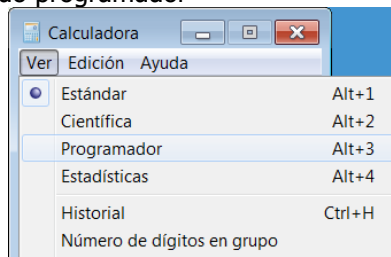
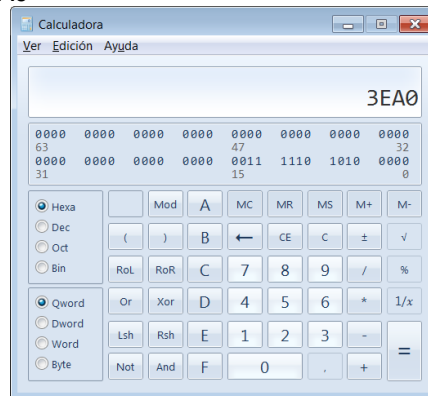


Actividad: Uso de calculadora de Windows para pasar el número hexadecimal 3EA0 a binario

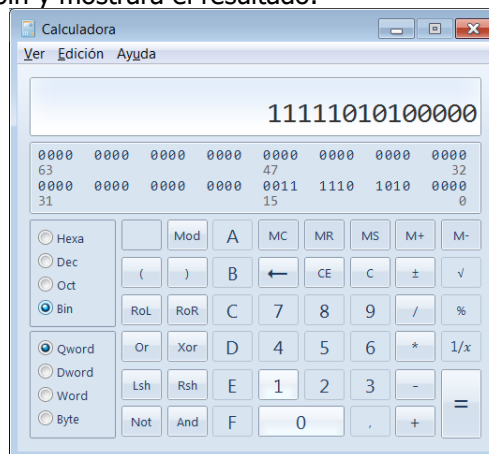
1.- Poner la calculadora en modo programador



2.- Marcar Hexa y escribir 3EA0



3.- Ya solo queda marcar bin y mostrará el resultado:



Actividad: Expresar la IP 192.168.0.1 en formato binario

Recordemos que una IP expresada en 4 números separados por puntos está utilizando 4 cantidades decimales independientes, cada una equivale a 8 bits.

192 (decimal) = 11000000 (binario)

168 (decimal) = 10101000 (binario)

0 (decimal) = 0 (binario)

1 (decimal) = 1 (binario)

Pero, cuidado, la IP debe tener 32 bits, por tanto, las dos últimas cantidades binarias las tenemos que rellenar con 0 por la izquierda hasta completar los 8 bits:

110000001010100000000000000000001

**Actividad: Expresar la MAC 94:DE:80:80:72:AF en formato binario**

Recordemos que cada hexadecimal son 4 bits y que podemos hacer la transformación transformando cada dígito hexadecimal pero, evidentemente, lo más cómodo es la calculadora:

100101001101111010000000100000000111001010101111

**Actividad: ¿Cómo influye el cambio del protocolo IPv4 a IPv6 en el protocolo TCP?**

No influye, el protocolo IP es un protocolo de la capa IP y el planteamiento de las redes por capas persigue precisamente que un cambio en una capa (en este caso IP) NO afecte a otras capas (como transporte en este caso).

**Actividad: Si navegando por internet no nos muestra la página web en nuestro navegador ¿en qué capa del modelo TCP/IP se está produciendo el problema?**

Es imposible de determinar en capa se produce con ese único dato. El navegador es una aplicación que maneja el usuario y, por tanto, está incluido en la capa de aplicación. Pero la capa de aplicación necesita de los servicios de la capa de transporte, está a su vez necesita los servicios de la capa de internet y así hasta llegar a la capa de Acceso a red (o subred); en conclusión si fallan las capas inferiores tampoco podremos visualizar la página web.

