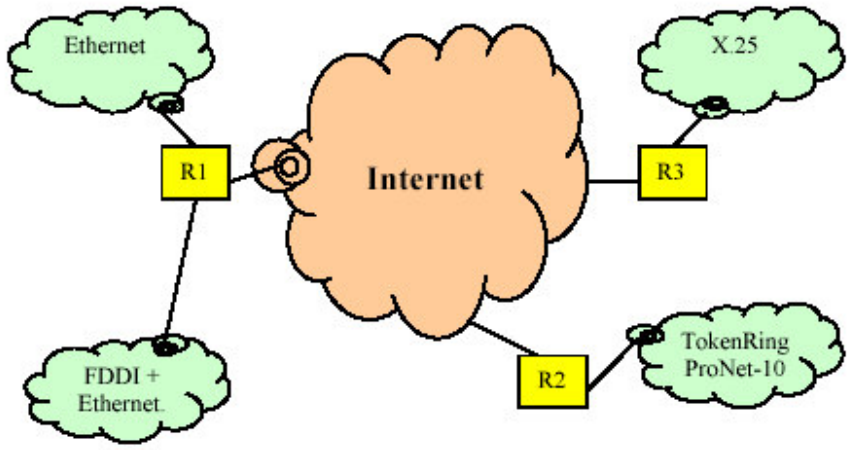

Fig.1 Redes conectadas a Internet a través de routers IP

En la estructura de Internet (Figura 1) se definen unos elementos conocidos como pasarelas o routers IP que se encargan de conectar dos o más redes entre sí y que trabajan a nivel de paquete IP (nivel 3 OSI). Estos elementos, definen las fronteras de las redes a este nivel, conocidas como redes IP. En la figura, podemos observar una de estas redes IP que contienen redes Ethernet y FDDI. Este podría ser el ejemplo de las red actual de la UPV que en realidad es una única red IP que está compuesta por diversos segmentos de red Ethernet conectados por una troncal basada en un doble anillo FDDI. Los elementos que separan estos segmentos de red, los puentes o bridges, trabajan a nivel de trama (nivel 2 OSI), por lo que una difusión Ethernet (dirección destino: FF:FF:FF:FF:FF:FF), se propagará a todas las máquinas de la red IP. Esta difusión no

pasa a través de la pasarela R1, ya que esta define la frontera de la red IP y por otro lado trabaja con los paquetes de nivel 3.

El protocolo, por tanto, permite la interconexión de redes de forma independiente al hardware de las mismas. Veamos algunas de sus características:

- Define una red virtual, Internet, con un espacio de direcciones virtuales, direcciones IP, que son asignadas de forma exclusiva a los hosts que pertenezcan a la misma.
- Se encarga de llevar los mensajes de un host a otro cualquiera de Internet, independientemente de donde esté conectado.
- El protocolo IP realiza las funciones del nivel de red, según OSI, ofreciendo un servicio sin conexión. Por lo que NO garantiza la entrega de los mensajes, el orden en que han sido enviados ni la ausencia de errores, entre otras cosas.
- La unidad de información con la que trabaja se la denomina *datagrama*.
- Los hosts y las pasarelas implementan este protocolo. Estas últimas, se centran en la tarea de conducir los datagramas desde el host origen hacia el destino remoto a través de las redes intermedias que sea necesario cruzar (encaminamiento IP).

Direcciones IP.

Las direcciones IP son de 32 bits y se dividen en dos campos: Identificación de la red IP (Net_Id) e identificación del host (Host_id) perteneciente a esa red. En la Figura 2 se muestran las distintas clases de direcciones IP.