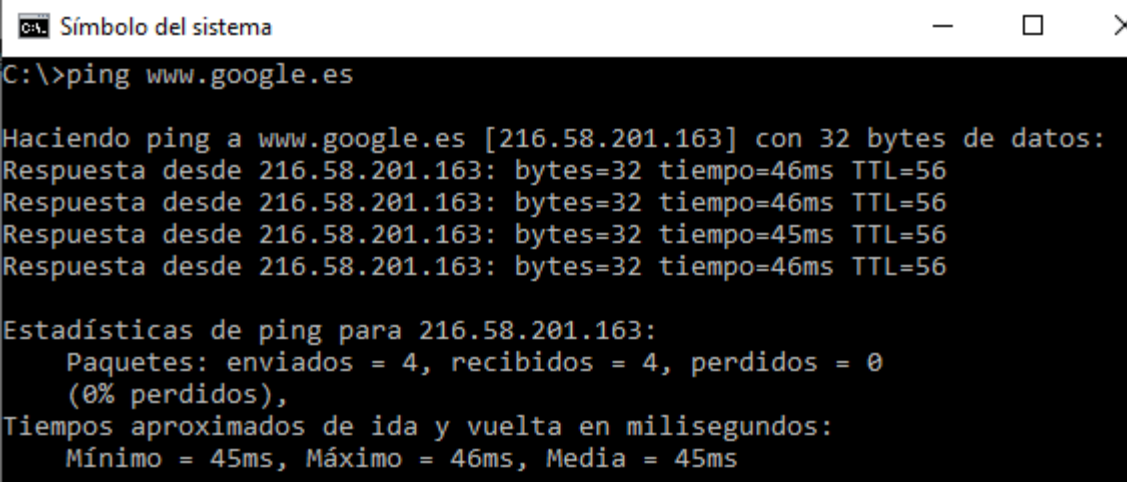
**Actividad: Si enviamos un ping a un equipo y este no responde ¿Qué capa del nivel TPC/IP está fallando?**

Tampoco podemos determinar que capa falla (de hecho en algunos casos no falla nada simplemente el cortafuegos por seguridad lo bloquea), aunque en este caso podemos acotar el problema puesto que el protocolo ICMP (responsable del ping) pertenece a la capa IP y, por tanto, necesita de los servicios de las capas inferiores pero no necesita a la capas de sesión ni a la capa de aplicación.

**Actividad: ¿Cómo puedo saber la IP del servidor web [www.google.es](http://www.google.es)?**

Lo más fácil es ir a la línea de comandos (Accesorios – Símbolo del sistema, o bien, ejecutar cmd) y escribimos el comando ping [www.google.es](http://www.google.es)

Ping es un comando que envía una señal a un dispositivo y espera respuesta, si la recibe muestra un mensaje con el tiempo que ha tardado en responder el dispositivo si no la recibe indica que el tiempo de espera agotado.



```
Símbolo del sistema
C:\>ping www.google.es

Haciendo ping a www.google.es [216.58.201.163] con 32 bytes de datos:
Respuesta desde 216.58.201.163: bytes=32 tiempo=46ms TTL=56
Respuesta desde 216.58.201.163: bytes=32 tiempo=46ms TTL=56
Respuesta desde 216.58.201.163: bytes=32 tiempo=45ms TTL=56
Respuesta desde 216.58.201.163: bytes=32 tiempo=46ms TTL=56

Estadísticas de ping para 216.58.201.163:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 45ms, Máximo = 46ms, Media = 45ms
```

La IP es 216.58.201.163

### Actividad: ¿Podría navegar por internet sin DNS?

La función principal del protocolo DNS es convertir los nombres de dominio en las IPs asociadas, es como una agenda, pero puedo navegar por internet si conozco las IPs, similar a marcar el número de teléfono en un móvil sin usar la agenda. Por ejemplo, para visitar la web [www.google.es](http://www.google.es) basta con marcar su IP 216.58.201.163

¿Y el puerto?

El puerto viene a ser algo similar a la extensión con la que deseamos hablar. Al no indicar el puerto se asume que se quiere conectar con el puerto 80, es decir, que si en el navegador ponemos 216.58.201.163:80 nos aparecerá también la página.

### Actividad: Traducción DNS en local. Bloqueo del acceso a una web

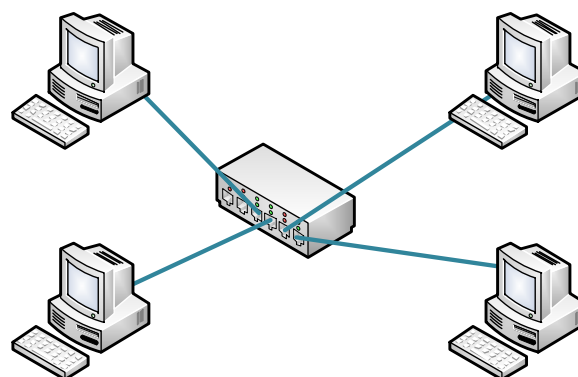
No siempre se hace una consulta a nuestros servidores DNS para saber la IP asociada. Tanto Windows como Linux, hay un fichero especial "hosts" donde se encuentra una relación de IPs y dominios que se consultan antes de realizar la petición al servidor DNS.

Si manipulamos estos ficheros poniendo una IP errónea asociada a un determinado dominio se producirá una traducción equivocada y no se conseguirá acceder a la web. Por ejemplo, si en Windows abrimos el bloc de notas (ejecutado como administrador) y editamos el fichero `c:\windows\system32\drivers\etc\hosts` escribiendo las líneas siguientes bloqueamos youtube:

```
hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
127.0.0.1 | www.youtube.com
127.0.0.1 www.youtube.es
127.0.0.1 youtube.com
127.0.0.1 youtube.es
```

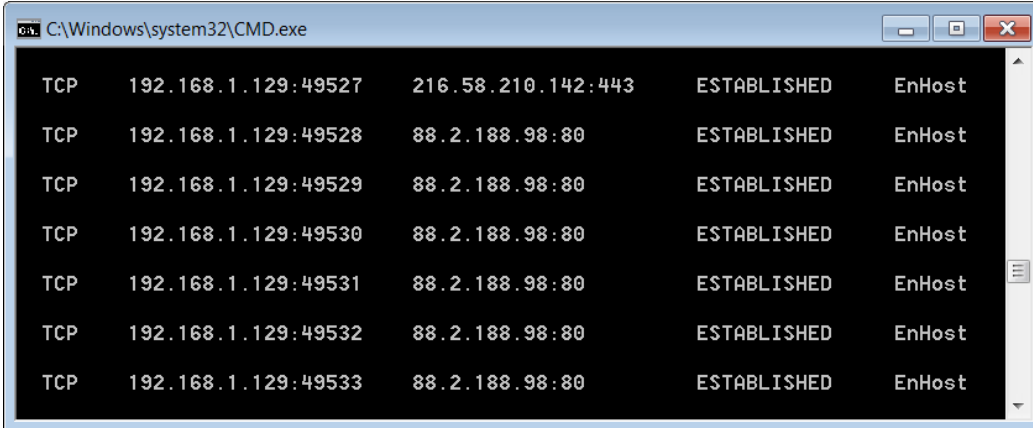
### Actividad: ¿qué topología física tiene la red del siguiente esquema?



La topología física es en estrella.

### Actividad: ¿Qué conexiones tenemos abiertas desde nuestro equipo?

Con el comando netstat podemos mostrar en pantalla las conexiones abiertas.



```
C:\Windows\system32\CMD.exe
TCP    192.168.1.129:49527    216.58.210.142:443    ESTABLISHED    EnHost
TCP    192.168.1.129:49528    88.2.188.98:80        ESTABLISHED    EnHost
TCP    192.168.1.129:49529    88.2.188.98:80        ESTABLISHED    EnHost
TCP    192.168.1.129:49530    88.2.188.98:80        ESTABLISHED    EnHost
TCP    192.168.1.129:49531    88.2.188.98:80        ESTABLISHED    EnHost
TCP    192.168.1.129:49532    88.2.188.98:80        ESTABLISHED    EnHost
TCP    192.168.1.129:49533    88.2.188.98:80        ESTABLISHED    EnHost
```

### Actividad: ¿Cómo puedo saber la MAC del equipo de mi red con IP 192.168.0.10?

La asociación entre MAC e IPs la gestiona nuestro PC desde la tabla ARP, la tabla conserva las MAC de los equipos con los que nos hemos comunicado recientemente, para consultar esta tabla basta escribir desde la línea de comandos: arp -a

Si la IP no aparece en la tabla es porque con ese equipo no nos hemos comunicado, forzamos la comunicación con ping 192.168.0.10 y volvemos a mostrar la tabla con arp -a, y nos aparecerá la MAC asociada a 192.168.0.10