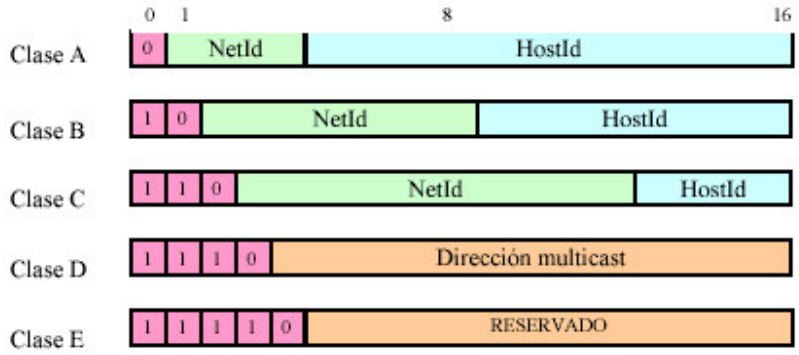

Fig. 2. Clases de direcciones IP

Las direcciones IP se suelen representar en formato decimal (4 octetos separados por un punto decimal) en lugar de expresarlas como un número de 32 bits. De esta forma podemos identificar rápidamente los octetos que pertenecen al identificador de red y los del host.

Ejemplos de direcciones:
150.214.53.127 (clase B: NetID=150.214 y HostID=53.127),
192.168.13.102 (clase C: NetID=192.168.13 y HostID=102),
11.10.200.1 (clase A: NetID=11 y HostID=10.200.11).

Sin embargo existen direcciones especiales que no deben ser asignadas a un host, ya que tienen un significado propio, asi:

- ***Dirección de red***: Las redes tienen su dirección, que no es más que el Net_Id con el identificador de la red y el Host_Id a cero. Ejemplo: 150.214.0.0 (dirección de red de la Ujaen).

- ***Dirección de broadcast***: Define la dirección de difusión a nivel de IP. Consiste en el Net_Id con el identificador de la red donde se va a realizar la difusión, y en el Host_Id se coloca todo a "1s". Ejemplo: 150.214.255.255 (dirección de difusión de la Ujaen).
- ***Difusión limitada***: Es otro tipo de difusión pero que se extiende solo sobre la red IP donde ha sido generada. Los dos campos de la dirección IP a "1s". Ejemplo: 255.255.255.255.
- ***Dirección de bucle*** (*loopback*): Es una dirección de clase A, 127.x.x.x, que se ha reservado para soportar comunicaciones entre aplicaciones del mismo host y para comprobar el funcionamiento de aplicaciones de red sin interferir en ella. Si utilizamos esta dirección para enviar un datagrama, el protocolo IP la reenvía hacia el protocolo superior, NUNCA la enviará hacia la red. Habitualmente se utiliza la dirección de bucle: 127.0.0.1.

Formato de un datagrama IP.

Los datagramas IP se encapsulan dentro de una trama, ocupando el espacio dedicado al campo de datos
de la misma (Figura 3).

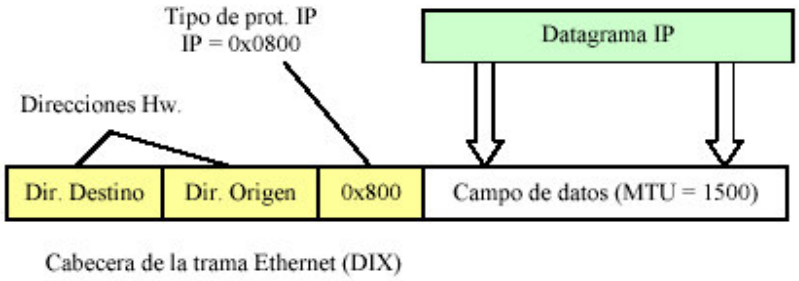

Fig. 3. Encapsulado de un datagrama IP en una trama ethernet

El tamaño máximo de un datagrama, 64Kb 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[1] 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 octetos.
El protocolo IP, lógicamente usa direcciones IP para identificar la fuente y el destino de datagrama. Ahora bien, el datagrama viaja dentro de una trama, y ésta utiliza direcciones hardware. Y por este motivo, necesitamos los servicios del protocolo ARP, para determinar la dirección hardware que corresponde a la dirección IP del destinatario.
El datagrama, 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 4 se muestra el formato de un datagrama.

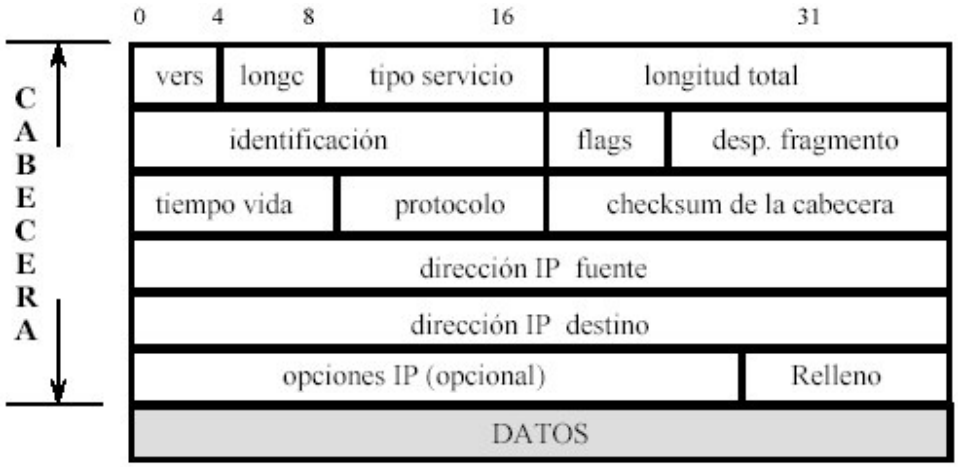

Fig. 4. Formato de un datagrama IP

- **Versión.** Especifica la versión del protocolo IP a la que pertenece el datagrama, actualmente se está utilizando la versión 4 del protocolo.
- **Longitud de la cabecera**: Define el tamaño de la cabecera IP en palabras de 32 bits, ya que esta puede ser de tamaño variable. A efectos prácticos consideraremos la cabecera IP de tamaño fijo (sin campo de opciones).
- **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. Actualmente, en esta versión de IP, este campo no es utilizado y su valor suele ser 0.
- **Longitud total**: Como su nombre indica, define el tamaño total del datagrama (cabecera + datos) en bytes.
- **Identificación**: Es un entero de 16 bits que identifica a este datagrama y lo distingue de otros datagramas que hemos enviado. Es una especie de número de secuencia que se incrementa cada vez que IP envía un datagrama.
- **Flags + Desplazamiento de fragmento**: Estos campos incluyen información útil para el mecanismo de fragmentación de datagramas. Cuando un datagrama cruza una pasarela y al otro lado existe una red con un MTU inferior al tamaño del datagrama, la pasarela lo fragmenta en trozos. Estos fragmentos son datagramas que viajan hacia el destino de forma independiente, donde son recogidos por el protocolo IP para reconstruir el datagrama original.
- **Tiempo de vida (TTL)**: 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 una pasarela, este campo es decrementado en una unidad, de forma que cuando alcanza el valor nulo, es eliminado de la red.
- **Protocolo**: Identifica el protocolo al que pertenecen la información almacenada en el campo de datos del datagrama. De forma que cuando se recibe un datagrama dirigido a nuestra máquina, y después de realizar las comprobaciones pertinentes, el protocolo IP debe saber a quién entrega los datos que lleva dicho datagrama. Así, para los protocolos ICMP, UDP y TCP los valores de este campo serán 1, 17 y 6 respectivamente.
- **Checksum de la 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 "incómodas" en la red.

- **Direcciones IP origen y destino**: Direcciones origen y destino del datagrama. Aunque el datagrama viaje a través de varias pasarelas, estos campos nunca cambian.
- **Opciones IP**: Este campo es opcional y de longitud variable. Por esto último, es necesario añadir un campo de relleno con el fin de ajustar el tamaño de este campo a múltiplos de 32 bits. Actualmente este campo está en desuso, por lo que nosotros no lo tendremos en cuenta.