### Actividad: Resume lo máximo posible las siguientes direcciones IPv6

- 2000:0002:2000:0002:2000:0002:2000:0002
- 0000:0000:0000:0000:0000:0000:0000:000A
- 2000:2:2000:2:2000:2:2000:2
- ::A

### Actividad: Detalla con todos los caracteres las siguientes IPv6

- 2::A000
- 2222:0:0:2::A0C
- 0002:0000:0000:0000:0000:0000:0000:A000
- 2222:0000:0000:0002:0000:0000:0000:0A0C

### Actividad: ¿Cómo podemos ver la configuración IPv4 de nuestro dispositivo?

Depende del sistema que usemos y de las diferentes versiones que hay, pero aquí os dejo algunas posibles:

- a) Windows: A través del símbolo del sistema (cmd) podemos teclear el comando ipconfig /all. También en modo gráfico (depende de la versión), a través del panel de control – configuración de red – detalles de la conexión de red.
- b) Linux: Hay muchas distribuciones pero desde el símbolo del sistema con ifconfig nos muestra la configuración.
- c) Android: Si estamos conectados por WIFI: Ajustes – conexiones - wifi – Nombre de red a la que estamos conectados. Si estamos conectados por HSDPA o similar en acerca del teléfono – estado.

### Actividad: ¿Cómo puedo saber si mi red es pública o privada?

La manera más sencilla es por la IP, si está dentro de los rangos reservados a IPs privadas será una red privada y el resto (salvo alguna dirección especial) será pública. Recordemos que los rangos son: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.0.0, 192.168.0.0 - 192.168.255.0. Por ejemplo, la típica red doméstica formada por los ordenadores, móviles, Smart tv, etc que tenemos en casa conectados a través de router de fibra es una red privada y suele ser la red 192.168.0.0/24

### Actividad: ¿Cómo puedo saber si mi IP pública es dinámica o estática?

Si estamos en una red privada, como en el ejemplo mencionado antes, nuestro router está compartiendo una IP pública para todos los dispositivos de casa (poniendo en un buscador cual es mi IP pública podemos conocerla). La solución más sencilla mirar la IP pública, apagar el router, esperar unos segundos y volver a encender el router. Si al mirar de nuevo la IP se mantiene es estática sino es dinámica. Algunas web controlan los accesos desde la misma IP, si es dinámica un truco para cambiarla y "engañar" a la web es apagar y encender el router.

**Actividad: Reflexiona sobre cómo afectará el internet de las cosas al direccionamiento (Internet of things, consiste en conectar los objetos cotidianos como electrodomésticos, coches, semáforos, alarmas, etc. a internet para poderlos controlar desde cualquier lugar. Esto supondrá en 2020 que unos 50.000 millones de dispositivos se conectarán a Internet).**

Tal como hemos visto en el tema, hay direccionamiento a todos los niveles, es decir, tenemos que poder identificar a cada dispositivo en los diferentes niveles.

A nivel más bajo nos encontramos con la MAC, una dirección que tiene que ser exclusiva de cada dispositivo, cada MAC son 48 bits, lo que supone unas combinaciones posibles de  $2^{48} = 281.474.976.710.656$  suficiente para el número de dispositivos que se espera.

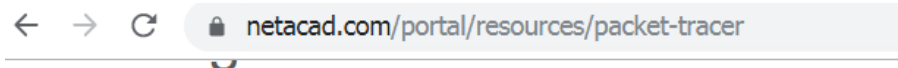
El siguiente nivel es IP una dirección que también debe identificar a cada dispositivo, IPv4 son 32 bits, las combinaciones posibles son 4.294.967.296, insuficientes para los 50.000 millones. Pero ya se está implantando la sustituta IPv6, una dirección de 128 bits, que suponen  $3,4 \times 10^{38}$ , que no plantearía ningún problema.

El siguiente nivel es TCP, realmente este nivel se utiliza para identificar elementos dentro del dispositivo, o sea, va siempre en combinación con la IP. Por ejemplo, si queremos acceder a las carpetas compartidas de un ordenador, conectamos al puerto 139 y a la IP del ordenador, si queremos ver la web alojada en ese mismo ordenador, accedemos al puerto 80 y a la misma IP. Si en el internet de las cosas, si se mantiene algo similar, sería una IP para acceder al control de la calefacción de nuestra casa y un puerto para encenderla en una habitación en concreto.

En el nivel de aplicación no habrá tampoco ningún inconveniente porque el direccionamiento es una combinación de caracteres que podemos alargar lo que necesitemos.