Configuración TCP/IP

La orden **ipconfig** (orden de consola), para Windows 98 y 2000, proporciona información sobre la
configuración de la red en nuestra máquina (para cada uno de los adaptadores de red instalados). A
continuación se muestra la ayuda correspondiente al uso de este comando:

```
C:\Documents and Settings\l>ipconfig /?

USO:
    ipconfig [/? ¦ /all ¦ /renew [adapter] ¦ /release [adapter] ¦
              /flushdns ¦ /displaydns ¦ /registerdns ¦
              /showclassid adapter ¦
              /setclassid adapter [classid] ]

donde
    adaptador         nombre de conexión
                   (se permiten caracteres comodines * y ?, vea los ejemplos)

    Opciones:
       /?             muestra la ayuda
       /all           muestra toda la información de configuración.
       /release       libera la dirección IP para el adaptador específico.
       /renew         renueva la dirección IP para el adaptador específico.
       /flushdns      purga la caché de resolución de DNS.
       /registerdns actualiza todas las concesiones y vuelve a registrar los
                      nombres DNS.
       /displaydns    muestra el contenido de la caché de resolución DNS.
       /showclassid muestra todas las id. de clase dhcp permitidas para
                      este adaptador.
       /setclassid    modifica la id. de clase dhcp.

De manera predeterminada se muestra solamente la dirección IP, la máscara de
subred y la puerta de enlace para cada adaptador enlazado con TCP/IP.

Para Release y Renew, si no hay ningún nombre de adaptador especificado, se libe
ran o renuevan las concesiones de dirección IP enlazadas con TCP/IP.

Para Setclassid, si no hay ClassId especificada, se quita ClassId.

Ejemplos:
    > ipconfig                    ... muestra información
    > ipconfig /all               ... muestra información detallada
    > ipconfig /renew             ... renueva todos los adaptadores
    > ipconfig /renew EL*         ... renueva cualquier conexión cuyo nombre
                                      comience con EL
    > ipconfig /release *Con*     ... libera todas las conexiones que coincidan
                                      por ejemplo:
                                      "Conexión de área local 1" o
                                      "Conexión de área local 2"
```

La orden **ipconfig**, que se invoca desde una ventana MS-DOS (*Inicio-Programas-Accesorios-Simbolo del Sistema*), ofrece entre otras cosas la siguiente información:

- **Dirección de adaptador de red**: Es la dirección física que corresponde a la tarjeta de red(Ethernet en nuestro caso) que está instalada en nuestro computador y nos facilita el acceso a red
- **Dirección IP**: Dirección IP asignada a nuestra máquina, bien de forma permanente, o bien de forma dinámica mediante el protocolo DHCP.
- **Máscara de subred**: Indica qué parte de la dirección IP identifica la red, y qué parte identifica al computador (a un adaptador de red).

- **Puerta de enlace predeterminada**: Dirección IP del router que conecta nuestra LAN con el exterior (INTERNET).

EJERCICIO 1

Ejecuta la orden **ipconfig** y completa la información de la tabla siguiente:

Dirección física del adaptador Ethernet	
Dirección IP	
Máscara de subred	
Dirección IP del router (puerta de enlace)	

¿A qué clase/tipo de direcciones IP pertenece la red a la cual está conectado tu equipo?. Cual es la dirección de la red

EJERCICIO 2.
Paquetes IP

Con el analizador de protocolos, captura una sesión de paquetes IP generados al solicitar al navegador
Web el acceso a la página www.ujaen.es. Para ello se deberá filtrar el resto de tráfico, quedándonos
únicamente con los paquetes generados por esta acción.
Analiza la secuencia de paquetes IP capturados y responde a las siguientes cuestiones:

Tabla 2.1

	Identificador	TTL	Source IP	Destination IP
Paquete n. 1				
Paquete n. 2				
Paquete n. 3				
Paquete n. 4				
Paquete n. 5				

2.2 Con respecto al campo TTL (Time To Live) de la cabecera IP de los paquetes capturados, ¿son siempre iguales?, Todos los paquetes IP que envía una maquina ¿tienen el mismo TTL?

2.3. Tras analizar los campos de la cabecera IP (opciones y tipo de servicio) de los paquetes capturados IP ¿a que conclusión llegas?

EJERCICIO 3.
Fragmentación IP

No podemos observar la fragmentación que se produce en los routers pero podemos utilizar un pequeño truco para generar fragmentación en la propia interfaz del computador. Desde una ventana de DOS ejecutamos la orden siguiente (previamente habremos iniciado una captura de tramas con el filtro "icmp" para recoger todo el tráfico generado):

```
C:\> ping –n 1 –l 4000 www.ujaen.es
```

Con ello estamos forzando a nuestro computador al envío de un mensaje de 4000 bytes al destino especificado. Como estamos conectados a una red Ethernet cuya MTU es de 1500 bytes, el envío solicitado exigirá la fragmentación del mensaje en tres paquetes IP.

Compara las cabeceras de ambos fragmentos, fijándote especialmente en los campos **longitud total**, **flags**, y **desplazamiento del Fragmento**.

Primer fragmento:

Segundo fragmento:

Tercero fragmento:

3.1 ¿Cuál es el valor del campo *protocolo* de la cabecera de los tres fragmentos? Debe de ser el mismo para los fragmentos?

3.2 ¿Cuál es el valor del campo offset del segundo fragmento?. Calcula el tamaño del mensaje para que deberíamos enviar para que se generaran 4 fragmentos de tamaño máximo

3.3 ¿Cúantos bytes de información viajan en cada paquete?

EJERCICIO 4.
El comando ROUTE

El comando ROUTE permite la manipulación de la tabla de encaminamiento de nuestro sistema. Cuando
se invoca el comando sin ningún argumento se muestra la ayuda del comando:

```
E:\>route
Manipula tablas de enrutamiento de red.
ROUTE [-f] [-p] [comando [destino] [MASK máscara_red] [puerta_enlace]
[METRIC métrica] [IF interfaz]

          -f Borra las tablas de enrutamiento de todas las entradas de
          puerta de enlace. Si se usa junto con uno de los comandos,
          se borrarán las tablas antes de ejecutarse el comando.
          -p Cuando se usa con el comando ADD, hace una ruta persistente
          en los inicios del sistema. De manera predeterminada, las
          rutas no se conservan cuando se reinicia el sistema. Se
          pasa por alto para todos los demás comandos, que siempre
          afectan a las rutas persistentes apropiadas. Esta opción no
          puede utilizarse en Windows 95.

          comando Uno de los siguientes:
          PRINT Imprime una ruta
          ADD Agrega una ruta
          DELETE Elimina una ruta
          CHANGE Modifica una ruta existente

          destino Especifica el host.

          MASK Especifica que el siguiente parámetro es el valor de
          "máscara_red'.

          máscara_red Especifica un valor de máscara de subred para esta entrada
          de ruta. Si no se especifica, se usa de forma predeterminada el valor
          255.255.255.255.

          puerta_enlace Especifica la puerta de enlace.

          interfaz El número de interfaz para la ruta especificada.

          METRIC Especifica la métrica; por ejemplo, costo para el destino.
```

Ejemplos:
> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
Si no se indica IF, intentará buscar la mejor interfaz para una puerta de enlace determinada.

> route PRINT
> route PRINT 157* .... Sólo imprime las que coincidan con 157*

> route DELETE 157.0.0.0
> route PRINT

4.1. Imprime la tabla de encaminamiento de tu computador y explica las entradas.

4.2 Identifica la entrada en la tabla que corresponde con la red propia del equipo desde donde haces la práctica y elimínala.
Haz un ping a una máquina de dicha red. ¿Que ha pasado?. Apunta la dirección a la que haces el ping y la respuesta.

4.3 Vuelve a insertar la línea que antes eliminaste.

4.4.Haz lo mismo que el caso 4.2 pero elimina la entrada de la dirección de red por defecto. Intenta acceder a una dirección de internet.

ping www.ujaen.es

Explica que pasa.

4.5 Invoca el comando ping hacia una máquina de la red del laboratorio y captura el tráfico generado. Rellena la siguiente tabla.

	Dirección Física Destino	Dirección IP de destino
Pregunta		
Respuesta		

4.6 Las tablas de rutas de tu ordenador, ¿son estáticas?, justifica tu respuesta