### Actividad: Instalación de Cisco Packet Tracer

Para poder descargar el simulador de Cisco debemos registrarnos en la web [www.netacad.com](http://www.netacad.com):



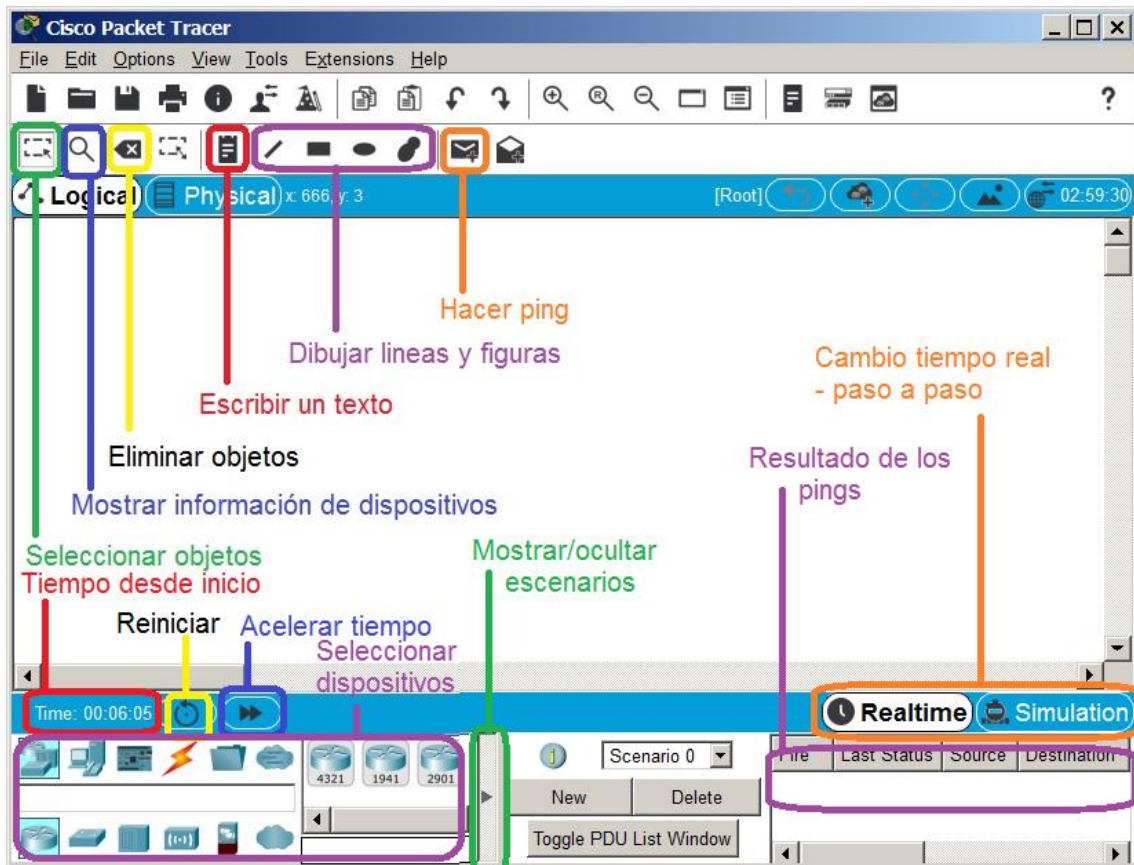
Elija el sistema operativo que está usando y descargue los archivos relevante [preguntas frecuentes](#). Vea los [tutoriales](#).

Packet Tracer requerirá autenticación con su usuario y contraseña cuando lo para cada inicio de sesión en un SO nuevo. (1)

**Windows versión 7.2.2 para equipos de escritorio (en inglés)**

[Descarga de 64 bits](#)

[Descarga de 32 bits](#)



Actividad: Describir un envío de correo electrónico a través de las capas del modelo TCP-IP

Seguiremos el siguiente esquema a la hora de indicar el traspaso de información entre capas:

Destino	Datos
Remite	

Supongamos un correo electrónico de [juan@juan.es](mailto:juan@juan.es) a [maria@maria.es](mailto:maria@maria.es), asunto "Saludos", mensaje "Hola". El usuario Juan a través de, por ejemplo, Outlook redacta el correo a María y lo envía (capa de aplicación, que es la capa más cercana al usuario).

<a href="mailto:maria@maria.es">maria@maria.es</a>	Asunto:Saludos
<a href="mailto:juan@juan.es">juan@juan.es</a>	Mensaje:Hola

La capa de aplicación envía a la capa de transporte el correo para que lo procese. Esta capa tomará todo lo anterior como datos (no entiende los protocolos superiores, se limita a capturar lo recibido) y le incluirá su remite (puerto origen) y su destino (puerto destino) y lo pasará a la capa de internet.

25	<a href="mailto:maria@maria.es">maria@maria.es</a>	Asunto:Saludos
1536	<a href="mailto:juan@juan.es">juan@juan.es</a>	Mensaje:Hola

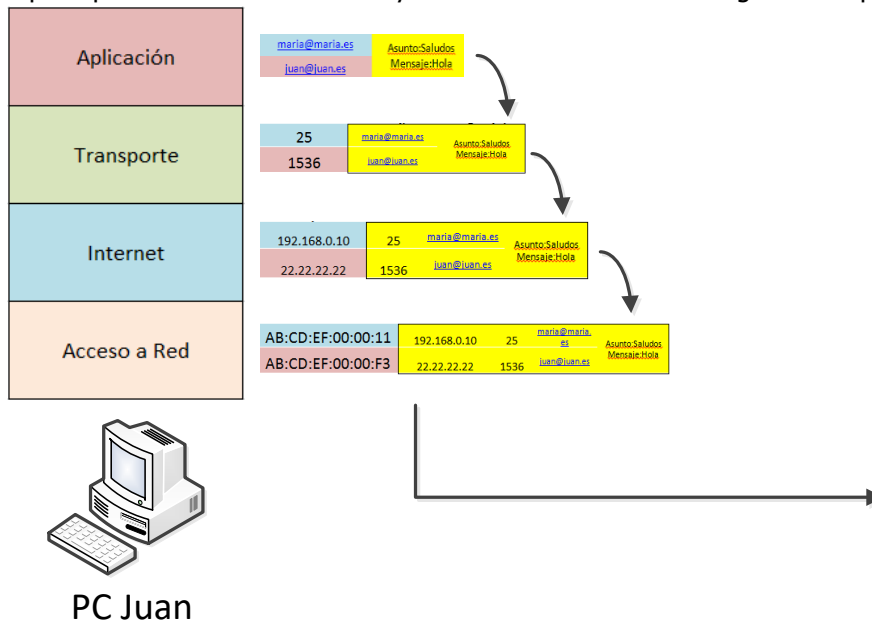
La capa de internet tomará todo lo recibido como datos, le añadirá IP origen e IP destino y lo pasará a la capa de acceso a red:

192.168.0.10	25	<a href="mailto:maria@maria.es">maria@maria.es</a>	Asunto:Saludos
22.22.22.22	1536	<a href="mailto:juan@juan.es">juan@juan.es</a>	Mensaje:Hola

Por último, la capa de acceso a red le añadirá la MAC de su tarjeta de red y la MAC del siguiente salto en la red.

AB:CD:EF:00:00:11	192.168.0.10	25	<a href="mailto:maria@maria.es">maria@maria.es</a>	Asunto:Saludos
AB:CD:EF:00:00:F3	22.22.22.22	1536	<a href="mailto:juan@juan.es">juan@juan.es</a>	Mensaje:Hola

En el equipo destino ocurrirá el proceso inverso. La tarjeta de red eliminará la MAC y enviará a la capa superior los datos recibidos y así sucesivamente hasta llegar a la capa de aplicación.



*Nota: El proceso no es exactamente como se ha descrito pero sirve para comprender el funcionamiento de la comunicación entre niveles y el concepto de encapsulamiento. Realmente, como curiosidad que no es tema de aprendizaje en esta unidad: los correos se envían a los servidores de correo y se descargan de los servidores de correo (no se envían directamente al destinatario, este puede tener su PC apagado por ejemplo); la IP de destino no ha aparecido por casualidad sino que paralelo a este proceso ha habido una consulta a los servidores DNS sobre la IP asociada a maria.es; la primera MAC que aparece no es la del equipo de María sino el primer salto para salir de la red local en la que estamos (el mensaje atravesará redes que no tienen por qué utilizar MAC en su nivel inferior, como en redes Ethernet, puede ser red Frame Relay).*